An Efficient Mechanism for Dynamic Survivable Multicast Traffic Grooming

Xiaojun Yu, Gaoxi Xiao*, Tee Hiang Cheng

School of Electric and Electronic Engineering, Nanyang Technological University, Singapore, 639798

Abstract

Recent advances in wavelength division multiplexing (WDM) networks have helped enhance the popularity of multicasting services. However, as a single network failure may disrupt the information transmission to multiple end-users, protecting multicast requests against network failures becomes an important issue in network operation. This paper investigates the sub-wavelength level protection for dynamic multicast traffic grooming. A new method named Lightpath-Fragmentation based Segment Shared Protection (LF-SSP) scheme is proposed. By carefully splitting primary/backup lightpaths into segments to improve resource sharing for both traffic grooming and protection, LF-SSP aims to minimize the network resources allocated for request protection. Extensive simulations are carried out to compare the performance of LF-SSP to some existing approaches, on sub-wavelength-level as well as wavelength-level multicast protections in different cases. Results show that LF-SSP steadily outperforms these existing methods as long as the network resources are not too limited. Influences of the add/drop port resources and the average number of destinations per connection request on the LF-SSP performance are also evaluated.

Keywords: Dynamic traffic grooming; Multicast; Lightpath fragmentation; Segment shared protection.

*Corresponding author

Email addresses: `E070035@e.ntu.edu.sg` (Xiaojun Yu), `EGXXiao@ntu.edu.sg` (Gaoxi Xiao), `ETHCHENG@ntu.edu.sg` (Tee Hiang Cheng)

1. Introduction

The increasing bandwidth demands over the past decades have driven wavelength-division-multiplexing (WDM) networks to become the dominant infrastructure for backbone networks [1]. In such networks, data is transmitted through all-optical wavelength channels, referred to as *lightpaths* [2], using optical-cross-connects (OXCs). A lightpath may span several physical links. If all OXCs are not equipped with any wavelength converter, the lightpath has to be served using the same wavelength along its route, which is known as the *wavelength continuity constraint* [3].

Multicast involves the delivery of a message from a single source to a group of destinations simultaneously. As WDM networking technologies become mature, and bandwidth intensive multicast applications, such as interactive distant learning, high-definition-television (HDTV), live-video conferencing, etc., become increasingly popular, it is widely believed that a large portion of the future Internet traffic will be multicast in nature. To support the physical-layer multicasting, various methods utilizing either lightpath, or *light-tree* [4], or both have been proposed.

For many multicast sessions, the bandwidth they require is usually less than $OC-3(155Mb/s)$, which is much lower as compared to the capacity that can be provided by a single wavelength channel in today's WDM networks, e.g., $OC-192(10Gb/s)$. To efficiently utilize wavelength capacity, *traffic grooming* [5] is usually adopted to pack multiple sub-wavelength granularity requests into a single wavelength channel for transmission. Multicast traffic grooming has received considerable attention, and the early-stage work has been mainly focusing on the static problems, wherein the network resources and all the traffic demands are known a priori [5–7]. In recent years, however, as more and more agile components are developed and widely deployed in optical networks, multicast traffic tends to show its dynamic nature and consequently, dynamic multicast traffic grooming is becoming increasingly important. With the requests arriving and leaving the networks dynamically, studies on dynamic multicast traffic grooming problem mainly focus on algorithm design for minimizing request blocking probability or maximizing network throughput, e.g., [7–9].

Optical networks are vulnerable to various component failures, and a single failure may cause massive information losses and serious service interruptions. In networks supporting a large number of bandwidth-intensive multicast applications, influences of network failures could be even more devastating. Having proper survivability mechanisms to protect multicast sessions against network failures is therefore of essential importance. Generally speaking, the network survivability methods can be classified into two categories: *restoration* [10] and *protection* [11]. While restoration is reactive with efficient resource utilization, protection is proactive and recovers more quickly after the failures. In high-speed WDM backbone networks, protection is usually regarded as a more favorable option as it guarantees full recovery and faster restoration speed [12].

A number of multicast protection mechanisms have been proposed in literature [13–19]. According to whether backup resources can be shared or not, such protection mechanisms can be classified into *dedicated* or *shared* protections; while according to how the backup route is calculated, they can be classified into five categories [17]: *tree*-based, *ring*-based, *path*-based, *segment*-based, and *cycle*-based. Results in [18, 19] showed that the tree- and ring-based methods are not resource efficient, while the cycle-based ones are not flexible enough for dynamic request protection, especially for the dynamic multicast requests. Between the path-based and segmented-based schemes, the latter one is reported to achieve better blocking performance, faster restoration speed and higher resource efficiency in protecting wavelength-level multicast requests [19].

Compared to the extensive research efforts dedicated towards wavelength-level multicast request protection, sub-wavelength-level multicast request protection, which is also known as survivable multicast traffic grooming (SMTG), has received rather limited attention: though two methods, which will be reviewed in Section 2.3, have been proposed in [20] for SMTG, some assumptions adopted therein may not necessarily be valid in modern optical communication networks. Specifically, as pointed out in [18], in current backbone networks, the capacity reserved for protection within a fiber cannot be utilized in two opposite directions by simply reconfiguring the switches at its two end nodes. Therefore, we do not adopt such assumptions in our proposed scheme.

In this paper, we address the problem of protecting sub-wavelength-level multicast requests in dynamic traffic grooming process. A novel mechanism, named lightpath-fragmentation based segment shared protection (LF-SSP) scheme, is proposed to protect multicast requests at the connection level. The primary objective of the algorithm design is to protect requests against any single link failure while minimizing the network's bandwidth blocking ratio (BBR), which is defined as

$$BBR = \frac{\sum \text{Blocked request bandwidth}}{\sum \text{Bandwidth of all requests}}$$

By adopting the lightpath fragmentation (LF) method to fragment new lightpaths into shorter segments to improve resource sharing for both traffic grooming and request protection, the LF-SSP scheme attempts to minimize the network resources allocated to protect each request. To evaluate the performance of LF-SSP, extensive simulations are carried out. We firstly compare the LF-SSP scheme against an existing method for sub-wavelength-level multicast request protection, and then extend the comparison to a few existing methods for wavelength-level request protection. Simulation results demonstrate that LF-SSP outperforms the existing methods in different cases as long as the network resources are not too limited. In addition, the effects of a few factors, including the redundancy level of add/drop port resources and the average number of destinations per multicast session, are also evaluated.

The remainder of this paper is organized as follows. Section 2 defines the network model and the problem to be addressed, followed by a brief description of related work. Section 3 describes the proposed LF-SSP scheme for dynamic SMTG. The simulation results are presented and discussed in Section 4. Section 5 concludes the paper.

2. Network Model and Problem Definition

2.1. Network Model

We consider dynamic multicast traffic grooming problem in wavelength-routed WDM networks. The network is represented by a directed graph $G = (V, E)$, where V and E denote the sets of network nodes and fiber links, respectively. Specifically, we assume that the physical-layer topology of the network is a set of nodes interconnected by fiber links. Each fiber link is composed of two fibers in opposite directions, each of which carrying W wavelengths. The capacity of each wavelength is B units. Each network node is equipped with a grooming-capable optical cross-connect (GC-OXC) [7] as shown in Fig. 1. Each GC-OXC is equipped with a certain number of add/drop ports, which generally equals the number of transceiver pairs on the node. As both the add/drop ports and the transmitters/receivers are high-cost components, a network node is usually equipped with a limited number of ports shared by all wavelengths going through it. In this paper, we define the *add/drop ratio* r ($0 < r \leq 1$) as the ratio of the number of add/drop port pairs over the total number of wavelengths passing-through the OXC. We refer to a network node with $r < 1$ as a port-limited node; and a port-unlimited one otherwise.

