A Framework for Service-Guaranteed Shared Protection in WDM Mesh Networks

Pin-Han Ho and Hussein. T. Mouftah, Queen's University at Kingston, Ontario, Canada

ABSTRACT

In this article a framework for end-to-end service-guaranteed shared protection in dynamic wavelength division multiplexing (WDM) mesh networks, called Short Leap Shared Protection (SLSP), is introduced. The idea of SLSP is to divide each working path into several overlapped protection domains, each of which contains a working and protection path pair. In addition to a guaranteed restoration service, SLSP is designed to satisfy the future requirements of wavelength-routed optical mesh networks in scalability, class of service, and capacity efficiency. Tutorial-like discussions are given in the architecture design and signaling mechanisms for implementing the SLSP framework in a dynamic network environment with examples and illustrations. To show that SLSP can improve capacity efficiency, simulations are conducted using four networks (22-, 30-, 79-, 100-node) for a comparative study between ordinary shared protection schemes and SLSP.

INTRODUCTION

As metropolitan area networks (MANs) and other medium-sized networks become more prevalent and commercially important, new research is focusing on design issues that are very different from those of the Internet core networks. The differences are mainly due to the fact that bandwidth demand is becoming more dynamic with smaller granularity. In addition, a multiservice network environment is strongly solicited for satisfying lightpath provisioning of different service requirements. Therefore, design of control and management for this type of networks has to consider survivability, class of service, and dynamicity from a different viewpoint than the Internet core networks.

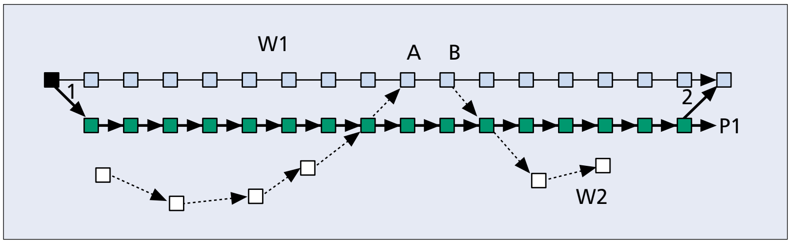
THE ERA OF DYNAMIC PROVISIONING

Research and development in dynamic and automatic provisioning of lightpaths have seen rapid progress in both industry and academia for a number of years. These provisioning mechanisms are greatly enhanced by the advent of photonic cross-connects (PXCs) [1] and tunable transceivers. With PXCs, optical switching can be performed at less cost than in traditional optical cross-connect (OXC) networks due to the fact that less optical-electronic-optical (O/E/O) conversion, and fewer inventories and layers of management are needed. Meanwhile, extensive efforts are underway to exploit lightpath provisioning speed and signaling responsiveness, and to further develop and improve queue-length initiated automatic provisioning and the integration of signaling instances between different control layers. With the above improvements on traditional OXC networks, the era of dynamic configuration and automatic provisioning of lightpaths in wavelength-division multiplexing (WDM) mesh networks has come of age. Dynamic routing is implemented with a suite of online algorithms and automatic signaling mechanisms to satisfy the connection requests that arrive one by one with no prior knowledge of future arrivals.

SURVIVABILITY WITH DYNAMIC TRAFFIC

As network traffic becomes more dynamic, survivability and class of service requirements have never been relaxed. For the past decade, spare capacity allocation in survivable networks has been an area of much work and interest, but many approaches still utilize NP-hard optimization processes based on static working traffic demands [2–5]. Although most of the static schemes can be used for conducting the reallocation of spare capacity while the network is running, their fatal flaw is that after a time-consuming optimization process, the derived solution can be far from optimal as traffic rapidly changes. Therefore, the static schemes are more suited to use in designing small-sized networks, or networks where demands are less dynamic. To serve large networks with traffic that changes frequently, issues of survivability and service continuity have become a challenge compared to dealing with only static network traffic.