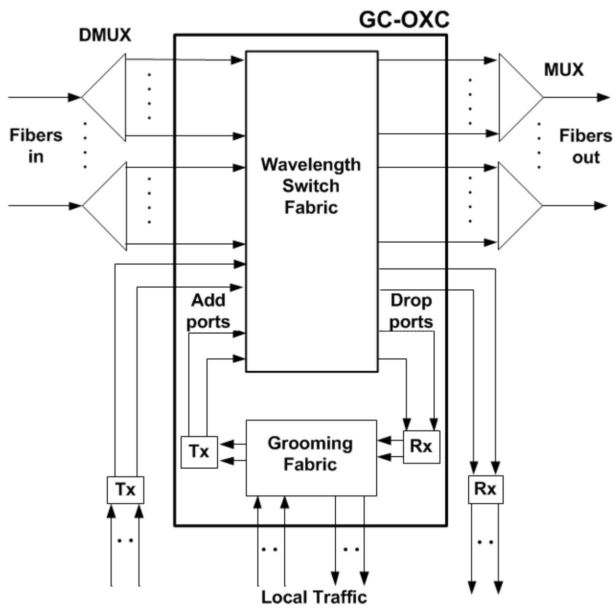

Figure 1: A typical grooming-capable OXC architecture.

To support multicasting services, a lightpath-based scheme is adopted in this paper: as demonstrated in our previous study [9], the lightpath-based approaches steadily outperform the light-tree based ones in achieving better bandwidth blocking performance for dynamic multicast traffic grooming. A lightpath occupies a wavelength along its route, a transmitter at its source node, and a receiver at its destination node, whereas a multicast request may traverse several lightpaths along its route, and consumes a portion of the bandwidth provided by each lightpath it traverses.

2.2. Problem Statement

The dynamic SMTG problem in WDM networks can be formulated as follows. Upon the arrival of each multicast request $R\{s, D, b\}$, where s, D and b denote the request source, specified destination set and required bandwidth respectively, the central network controller must identify both primary and backup routes for the request using accurate global information regarding the network state, so that the request can survive any single link failure. The primary objective of the algorithm design is to minimize the network BBR by improving resource sharing in both the traffic-grooming and request-protection processes.

We assume that all multicast requests arrive/leave the network dynamically with no prior information regarding future requests, and that a request is supported only when all its destinations can be served; otherwise the request will be blocked. All requests are protected at the connection level, i.e., the connection to each request destination shall pass through a certain number of *survivable* lightpaths. A lightpath is "survivable" if it is protected by a link-disjoint backup path, which may pass through one or multiple lightpaths with sufficient bandwidth reserved for backup purpose. The backup paths of different survivable lightpaths can share capacities if their primary paths are link-disjoint. Since it is shown in [21] that grooming primary and backup paths separately helps improve the network blocking performance, we adopt the same grooming mechanism in this paper. We refer to lightpaths that are utilized for working paths as *working lightpaths*, and those solely for request protection as *backup lightpaths*.

To be more precise, in this paper, we assume that each fiber link comprises two directional fibers in opposite directions and that a single link failure will sever the fibers in both directions. We also assume that an ongoing transmission cannot be interrupted until it is completed.

2.3. Related Existing Work

The problem of wavelength-level multicast request protection has been extensively studied, and various link-, path- and segment-based protection schemes have been proposed [13–19]. Among them, the segment-based protection schemes, as discussed in Section 1, are believed to achieve the best blocking performance for dynamic multicast request protection; hence, a segment-based protection scheme is considered in this paper.

The first segment-based protection method was proposed in [13]. By protecting each segment on the primary tree using a link-disjoint path from the segment source to its end node, the proposed segment-based method is able to protect a multicast session against any single link failure. By adopting a similar idea, a different segment-based mechanism known as the Segment-based Protection Tree (SPT) was proposed in [18]. With the SPT scheme, each primary tree is divided into tree-segments, each of which is then protected by a link-disjoint tree that connects the session source and all its destinations. The minimum-cost survivable topology, which takes into account the costs for both the primary and backup trees, is chosen to fulfill the connection request. It has been demonstrated that the SPT mechanism outperforms the best existing path-based method in certain cases.

More recently, another new segment-based protection method known as level-protection (LP) was proposed in [19]. Once a primary tree has been found, the LP scheme attempts to protect the session destinations one by one in an ascending order of their distances from the request source, with the objective of efficiently sharing resources on both the primary and backup trees. The LP scheme has been demonstrated to achieve superior performance with respect to the algorithms proposed in [14, 16].

To date, the problem of sub-wavelength-level dynamic SMTG has received limited attention. The authors of [20] have proposed the first two algorithms, namely Multicast Traffic Grooming with Segment Protection (MTG-SP) and Multicast Traffic Grooming with Shared Segment Protection (MTG-SSP) respectively, attempting to address this problem. As discussed in Section 1, however, as the assumptions adopted by these algorithms are not necessarily valid in modern optical network infrastructures, while the implementations of these methods strongly rely on these assumptions, we would not include these two methods for comparison in this paper.

In [22], we proposed a scheme known as connection-level segment shared protection (CL-SSP) scheme for SMTG. For each multicast request, CL-SSP attempts to protect it against any single link failure at the connection level. To improve resource sharing, CL-SSP adopts a simple method to fragment the new primary/backup lightpaths into shorter segments on those intermediate nodes with redundant transceiver resources. Our results indicated that such a simple approach, although very effective in fulfilling the multicast transmissions without protection [9], may not easily achieve satisfactory performance for dynamic SMTG. Among the several methods we investigated, the best performance was achieved by fragmenting only the backup paths. To further improve the network performances, better approaches for more effective lightpath fragmentation are needed.

In this paper, we propose a new LF-SSP method in which both working and backup lightpaths are carefully fragmented with the objective of minimizing network BBR. The BBR performance of the new method is compared against those of the best existing wavelength-level schemes including the SP-

T and LP methods, and that of the sub-wavelength level CL-SSP method in which only the backup lightpaths are fragmented. For simplicity, we henceforth refer to CL-SSP scheme with only backup path fragmentation simply as the CL-SSP method.

3. LF-SSP Mechanism for Survivable Dynamic Multicast Traffic Grooming

This section presents the proposed LF-SSP mechanism in detail. We first briefly describe the main idea of the segment shared protection (SSP) method for dynamic SMTG and then discuss the major steps of the proposed two-phase LF-SSP method. Finally, the detailed LF-SSP mechanism is presented.

3.1. Segment Shared Protection (SSP) Method

Segment shared protection is an efficient mechanism that has been utilized to support survivable unicast [21, 23, 24] and multicast transmissions [13, 18, 19]. For unicast services, the basic concept of SSP is to split the working path into a few segments and then protect each of them separately. It has been demonstrated in the literature that properly designed segment protection can achieve better blocking performance than path- or link-protection methods [21, 23, 24]. The example presented in Fig. 2 illustrates the higher resource sharing efficiency of the SSP scheme: when a path-protection scheme is adopted, as shown in Fig. 2(a), the backup-path capacity along the lightpath from s to d cannot be shared when serving the new request from s' to d', whereas when a segment-protection scheme is adopted, capacity sharing of the backup lightpaths is permitted, as shown in Fig. 2(b).

To support survivable multicast requests, SSP attempts to fragment a multicast tree into segments, e.g., a number of paths or smaller trees, and then protect each segment separately using a link-disjoint path. Meanwhile, to improve resource utilizations, the backup resources for different segments can be shared. Typically, there are two approaches for backup resource sharing: *self-sharing* and *cross-sharing* [25]. Self-sharing refers to the sharing of resources among backup routes within the same session, and cross-sharing refers to the sharing of backup resources among different sessions.

In this paper, both self- and cross-sharing are considered in the proposed SSP scheme. Specifically, to identify the sharing potential of the backup paths, each backup lightpath is associated with a link set A. Consider a backup lightpath e: its associated link set can be described as $A = \{a|a \in$

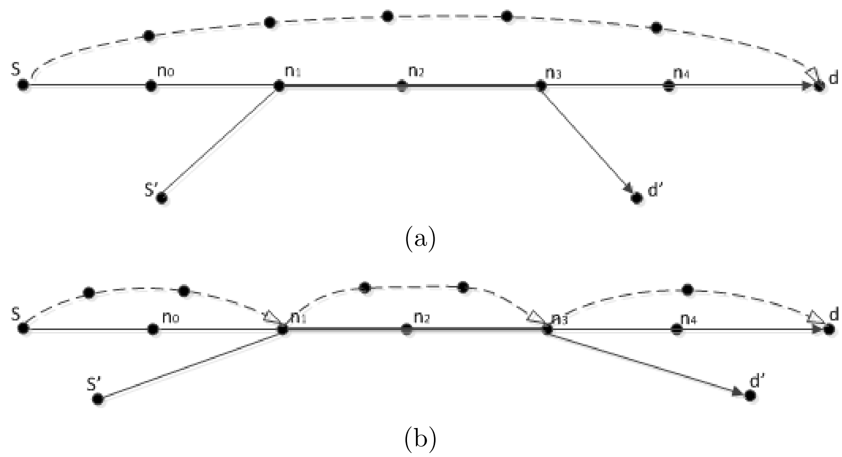

Figure 2: A comparison between the shared path protection and SSP against single link failure: (a) shared path protection; (b) SSP.

$E, 0 < b_e^a \leq B\}$, where b_e^a represents the amount of capacity that would be rerouted to e if its protected link a fails. Hence, the total amount of capacity that has been reserved for protection on e is $b_t = \max_{a \in A} b_e^a$, and its residual capacity is $r_m = B - b_t$. The capacity along e that can be shared by the backup path of any new primary lightpath l, which is link-disjoint to e, is $b_f^l(L) = b_t - \max_{a \in (L \cap A)} b_e^a$, where L denotes the set of physical links that l goes through. Note that $b_f^l(L)$ is non-negative.

The proposed SSP mechanism consists of two phases: the first phase is to establish a primary tree routing from the request source to all its destinations using the existing survivable lightpaths as much as possible, and setting up new primary lightpaths only when such is necessary; the second phase is to protect each new primary lightpath, if any, against any single link failure using SSP scheme. As we have previously demonstrated in [22], properly fragmenting new primary/backup lightpaths into shorter ones helps improve network BBR performance, a lightpath-fragmentation (LF) method is adopted in the proposed SSP method to conservatively split new lightpaths into shorter ones. In this manner, the SSP scheme attempts to minimize the total amount of network resources allocated for routing and protecting each request

Below we present the detailed two-phase SSP scheme for dynamic SMTG.

3.2. Two-Phase SSP Scheme for Dynamic SMTG

(i) First-phase Primary Tree Route Calculation

As aforementioned, since establishing new lightpaths consumes additional wavelength and transceiver resources, we use the existing survivable lightpaths to serve as many request destinations as possible, and new lightpaths are established to serve the remaining destinations only when such is necessary.

It is well known that identifying the minimal-cost primary tree route is an NP-complete problem. We adopt the simple yet efficient minimum cost path heuristic (MPH) [26] to connect the request destinations one by one to the primary tree. Procedure I presents the process for calculating the primary route T for a multicast request.

Procedure I: Primary_Route_Calculation_sub_Algorithm

input : A network $G(V, E)$ and a multicast request $R\{s, D, b\}$.
output: A primary tree route T for serving $R\{s, D, b\}$.

1 Generate an auxiliary graph (AG) using all the existing survivable lightpaths; Call **MPH** on AG to initiate a tree from s to as many members of D as possible. Remove those served members from D. If D is empty, go to Step 12; otherwise, save the partial tree T, and continue. //*Grooming with existing survivable lightpaths*
2 Add s and all the other nodes on T to a node set S; //*optical layer primary tree routing (2-11)*
3 **while** $D \neq \Phi$ **do**
4   Generate an optical-layer AG; calculate all-to-all shortest paths between each node in S to each node in D by adopting a certain lightpath cost definition;
5   Choose the shortest path among all paths that connecting any member of S to any member of D. If there is a tie, break it randomly. Denote the selected path as P, the end node of P in D as d, and the length of P as dis.
6   **if** $dis < \infty$ **then**
7         $S = S \cup \{d\}$; $D = D \backslash d$; save the path P onto the primary tree T;
8   **else**
9   Block the request $R\{s, D, b\}$ and break;
10   **end**
11 **end**
12 Return the primary tree route T.

Step 1 attempts to utilize the existing survivable lightpaths to serve as many request destinations as possible. If there are sufficient existing survivable lightpaths, the request will be served directly; otherwise, the remaining destinations will be connected to the primary tree one by one using new lightpaths as shown in Steps $2 - 11$.

Note that various path cost definitions can be adopted in Step 4 to define the distance between two nodes. To improve the network's BBR performance while balancing the resource consumptions, the cost definition shown below is adopted [9],

$$C_{ij} = \begin{cases} \frac{1-r}{p\times r\times(\overline{H}+1)} - H_{ij}\ln\left(1-\frac{1}{\omega_{ij}+1}\right) & \text{if } \omega_{ij}>0 \text{ and } p>0 \\ \infty & \text{if } \omega_{ij}=0 \text{ or } p=0 \end{cases} \tag{1}$$

where p is the smaller one among the number of transmitters on the source node and the number of receivers on the destination node of the lightpath, ω_{ij} is the number of wavelengths available along the lightpath route, $\overline{H}$ is the average path length of the network, and H_{ij} is the minimum hop length between the two end-nodes of the lightpath. The intent of this function is to balance the consumptions of wavelength and transceiver resources. Specifically, if both resources are abundant, the costs of consuming them will be low and not so different from each other; whereas if either becomes scarce, the cost of consuming the scarce resource will be increased. Our previous studies demonstrated that such a definition steadily leads to satisfactory performance [9].

(ii) Second-Phase LF-Based SSP

Once the primary tree route is identified for a request in the first phase, the proposed method enters its second phase to identify a backup route for each new primary lightpath, wherein auxiliary graphs are generated for routing purpose.