0163-6804/02/$17.00 © 2002 IEEE



■ **Figure 1.** *An example to illustrate the SRLG constraint.*

To overcome the computational complexity problem, heuristic algorithms have been reported [6–8], resulting in a compromise between performance (*probability of blocking* is the most commonly used performance index) and computational efficiency. The above process is also called *survivable routing*. A survivable routing algorithm is used to dynamically allocate the current connection request into a network with protection service, while maximizing the probability of successfully allocating subsequent connection requests in the network. With survivable routing, each traffic flow's working lightpath is routed first, followed by its protection lightpath in the source node, so the difference of importance between the two paths can be emphasized. The working and protection lightpaths must be node-disjoint, and the search for protection resources has to follow the shared risk link group (SRLG) [9] constraint. To be more specific, a protection path is derived by using the shortest path algorithm with a well designed cost function and link metrics on the network link state with the corresponding working path and prohibited protection resources excluded.

Modeling for Restoration Latency

In contrast to dedicated protection such as 1+1, shared protection that allows several working paths to make use of the same protection resources can yield better capacity efficiency. However, for shared protection the speed of recovering service availability after the occurrence of failure is slower than in dedicated protection, because shared protection resources must be configured before the optical traffic flow can be switched to them. In addition, with shared protection it is important to consider the latency of on-the-fly signaling between the path switch label switched router (LSR) (PSL) and path merge LSR (PMLs) [10], in the terminology of multiprotocol label switching (MPLS), which switch the traffic over the protection path and merge the traffic back to the original working path, respectively. The following modeling for the restoration time, T_R, in using the shared protection is necessary for further discussion:

$T_R = T_{signaling} + T_{config} + T_{detection}$,

where $T_{detection}$ is for failure detection and localization, $T_{signaling}$ is for signaling propagation and node processing, and T_{config} is the time duration for configuring the optical network elements along the protection path. The above relationship can be reformed as

$$T_R \approx \frac{D_w + D_p}{u} + T_{\det ection} + T_{config},$$

where u is the speed of light in the medium (generally, $u = 2 \times 10^8$ m/s), and D_w and D_p are the physical distance of the working and protection path segments. Note that $T_{detection}$ and T_{config} are independent of the distance between the PSL and PML. T_{config} is independent because the configuration process along the protection path after the occurrence of failure can be conducted in a pipeline manner. Since this article investigates the impact of routing strategy on restoration time, the signaling delay is taken as the main contribution to the restoration time T_R, which is directly proportional to the physical distance of working and protection paths.

Toward a Generalized Framework

In order to improve the scalability and capacity efficiency, and meet the class of service requirements for generating more revenue, a generalized framework of shared protection schemes needs to be defined. In this article, we introduce Short Leap Shared Protection (SLSP), which is devised as an approach to survivable routing in dynamic WDM networks as a solution to the above requirements. We give an overview of the constraints on resource sharing and a general idea of restoration service. A series of tutorial-like examples and illustrations are provided for presenting the idea of the SLSP framework. Discussions are given for deeper understanding of the characteristics of the framework. Lastly, a simulation is conducted to verify its performance behavior.

A Spectrum of Restoration Service

In this section the constraint imposed by the SRLG and conventional shared protection schemes (including path-based and link-based protection) are briefly overviewed.

Shared Risk Link Group Constraint

The SRLG constraint defines the availability of protection resources to a working path, which stipulates that any two working paths sharing the same risk of failure (or in the same SRLG) cannot make use of the same protection resources. The SRLG constraint is imposed on the selection of protection resources for a newly arrived working path, which marks some of the existing protection wavelength channels as *prohibited* to avoid a resource conflict during a restoration process after failure. The purpose of following the SRLG constraint is to guarantee 100 percent restorability for failure on any single link or node in the network. An example demonstrating the SRLG constraint is given in Fig. 1. Since W2 traverses the link A-B, which shares the same risk of single failure with W1, the protection path for W2 should exclude the possibility of using any of the protection resources used by W1. Otherwise, a failure on link A-B will result in a resource conflict between W1 and W2 when both paths switch their traffic to the same protection channel. Therefore, the SRLG constraint stipulates that W2 cannot take any network resources along P1 for protection purposes.