3.2.1. Graph Generation for Backup-Route Calculation

For each new lightpath added into the primary tree route T, the SSP scheme is adopted to protect it at the connection level. Specifically, a new lightpath is usually fragmented into segments, which we refer to as *active segments* (ASs) following [23], and each segment is protected using one or more link-disjoint *backup segments* (BSs). For example, the new primary lightpath shown in Fig. 2(b) is fragmented into three ASs, i.e., $S \rightarrow n_1$, $n_1 \rightarrow n_3$, and $n_3 \rightarrow d$, and each AS is protected by a separate link-disjoint BS. The nodes n_1 and n_3, each of which acting as the source node of a segment, are called *switching nodes*.

To identify backup routes for a multicast session $R\{s, D, b\}$, a complete auxiliary graph with appropriate edge costs is generated. In such a graph, an edge represents either an existing backup lightpath that has been established or a new lightpath to be established between two network nodes. Suppose that P is a new primary lightpath to be protected, AS is an active segment of P, and SG is the set of links that AS traverses. The link-cost assignment policy below is adopted for the calculation of AS's backup route:

$$L_{ij} = \begin{cases} \infty & \text{a backup lightpath } e \text{ that is link-disjoint to AS cannot be found between node } i \text{ and } j; \\ \varepsilon + b_{ad} & \text{an existing backup lightpath } e \text{ that is link-disjoint to AS has a capacity } r_m + b_f^{AS}(SG) > b; \\ b \times C(e) & \text{a new backup lightpath that is link-disjoint to AS needs to be set up.} \end{cases} \tag{2}$$

where ε is a small positive value (10^{-2} used in the paper) and b_{ad} is is the amount of additional capacity that should be reserved on the existing backup lightpath for AS protection. It can be calculated as $b_{ad} = \max\Big(0, b - b_f^{AS}(SG)\Big)$.

As indicated in Eq. (2), for those existing backup lightpaths that have enough residual capacities, their costs approximately equal the additional capacity that has to be reserved for the request protection; while for new backup lightpaths to be established, their costs equal the request bandwidth times parameter $C(e)$, which is defined as follows:

$$C(e) = \begin{cases} \left(\frac{(1-r)}{p \times r(\overline{H}+1)} - H_e \ln\left(1 - \frac{1}{\omega_e + 1}\right)\right) \times amp & \text{if } \omega_e > 0 \text{ and } p > 0 \\ \infty & \text{if } \omega_e = 0 \text{ or } p = 0 \end{cases} \tag{3}$$

where all symbols have the same meanings as those defined in Eq. (1), and amp is an amplification factor. This definition ensures that the typical cost for establishing a new backup lightpath, i.e., $C(e)$, is approximately 5 times as much as that of using an existing lightpath (The cost of using an existing lightpath is 1 by default.) when the network is in its typical operation status [28]. (In this paper, we assume that $\omega_e = W/2$ for the typical network status. A detailed discussion on this assumption may refer to [27].).

Once the auxiliary graph is generated, any shortest-path algorithm can be applied to identify a backup route for each primary path. However, since long lightpaths may impose a strict wavelength continuity constraint on the lightpath routing, thereby degrading resource sharing in the grooming process, an LF method is adopted in the proposed SSP mechanism for both AS determination and BS fragmentation.

Below, we briefly review the LF method proposed in [22], pointing out its limitation in network protection scenarios, and finally propose an improved LF-based method for SMTG.

3.2.2. *Greedy LF Method for AS Determination and BS Fragmentation [22]*

Suppose that L is a primary/backup route along which a new wavelength should be reserved; n is an intermediate node of L with a fan-out degree of d_n. The numbers of free transmitters and receivers on n are denoted by T_n and R_n respectively, and the numbers of free wavelengths along the incoming and outgoing links of n are denoted by ω_{in} and ω_{out} respectively. The three parameters defined as below are used to determine whether the path L should be segmented at n:

$$\alpha_m = \min\left(\frac{T_n}{d_n \times \omega_{out}}, \frac{R_n}{d_n \times \omega_{in}}\right), \tag{4}$$

$$\alpha_n^p = \frac{1}{H_n^p}, \tag{5}$$

$$\alpha_n^b = \frac{1}{H_n^b}, \tag{6}$$

where H_n^p and H_n^b are two topology-dependent constants denoting the average shortest primary and backup path lengths from n to all other network nodes, respectively. Specifically, with a given network topology, H_n^p is averaged over all the shortest primary lightpaths from n to each of the other network nodes, and H_n^b is averaged over all the corresponding shortest backup lightpaths.

In the above equations, α_m denotes the smaller one of the add and drop ratios on node n for the current network status; α_n^p and α_n^b are inversely proportional to the average primary and backup lightpath lengths from n to all the other network nodes respectively. The comparison between α_m and α_n^p or α_n^b helps indicate the relative availability of the port resources at node n for lightpath fragmentation under the current network status. When $\alpha_m > \alpha_n^p$ in a primary lightpath ($\alpha_m > \alpha_n^b$ in a backup lightpath), it indicates that the transceiver resources at n are relatively redundant and it may be beneficial to segment L at n to avoid establishing too long lightpaths, and thereby alleviates the wavelength continuity constraint on L's establishment; otherwise, the transceiver resources are regarded as relatively limited on node n, and it is better for L to bypass n to conserve transceiver resources.

We refer to a node n as a *fragment node* if $\alpha_m > \alpha_n^p$ for a primary lightpath or $\alpha_m > \alpha_n^b$ for a backup path that passes through n. Procedure II presents the major steps of the LF method.

A naive approach to apply the LF method is to adopt a greedy approach which segments a lightpath on a node whenever the transceiver resources

Procedure II: Lightpath_fragmentation_scheme(LF)

input : A network $G(V, E)$, a lightpath L

output: A set of new lightpaths.

while *(any node of L has not been checked)* **do**

  for *each intermediate node (if any) n along L* **do**

    Calculate α_m for n ;

    if *$\alpha_m > \alpha_n^p$ for the primary path (or $\alpha_m > \alpha_n^b$ for the backup path) going through n* **then**

      Fragment L at n, and obtain two new lightpaths L_a and L_b;

      $L = L_b$;

    end

  end

end

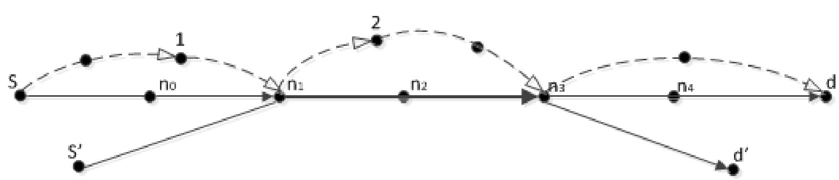

Figure 3: LF method adopted for primary path protection.

on this node are relatively redundant. An example is illustrated in Fig. 3, where a survivable lightpath is fragmented on nodes n_1, n_3, 1, and 2. Though such an approach helps alleviate the wavelength continuity constraint and achieve satisfactory performance in optical networks without protection, our previous results demonstrated that it may actually degrade the network BBR performance in SMTG [22]: protecting a large number of ASs requires a large amount of protection resources.

Inspired by such observation, we propose to apply the LF method conservatively for lightpath protection within the proposed SSP scheme. Specifically, Specifically, we develop a lightpath segmentation process similar to that applied in the PROMISE method in [23], with the objective of minimizing the network resources allocated for protecting each request.

3.2.3. Improved LF method for dynamic SMTG

After the first-phase route provisioning, we have obtained a primary tree that may contain some new primary lightpaths. The task now is to find the best fragmentation of these new primary lightpaths so that the resources allocated for protecting them are minimized. Denote a new lightpath as P, the number of optical hops that P traverses as h, and label the nodes along P from 0 to h. Assume that m ($0 < m < h$) is an intermediate node on P, AS_m is a candidate active segment from node m to node h along P, C_m is the shortest link-disjoint backup path that can protect AS_m, and $C_{m,i}$ is the shortest backup path that has been identified for protecting the active segment between node m and node i ($i < m < h$). Denote the costs of the latter two paths as $C(m)$ and $C(m, i)$, respectively. Note that they are the sums of the costs of all backup lightpaths that C_m and $C_{m,i}$ have traversed respectively. By adopting a similar main idea as that of the PROMISE method, Procedure III presents the major steps of the improved LF-method for backup-route calculation.

Procedure III begins by testing each node along the primary lightpath P, in a backward direction starting from the node adjacent to the end node h, to find all the candidate segment points where $\alpha_m > \alpha_m^p$ in Step 3. For each identified candidate fragment node (denoted as m), the corresponding minimum-cost link-disjoint backup path between nodes m and h is calculated in Steps 4-6. Steps 7-13 recursively test all the candidate fragment nodes between m and h, if any, with the objective of finding the minimum-cost segment protection path between m and h. Finally, when the testing on the primary lightpath nodes reaches the starting node 0, the minimum-cost segment protection path for the new primary lightpath is found. Note that the backup route BS may contain both existing backup lightpaths and new ones to be established. We adopt a simple policy that a new backup lightpath is segmented on all the candidate fragment nodes where $\alpha_m > \alpha_n^b$. Our simulation results show that such a simple approach steadily leads to satisfactory performance. In other words, good performance is achieved when we adopt conservative segmentation on the primary lightpaths yet greedy segmentation on the backup lightpaths.

It is easy to see that for a new lightpath with h candidate segment nodes, the number of BSs that we need to calculate is limited to $h(h+1)/2$. Here we count the starting node of the lightpath also as a candidate segment node.

Finally, we compare the complexity of LF-SSP to those of the existing wavelength- and subwavelength-level methods. For an arriving request with destination size D, all these methods firstly find a minimum spanning primary tree (MST) with a complexity of $O(D|V|^2)$, where $|V|$ is the number of network nodes. SPT method then protects each segment of such MST using a link-disjoint tree, its complexity hence is $O(D|V|^3)$; LP protects the request

Procedure III: LF_based_Backup_Path_Provisioning

input : A network $G(V, E)$, and new primary lightpath P for $R\{s, D, b\}$.
output: A set of backup lightpaths to protect P.

Clear the fragment node set S_F;
for *each intermediate node* $m = h - 1$ *to* 0 *along* P **do**
  if m *is fragment node with* $\alpha_m > \alpha_m^p$ **then**
    Set the links from m to h along P to be AS_m ;
    Generate an auxiliary graph (AG) for backup path routing according to Eq. (2); *//Graph generation for backup routing*
    Calculate the shortest path that is link-disjoint to AS_m on AG for its protection; denote its cost as $C(m)$, and record such path as C_m; *//C_m initialization*
    for *each node* i *in* S_F **do**
      Set AS to be the links from m to i along P ;
      Generate another new auxiliary graph (AG') according to Eq. (2); *//graph generation for AS protection*
      Calculate the shortest path that is link-disjoint to AS from m to i on AG' to protect AS, and denote this path by BS; *//backup routing*
      Call Procedure II (Lightpath Fragment scheme) to process each new backup lightpath along BS and return a set of new lightpaths, calculate the cost $C(m, i)$ using Eq. (2); record the processed BS route as $C_{m,i}$; *//LF for backup route processing;*
      Choose the backup route with smaller cost for AS_m protection: $C_m = \min(C_m, C_{m,i} + C_i)$; *//choose the back route for AS_m*
    end
    $S_F = S_F \cup \{m\}$
  end
end
Return C_0 for protecting the new lightpath P.

destinations on the MST one by one in an ascending order of their distances from the source, with a complexity of $O(D^2|V|^2)$. CL-SSP protects each new lightpath on the MST using a link-disjoint path its complexity therefore is $O(D|V|^2 + D(|E| + |V|\log(|V|)))$ with $|E|$ being the number of network links. For the LF-SSP method, since it adopts Procedure III to minimize the resources for both request grooming and protection, its complexity is $O(D|V|^2) + D^2(|E| + |V|\log(|V|))$ in the worst case. In a backbone network with a moderate number of network nodes, the complexity of LF-SSP is acceptable.

Using the primary- and backup-route provisioning sub-algorithms described above, we now present the proposed LF-SSP mechanism for SMTG.

3.3. The Proposed LF-SSP Mechanism

Algorithm I presents the major steps of the proposed LF-SSP mechanism.

To encourage traffic grooming when fulfilling a request, LF-SSP gives higher priority to the use of existing survivable lightpaths. Hence, Step 1 attempts to identify a primary route T_P for the request, and if a tree route that comprises only existing survivable lightpaths exists, it will be adopted to directly fulfill the request; otherwise, new lightpaths must be established for the request. Steps $2 - 5$ attempts to protect each new primary lightpath on T_P using the LF-based backup-path calculation sub-algorithm to minimize the amount of backup resources allocated for each lightpath; if a backup route cannot be found for any primary lightpath, the request will be rejected. Steps $6 - 20$ allocate the required network resources for a survivable lightpath, and finally Step 21 updates the network status. Note that for both the traffic grooming in Step 1 and the lightpath wavelength assignment in Steps $6 - 20$, the first-fit wavelength-assignment policy is adopted if there is more than one candidate route.

4. Performance Evaluation

In this section, we conduct a number of simulations to evaluate the performance of the LF-SSP mechanism in different cases. We first present the simulation setup and then compare LF-SSP method against a few existing approaches for sub-wavelength- and wavelength-level multicast request protection; finally, we assess the influences of a few factors on LF-SSP performance.

Algorithm I: LF-SSP for dynamic multicast traffic grooming

input : A network $G(V, E)$ and a multicast request $R\{s, D, b\}$.
output: A survivable multicast tree route for $R\{s, D, b\}$.

1 Call Primary_Route_Calculation_sub_Algorithm, which returns a primary route T_P; if T_P consists only of existing survivable lightpaths, go to Step 21 and otherwise, continue;
2 **for** *each new lightpath* P *on* T_P **do**
3   Call LF_based_Backup_Path_Provisioning for P protection;
4   If backup paths (BSs) can be found for P, assign the BSs to P and denote P as survivable on T_P; otherwise, block the request;
5 **end**
6 **for** *each new primary lightpath* P *on* T_P **do**
7   Fragment P according to its BSs; allocate transceiver and wavelength resources to each fragmented new AS of P; if any resource is unavailable, block the request;
8   **for** *each new backup lightpath along the BSs* **do**
9   Call Procedure II to fragment the lightpath, if possible;
10   **for** *each new lightpath* L *obtained from fragmentation* **do**
11   Reserve a wavelength along its route;
12   **if** *source node of* L *is neither* s *nor a fragment node on* P **then**
13   Allocate a transmitter at this node;
14   **end**
15   **if** *end node of* L *does not belong to* D *or is not a fragment node on* P **then**
16   Allocate a receiver at this end node;
17   **end**
18   **end**
19   **end**
20 **end**
21 Update the residual capacities of all survivable lightpaths along route T_P.