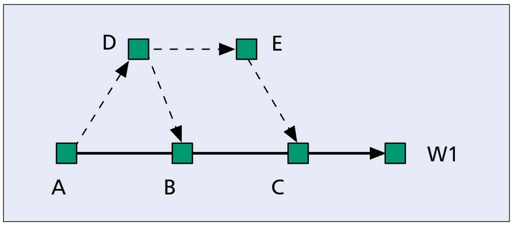


Figure 2. *An example of link-based protection.*

It is clear that as W1 becomes longer, there would be more working lightpaths belonging to the same SRLG that suffers the sharing constraint. We define the SRLG constraint to be *relaxed* if extra switch-merge node pairs are allocated along a working lightpath (or divide a large SRLG into several small ones) so that the sharing of protection resources can be improved.

Path-Based Shared Protection

For path-based protection, the source node of a working path computes a protection path by ensuring that the protection path is diversely routed from the working path according to the SRLG constraint. If a fault occurs on the working path, the terminating node in its control plane realizes the fault and sends a notification indicator signal (NIS) [10] to the first hop node of the path to activate a switchover. The source then immediately sends a wake-up packet to activate the configuration of the nodes along the protection path and then switches traffic over from the working path to the protection path. An example of path-based protection is shown in Fig. 1: W1 is protected by diversely routed protection path P1.

As discussed in the previous paragraphs, the restoration time is strongly determined by the total length of the working and protection path segments that circumvent the failed network element. Although path-based protection yields a simple signaling mechanism by circumventing any failure in an end-to-end fashion, it cannot guarantee the failure recovery time for the lightpaths that need to meet stringent requirements on service continuity. In addition, with the path-based protection scheme, the SRLG constraint may limit resource sharing without any relaxation, and as a result impair performance.

Link-Based Shared Protection

Link-based protection was originally devised for ring-based network architectures such as synchronous optical network (SONET), where network planning efforts significantly influence performance. The migration of link-based protection from ring-based networks to mesh networks was explored extensively in [3–5]. In general, link-based protection in mesh networks is defined as a protection mechanism that performs fault localization during the occurrence of a failure, restores the interrupted services by circumventing the traffic from a failed link or node at the upstream neighbor node, and merges the traffic back to the original working path at the downstream neighbor node. With this definition, to protect both the downstream neighbor link and node, two merge nodes must be arranged for every node along a working path. As an example (shown in Fig. 2), to protect W1 along link A-B and node B, two merge nodes, B and C, must be arranged for node A.

Link-based protection provides the fastest restoration due to fault localization and better throughput due to the relaxation of the SRLG constraint. However, the downstream neighbor node and link are required to have separate protection segments, which may impair performance by consuming extra protection resources. To perform link-based protection on both links and nodes along a working path, a new scheme is required such that the consumption of protection resources is reduced without losing much restoration speed.

SLSP Framework

This section introduces the strategy of SLSP through detailed discussion. We show that the SLSP framework generalizes traditional link- and path-based shared protection, and can provide a wider spectrum of service levels with finer restoration granularity.

SLSP Descriptions

The protection scheme, SLSP, is an end-to-end service-guaranteed shared protection scheme, which enhances the link- and path-based shared protection to provide finer service granularity and higher network throughput. The main idea of SLSP is to subdivide a working path into several equal-length and overlapped segments, each assigned (by the source node) a protection domain ID after the working path is selected, as shown in Fig. 3. The overlap between adjacent protection domains (or *P domains* in the following context) is for the purpose of protecting node failure along a working path. A diversely routed protection path segment is searched for each working path segment in a *P domain*. The diameter of a *P domain* is defined as the hop count of the shortest path between the PSL and PML of the *P domain*.

Unlike the reported survivable routing schemes, SLSP performs the restoration process within a predefined *P domain* instead of along the whole path. With each working path segmented, restoration service can be guaranteed by limiting the size (or the sum of the distance of working and protection path segments) of *P domains*. Compared with path-based protection, the segmentation of working paths also yields less computation latency during path selection by using a fully distributed computing process. With this, the task of end-to-end diverse routing is divided into several subtasks, each of which deals with less information and link states by the PSLs of the working path.