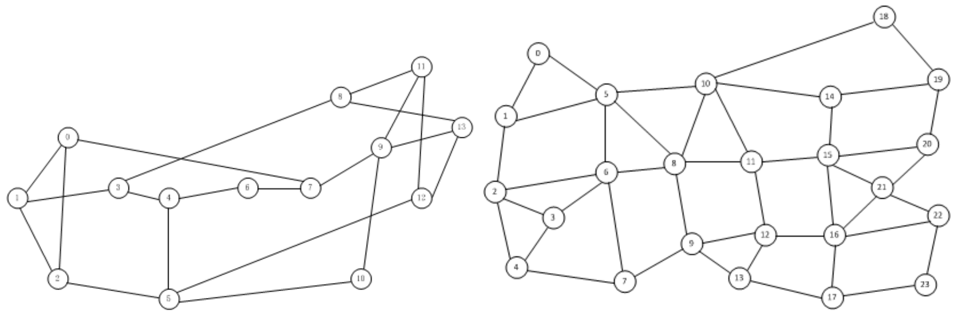

Figure 4: Two network topologies utilized for simulations. (a) 14-node 21-link NSFnet topology and, (b) 24-node 43-link USnet topology.

4.1. Simulation Setup

We simulate a dynamic network environment to evaluate LF-SSP performance in different cases. We assume that all requests arrive/leave the network dynamically according to a Poisson distribution with mean rate λ and that their holding time is negative exponentially distributed with a mean $\mu = 1$; the request source and destinations are randomly chosen among all network nodes, and the number of destinations of each request, denoted by N, follows a truncated geometric distribution [8] with a parameter $q(0 < q < 1)$. Specifically, the probability that a request has k destinations, and the mean number of the request destinations are given by Eq. (7) and Eq. (8), respectively,

$$P(N = k) = \frac{(1-q)q^{k-1}}{q - q^{|V|}}, 2 \leq k \leq |V| - 1 \tag{7}$$

$$\begin{aligned} E(N) &= \sum_{k=2}^{|V|-1} k \times P(N = k) \\ &= \frac{2q - q^2 - |V|\, q^{|V|-1} + (|V| - 1)q^{|V|}}{(1-q)(q - q^{|V|-1})} \end{aligned} \tag{8}$$

where $|V|$ is the number of network nodes.

Two commonly used network topologies as shown in Fig. 4 are utilized for simulation, which are 14-node, 21-link NSFnet and 24-node, 43-link USnet. We assume that

1. Each network link consists of two fibers travelling in opposite directions, each carrying $W = 32$ wavelengths; the full capacity of each wavelength is $B = 16$ units; *amp* is set to be 40 and 25 for NSFnet and USnet, respectively;
2. The average number of destinations of each session is 3. For sub-wavelength requests, the required bandwidth is an integer uniformly distributed in the interval $[1, 16]$, whereas for wavelength-level multicast requests, their required bandwidth is 16 units.
3. The number of transceivers on a network node is $W \times d_i \times r$, where d_i is the fan-out degree of the node;
4. Loss of signal power due to transmission attenuation or light-splitting is not considered.

Results in the following figures are averages of at least five independent simulations, each of which simulating at least 10^5 requests. Since the two topologies generate relatively consistent performance results, unless otherwise specified, we present only the results obtained using the NSFnet topology for comparisons and discussions.

4.2. Comparison of LF-SSP to the Existing Sub-wavelength Level CL-SSP Method

4.2.1. Comparisons in port-unlimited network

Figure 5 compares the LF-SSP method to the existing CL-SSP method in a port-unlimited network under various traffic loads for sub-wavelength-level multicast request protection. It is evident that LF-SSP consistently outperforms CL-SSP throughout the entire range of traffic loads: under low traffic loads, e.g., $\rho = 65$ Erlangs, LF-SSP is superior to CL-SSP by more than three orders of magnitude, whereas under higher traffic loads, e.g., $\rho = 110$ Erlangs, LF-SSP remains superior to CL-SSP by approximately 49.1% in terms of the network BBR.

4.2.2. Comparisons in port-limited network

Figure 6 presents a comparison between LF-SSP and CL-SSP in a port-limited network, where $r = 0.6$ for all network nodes, under various traffic loads. The results illustrate that LF-SSP again reliably outperforms CL-SSP throughout the entire range of traffic loads in the request grooming process. Specifically, when the traffic load is low, e.g., $\rho = 60$ Erlangs, LF-SSP is

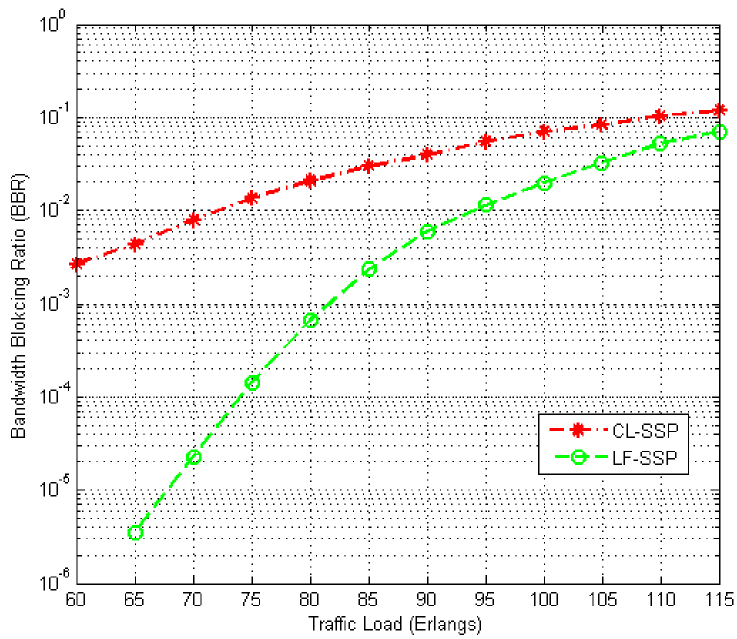

Figure 5: LF-SSP compared to CL-SSP in the port-unlimited NSFnet topology under various traffic loads ($r = 1.0$).

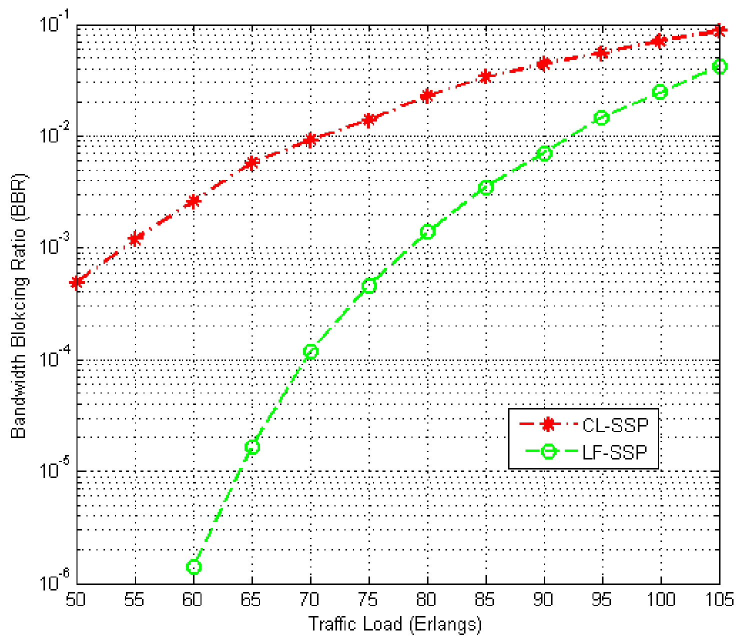

Figure 6: LF-SSP compared to CL-SSP in the port-limited NSFnet topology under various traffic loads ($r = 0.6$).

superior by more than three orders of magnitude, whereas under higher traffic loads, e.g., $\rho = 100$ Erlangs, it outperforms CL-SPP by approximately 65.2%.

The results presented above in both Fig. 5 and Fig. 6 convincingly demonstrate that LF-SSP is able to achieve satisfactory performances in networks with either limited or unlimited port resources under different traffic loads. Such observation is due to the fact that, compared to CL-SSP, LF-SSP utilizes the LF method more conservatively in splitting new primary lightpaths in order to minimize the total resources allocated for routing and protecting a new request, and hence allowing more efficiently utilization of network resources.

To evaluate the resource utilization of LF-SSP, we define a new metric, the average utilization of existing lightpath channel capacity, which is defined as the ratio of the total traffic loads carried by the network to the total capacities of all the existing channels. Figure 7 presents the values of this metric for both methods in the port-limited NSFnet topology under various traffic loads. It is evident that the greedy segmentation of primary lightpaths in CL-SSP leads to lower wavelength utilization. The LF-SSP method, by using the LF method more carefully, improves the channel capacity utilization by approximately 15% on average. Such improvements justify the extra computations needed by the segment protection calculations in Procedure III.

4.3. Comparison of LF-SSP versus the Existing Wavelength-Level SPT and LP Methods

Since there exist rather limited existing results for SMTG, to further assess the performance of the LF-SSP method, we have to extend its applications to the protection of wavelength-level multicast request protection (though it was not designed for such applications), and compare its performance versus those of the two best existing methods, namely SPT and LP, in various cases.

4.3.1. Comparisons in port-unlimited network

Figure 8 compares LF-SSP to SPT and LP in the port-unlimited NSFnet topology under various traffic loads. It is evident that LF-SSP consistently outperforms both SPT and LP methods throughout the entire range of traffic loads. Specifically, when under low traffic loads, i.e., $\rho < 45$ Erlangs, LF-SSP outperforms LP by approximately one order of magnitude, and outperforms SPT by about 83.6%; whereas when under higher traffic loads, e.g., $\rho = 70$

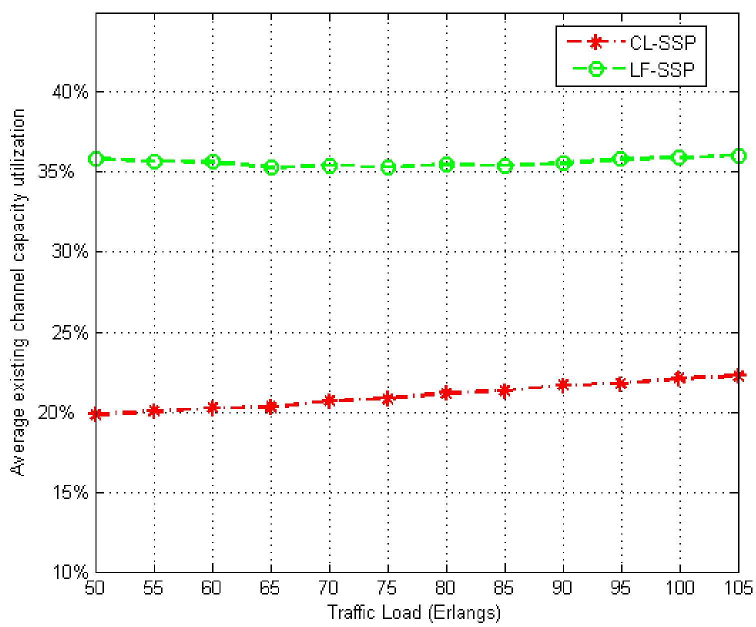

Figure 7: The average utilization of existing channel capacity versus the traffic load in the port-limited NSFnet topology ($r = 0.6$).

Erlangs, the performances of LF-SSP is still slightly better than those two methods. Such results can be understood: when the traffic load is low, the network resources are relatively abundant, and thereby, the method that is able to make more efficient usage of network resources can easily stand out; when the traffic load is high, however, the wavelength resources are rather limited, and consequently the differences between the performances of different methods become less significant.

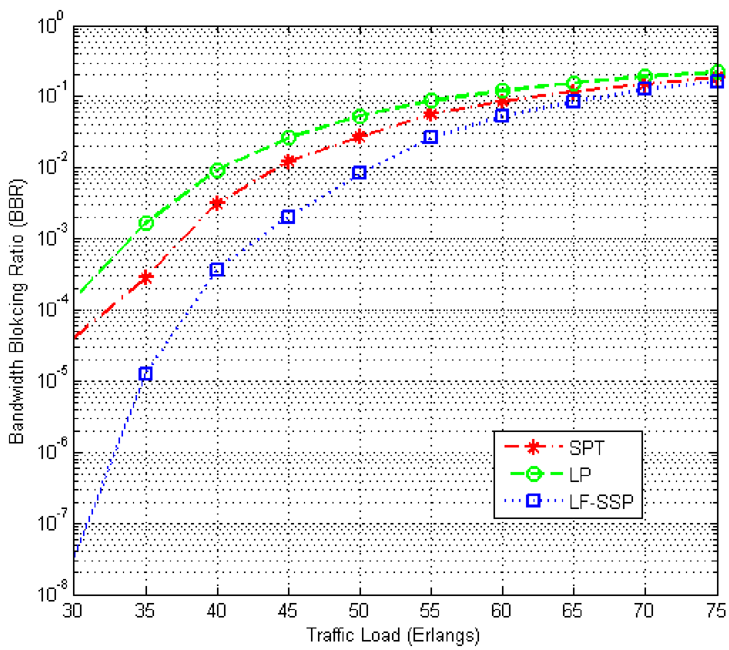

Figure 8: LF-SSP compared to the SPT and LP methods in the port-unlimited NSFnet topology under various traffic loads ($r = 1.0$).

4.3.2. Comparisons in port-limited network

Figure 9 compares LF-SSP against both SPT and LP in the port-limited NSFnet topology under various traffic loads. Again we can see that, LF-SSP evidently achieves better performance than both algorithms throughout the entire range of traffic loads: when under low traffic loads, e.g., $\rho = 45$ Erlangs, it outperforms LP by more than one order of magnitude, and outperforms SPT by more than 80%; whereas when under higher traffic loads, e.g. $\rho = 70$ Erlangs, performance of LF-SSP is still slightly better than those of SPT and LP methods. Such observation is due to the fact that when the traffic load is low, the network resources are relatively abundant, and thus LF-SSP is able to fragment the new lightpaths to improve resource sharing in protection process; whereas when the traffic load is high, both the wavelength and transceiver resources become exhausted, which cause connection requests to be blocked even under best utilizations. Consequently the performance superiority of the LF-SSP method becomes less significant.