The definition of SLSP generalizes the shared protection schemes, in which link- and path-based shared protection can be categorized as two extreme cases of SLSP with domain diameters of 1 and *H*, respectively, where *H* is the hop count of the working path. Note that SLSP1 (i.e., protection domains with a single hop as diameter) cannot perform node protection, and

The main idea of SLSP is to sub-divide a working path into several equal-length and overlapped segments, each of which is assigned (by the source node) a protection domain ID after the working path is selected.

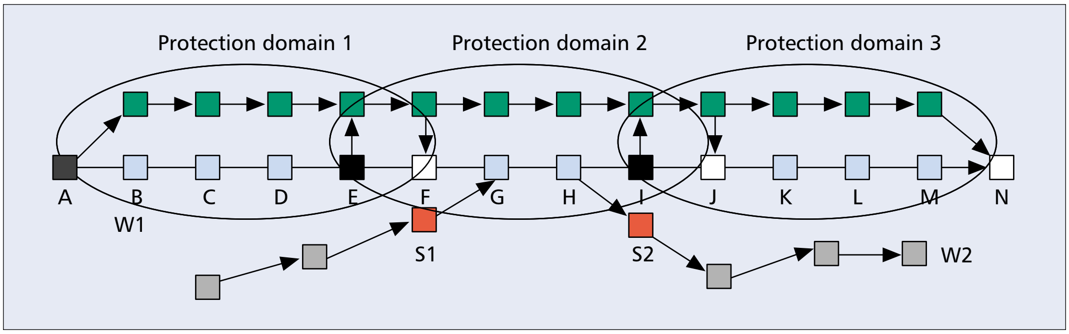


Figure 3. *The SLSP protection scheme divides the working path into several overlapped* P domains.

The adoption of a tell-and-go mechanism can further reduce the total configuration time to a minimum extent (i.e., the latency for configuring a single node.

needs to cooperate with SLSP2 to form the end-to-end link-based protection scheme defined in the previous section. This article focuses on SLSP2 and takes SLSP2 as an approximation of the link-based shared protection.

Here we use Fig. 3 to illustrate how a lightpath under SLSP is configured and recovered when a fault occurs. Node A is the source node and node N is the terminating node. The first *P domain* (protection domain 1) starts at node A and ends at node F. The second *P domain* (protection domain 2) is from node E to node J, and the third is from node I to node N. In this case, (A, F), (E, J) and (I, N) are the corresponding PSL-PML pairs for each *P domain*. Since each *P domain* overlaps its neighbor *P domains* by a link and two nodes, a single failure on any link or node along the path can be handled by at least one *P domain*. After a fault on the working path occurs, the PSL of the *P domain* where the failure occurs is notified to activate a traffic switchover. For example, a fault on link C-D or node C is localized by its downstream node D. A fault on link F-G or node F is localized by the downstream node G. In the former case, node C sends an NIS to notify node A that a fault occurred in its *P domain*. In the latter case, node G sends an NIS to node E for a fault notification. If a failure occurs to a link or node covered by two *P domains* (e.g., link E-F), the node localizing the fault (i.e., node F) will notify the closest upstream PSL (i.e., node E in this case) to perform a restoration. After receiving the NIS, the PSL (i.e., node A or E) immediately sends a wake-up packet to activate the configuration of each node along the corresponding protection path segment of its *P domain*, and then switches the traffic over the protection path. The adoption of a tell-and-go mechanism, by which the traffic flow is switched to the protection path in a small amount of time after the wake-up packet is sent without waiting for back and forth acknowledgments, can further reduce the total configuration time to a minimum extent (i.e., the latency for configuring a single node).

Allocation of Protection Domains

The heuristic approach of allocating *P domains* along a working path is introduced in this section. Fixed alternate routing (FAR) is adopted to route working paths. With FAR, each node is equipped with a routing table containing a group of alternate paths to all the other nodes in the network. As a connection request arrives, the source node coordinates the lightpath allocation process by deriving the alternate paths to the destination from its routing table, probing the availability of wavelength channels along each alternate path, and assigning PSLs and PMLs to a specific set of nodes for each available lightpath according to the restoration speed requirements. The nodes that behave as PSLs invoke the survivable routing algorithm to allocate the protection paths to form the corresponding *P domains*.

Using Fig. 3 as an example again, we assume that W1 is one of the available working lightpaths. The source node itself is a PSL, which also assigns nodes E and I as PSLs, and nodes F, J, and N as PMLs. Each PSL node derives residual network link states by excluding the whole working path (except its PML node) as well as the *prohibited* wavelength channels (i.e., protection resources that violate the SRLG constraint) from the network topology. Then the Shortest Path First algorithm is performed by each PSL to derive the protection path segment for its *P domain*. The source node coordinates the entire distributed computing process, and selects the most qualified allocation of *P domains* among the available working lightpaths.

In the distributed computing process, the coordination of the SRLG constraint is performed by each PSL along the working path instead of the source node that usually behaves as a border router with heavy workload. Each PSL is in charge of deriving the *prohibited* wavelength channels before calculating the corresponding protection path segment. As an example, shown in Fig. 3, let nodes S1 and S2 be one of the PSLs and PMLs for W2, respectively. S1 needs to inspect all the working path segments sharing the same risk with its working path segment E-F-G-H-I-J. Then S1 marks all the protection resources registered by those working path segments as *prohibited* before Dijkstra's Shortest Path First algorithm is invoked.

What SLSP Brings to Us

The advantages of the SLSP framework over the ordinary path protection schemes are stated below. First, both the notification and the traveling of the wake-up message are performed within a *P domain*, therefore, the restoration time can be guaranteed by adjusting the size of the *P domains* along a working path. Second, the com-

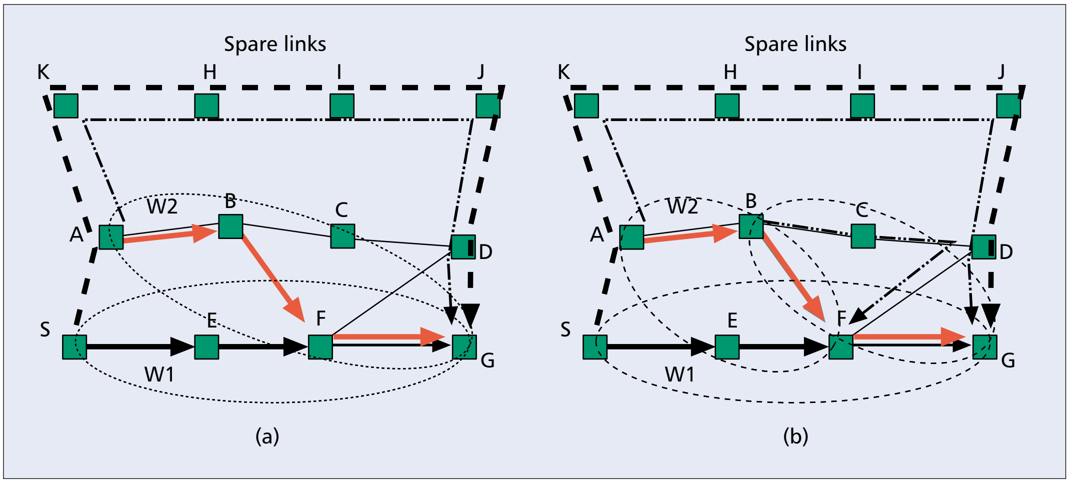


Figure 4. *In a), the spare capacity has to be the sum of the two working paths. In b), the spare capacity can be shared by W1 and W2 along A-K-H-I-J-D by dividing W2 into two* P domains*. The prtection path segment for W1 and W2 is marked as dashed line and dotted-dashed line, respectively. The circles in the two graphs are the protection domains.*

putational complexity of protection paths is simplified due to the segmentation of working paths. The fully distributed allocation process is scalable to the length of working paths. Compared with the path-based protection, since less protection resources need to be marked as *prohibited* by each PSL, the total computation complexity for correlating the SRLG constraint can be reduced. Third, due to the segmentation of working paths, more resource sharing can be achieved by relaxing the SRLG constraint. An example is shown in Fig. 4. In Fig. 4a, working paths W1 and W2 have an overlapped span in both of the *P domains* S-A-K-H-I-J-D-G-F-E and A-K-H-I-J-D-G-F-B for W1 and W2, respectively, so they share the same risk of a single failure. To restore W1 and W2 at the same time once a failure occurs on span F-G, the number of spare links prepared for W1 and W2 should be the sum of the bandwidth of W1 and W2 along the spans A-K-H-I-J-D-G. With W2 being segmented into two *P domains* A-K-H-I-J-D-F-B and B-C-D-G-F as shown in Fig. 4b, the spare capacity along the spans A-K-H-I-J-D for W1 and W2 can be the maximum bandwidth of the two working paths. In other words, the segmentation of the working path W2 at node F saves the spare capacity required. The protection path for F-G of W2 can be in the newly assigned *P domain* B-C-D-G-F. In this example, if each working path has the same bandwidth, two spare links of the bandwidth are saved after the reconfiguration.

In Fig. 4a, the spare capacity has to be the sum of the two working paths. In Fig. 4b, the spare capacity can be shared by W1 and W2 along A-K-H-I-J-D by dividing W2 into two *P domains*. The protection path segment for W1 and W2 is marked as dashed line and dotted-dashed line, respectively. The circles in the two graphs are the *p domains*.

From the network administrative perspective, SLSP provides a trade-off between restoration time and the amount of protection resources consumed, with which the class of service can be achieved with finer granularity. The major disadvantage incurred by using SLSP is the increase of signaling complexity, which is beyond the scope of this article.

No. nodes	No. of edges	Avg. nodal degree	Avg. distance	Best diameter	Size of *P domain*
22	44	4.0	2.49	**2**	**4.6**
30	63	4.2	2.71	**2**	**4.5**
79	108	2.73	6.57	**3**	**10.3**
100	179	3.58	9.5	**4 (or 5)**	**16.9**

Table 1. *Topology information and a summary of simulation results.*

Simulation

Assumptions

The simulation study aims to evaluate performance in terms of probability of blocking while dynamically setting up working paths with an end-to-end protection mechanism (either path-based or SLSP*n*, where $n \geq 2$). We examine the protection strategies listed above in 22-node, 30-node, 79-node, and 100-node networks. Without loss of generality, all connections are assumed to be a single lightpath between an S-D pair equipped with an end-to-end shared protection service.

The networks are assumed to have two fibers that share the same risk of single failure along each span in each direction. Each fiber contains 16 wavelength channels with the same bandwidth. Every node is provided with the shortest, second shortest, and third shortest paths in hop count to all the other nodes as alternate paths. Each connection request is for an establishment of a lightpath between two nodes, which arrives according to a Poisson process and departs after a period defined by an exponential distribution function. The protection resources must be on the same wavelength plane with the corresponding working lightpath, since no wavelength conversion is allowed in the PSLs along a working

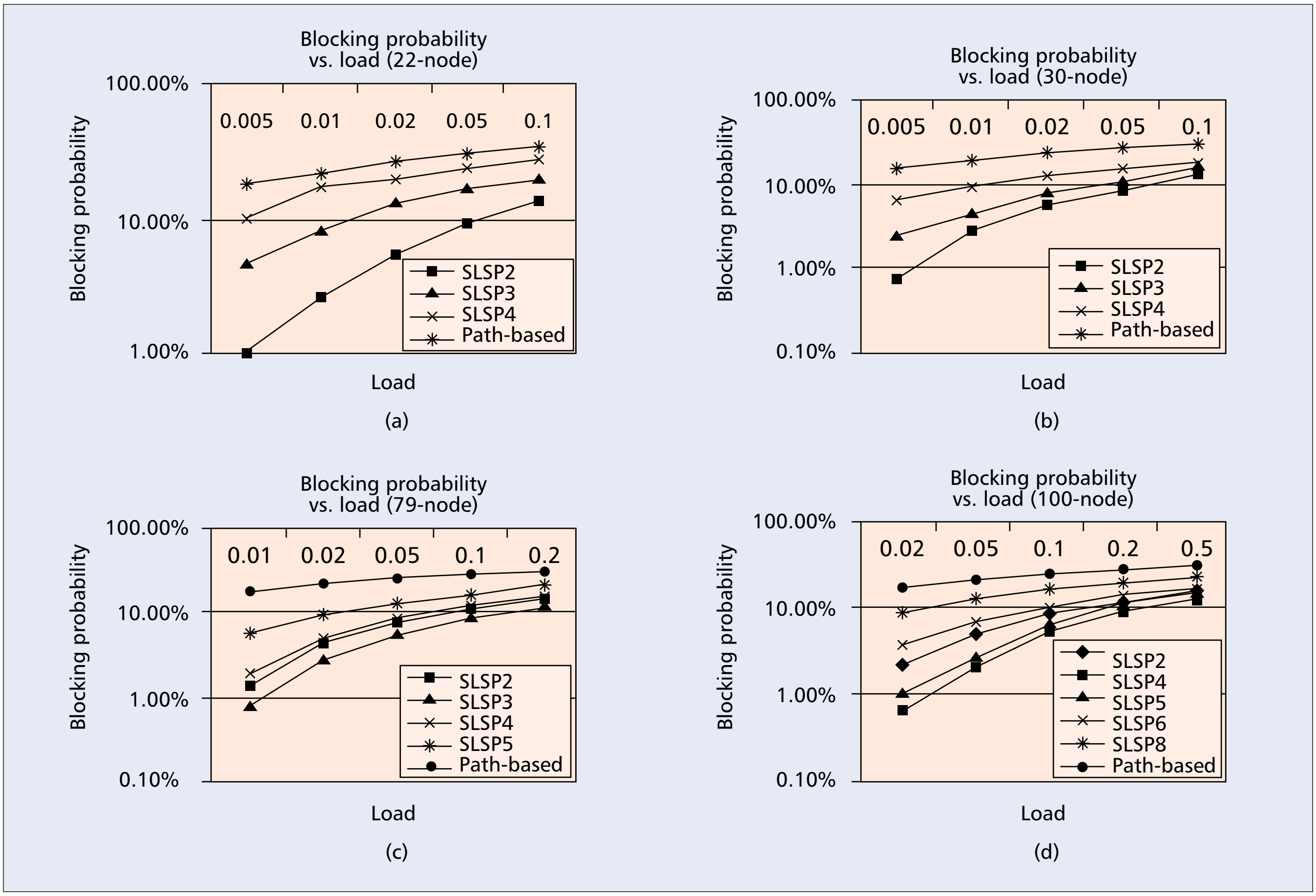


Figure 5. *Simulation results on SLSP for blocking probability with different traffic load and protection strategies.*

path. Blocking is counted if any connection request for a working lightpath with end-to-end protection cannot be established. After a lightpath is terminated, all the network resources reserved by the lightpath are released. In this simulation, each trial has 10,000 connection requests. Final data is derived by averaging results of four trials. We assume that every node has a traffic demand to all the other nodes with a random arrival and departure rate. The load of the kth S-D pair is defined as the ratio of λ_k over μ_k, where λ_k is the arrival rate and μ_k is the departure rate. Both λ_k and μ_k are random nonzero integers assigned to each S-D pair in the network.

Simulation Results

Figure 5 shows the simulation results in terms of probability of blocking. Path-based protection yields the worst efficiency, while SLSP with proper sizes of *P domain* can yield the best performance. The selection of the diameter of *P domains* determines the restoration time and capacity efficiency, which is policy-based and must follow the constraints stipulated in the service level agreement, such as the maximum allowable service interruption time. It is notable that SLSP2 outperforms most of the other schemes, especially for networks of smaller size, due to the fact that more resource sharing can be achieved. However, better sharing of network resources does not guarantee better performance all the time, since SLSP2 intrinsically requires more mileage of protection links than the other schemes, which impairs performance. The above observations explain why the best performance is given in the four networks with SLSP of different diameters, as shown in Table 1. The diameter of *P domains* determines the performance of networks of different sizes by trading off the effects of resource sharing and the mileage of protection links taken by a working path.

Conclusions

This article introduces the Short Leap Shared Protection (SLSP) framework for performing a services-guaranteed end-to-end shared protection in wavelength-routed WDM mesh networks. The control plane of future wavelength-routed optical networks needs online routing algorithms that can allocate working and protection paths dynamically without impairing scalability, class of service, or capacity efficiency. The SLSP framework satisfies these requirements by segmenting each working path into several equal-sized protection domains, which is committed to providing guaranteed restoration service and a distributed computation approach that can achieve a maximum extent of scalability. The simulation results show that the optimal capacity efficiency is derived by proper selection of the size of *P* *domains* according to network topology. We conclude that SLSP achieves 100 percent end-to-end restorability with better capacity efficiency than conventional shared protection schemes, and can contribute to optical network design efforts with improved scalability, efficiency, dynamicity, and class of service provisioning.

ACKNOWLEDGEMENT

The authors would like to thank John Doucette and the reviewers for valuable input in revising this article.

REFERENCES

[1] A. Doria, K. Sundell, and S. Shew, "Requirements for Adding Optical Switch Support to GSMP," Internet draft, draft-ietf-gsmp-reqs-00.txt, work in progress, July 2001.

[2] G. Ellinas, A. G. Hailemariam, and T. E. Stern, "Protection Cycles in Mesh WDM Networks," *IEEE JSAC*, vol. 18, no. 10, Oct. 2000.

[3] W. D. Grover and D. Stamatelakis, "Cycle-Oriented Distributed Preconfiguration: Ring-Like Speed with Mesh-like Capacity for Self-Planning Network Restoration," *Proc. IEEE Int'l. Conf. Commun.*, 1998, vol. 1, pp. 537–43.

[4] D. Stamatelakis and W. D. Grover, "IP Layer Restoration and Network Planning Based on Virtual Protection Cycles," *IEEE JSAC*, vol. 18, no. 10, Oct. 2000, pp. 1938–48.

[5] G. Ellinas, A. Gebreyesus and T. Stern, "Protection Cycles in Mesh WDM Networks," *IEEE JSAC*, vol. 18, no. 10, Oct. 2000, pp. 1924–36.

[6] J. Spath, "Resource Allocation for Dynamic Routing in WDM Networks," *Proc. SPIE*, vol. 4233, *OptiComm '00*, Dallas, TX, Oct. 2000, pp. 235–46.

[7] P. -H. Ho and H. T. Mouftah, "Issues on Diverse Routing for WDM Mesh Networks with Survivability," *Proc. 10th IEEE Int'l. Conf. Comp. Commun. Net.*, Phoenix, AZ, Oct. 2001, pp. 61–66.

[8] G. Mohan and Arun K. Somani, "Routing Dependable Connections with Specified Failure Restoration Guarantees in WDM Networks," *Proc. IEEE INFOCOM 2000*, vol. 3, pp. 1761–70, 2000.

[9] D. Papadimitriou *et al.*, "Inference of Shared Risk Link Groups," Internet draft, draft-many-inference-srlg-00.txt, work in progress, Feb. 2001.

[10] V. Sharma *et al.*, "Framework for MPLS-based Recovery," Internet draft, draft-ietf-mpls-recovery-frmwrk-03.txt, work in progress, July 2001.

BIOGRAPHIES

PIN-HAN HO (pinhan@ee.queensu.ca) received a B.Sc. and an M.Sc. in electrical engineering from National Taiwan University, Taipei, in 1993 and 1995, respectively; and an M.Sc. in electrical and computer engineering at Queen's University, Kingston, Ontario, Canada, in 2000. He is currently finishing his Ph.D. in electrical and computer engineering at Queen's University. He worked as a research/teaching assistant in the Department of Electrical and Computer Engineering, Queen's University (since January 2000).

HUSSEIN MOUFTAH [F] (mouftah@ee.queensu.ca) joined the ECE Department at Queen's University in 1979, where he is now a full professor and department associate head, after three years of industrial experience mainly at Bell Northern Research of Ottawa (now Nortel Networks). He served as editor-in-chief of IEEE *Communications Magazine* (1995–1997) and IEEE Communications Society Director of Magazines (1998–1999). He is author or coauthor of two books and more than 600 technical papers and 8 patents in the areas of broadband packet switching networks, mobile wireless networks, and quality of service over the optical Internet. He has received numerous IEEE and Professional Engineers awards.

From the network administrative perspective, SLSP provides a tradeoff between restoration time and the amount of protection resources consumed, with which the class of service can be achieved with finer granularity. The major disadvantage is the increase of signaling complexity.