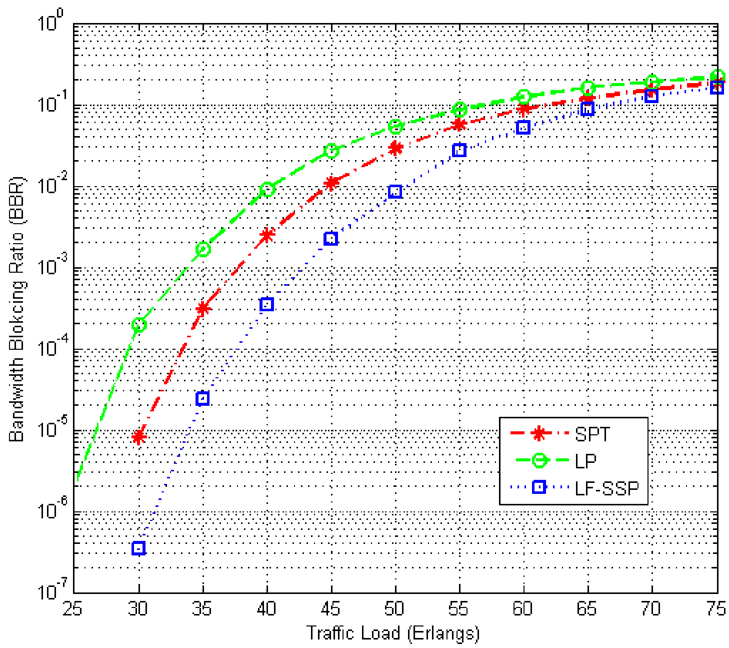

Figure 9: LF-SSP compared to the SPT and LP methods in the port-limited NSFnet topology under various traffic loads ($r = 0.6$).

The results in Fig. 8 and Fig. 9 illustrate that LF-SSP is able to achieve satisfactory performance even when it is used to protect wavelength-level multicast requests. It is also interesting to note that a comparison between Fig. 8 and Fig. 9 indicates that LF-SSP performs better when the port resources are more abundant. This finding can be attributed to the fact that LF-SSP is designed to make efficient utilization of transceiver resources to minimize the network BBR.

Below, by comparing LF-SSP with a few existing methods in various cases, we assess the effects of a few factors on the LF-SSP performance.

4.4. *Effects of the Add/drop Port Resources on Sub-wavelength and Wavelength Level Protection*

Figure 10 illustrates a comparison between LF-SSP and CL-SSP in the NSFnet network with various port resources for SMTG. We see that, when the port resources are too limited, i.e., $r < 0.2$, the performance differences between the two methods are not so big, whereas when the port resources increase to allow $r > 0.3$, the performance of LF-SSP improves rapidly and exceeds that of CL-SSP by more than one order of magnitude. When the port resources become relatively abundant, e.g., $r > 0.7$, LF-SSP outperforms CL-SSP by nearly two orders of magnitude.

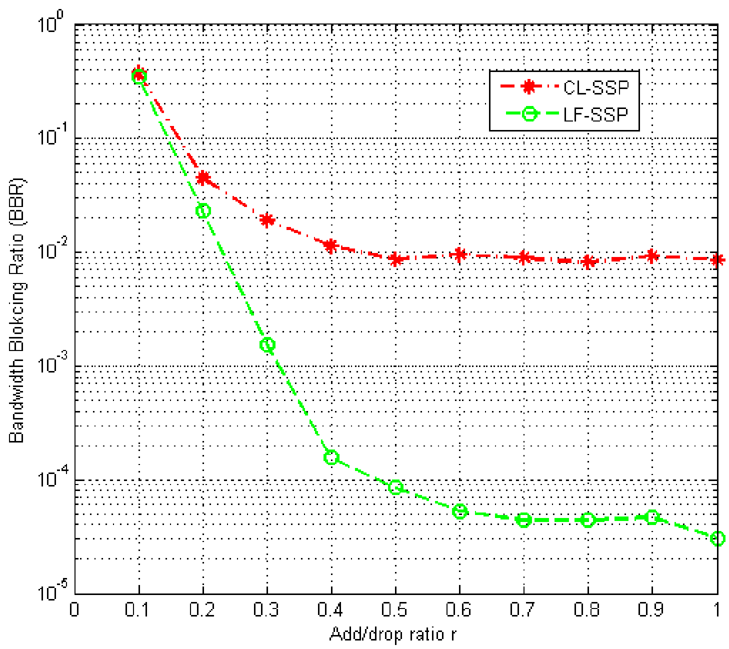

Figure 10: Comparison between LF-SSP and CL-SSP in terms of the add/drop ratio in the NSFnet topology for sub-wavelength-level request protection (traffic load $\rho = 70$ Erlangs).

Figure 11 compares LF-SSP to SPT and LP for protection of wavelength-level multicast requests in NSFnet network with different add/drop resources. It is again clear that, when the port resources are limited, i.e., $r < 0.35$, the BBR performances of these methods are not very different from one another. Whereas when the port resources are not so bottlenecked, e.g., $r > 0.35$, the

BBR performance of LF-SSP improves and supersedes those of SPT and LP; when $r > 0.5$, LF-SSP is superior to LP by nearly two orders of magnitude, and outperforms SPT by approximately one order of magnitude.

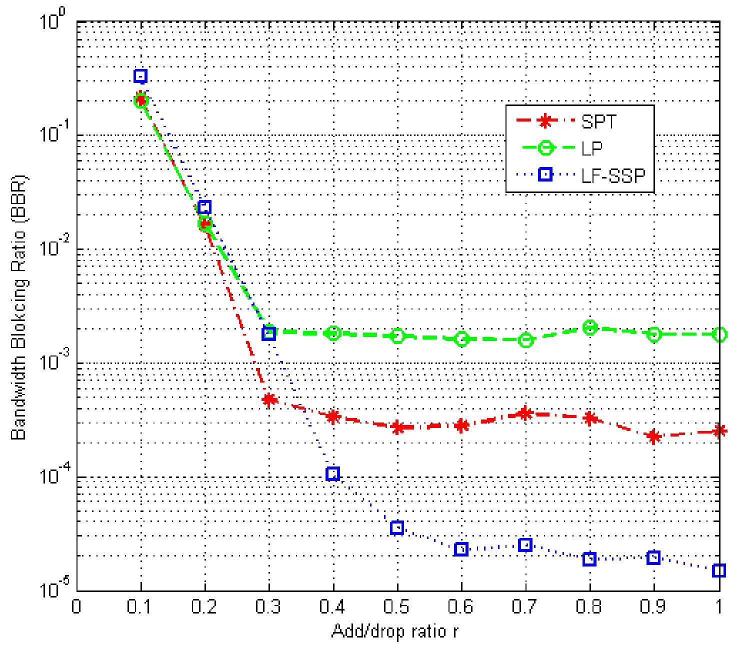

Figure 11: LF-SSP compared to the SPT and LP methods in terms of the add/drop ratio in the NSFnet topology for wavelength-level multicast request protection (traffic load $\rho = 35$ Erlangs).

Such comparisons clearly demonstrate that by utilizing the LF method to minimize the amount of resources allocated for protection of each request, LF-SSP is able to achieve satisfactory performances for both wavelength- and sub-wavelength-level multicast request protections as long as the transceiver resources on the network nodes are not too limited. More redundant transceiver resources basically lead to more significant performance superiority of the LF-SSP method.

4.5. Effects of the Averaged Number of Destinations of Each Request

We also study the influences of the average number of destinations per multicast session on the performance of the LF-SSP method. Once again, we consider different cases of wavelength- and sub-wavelength-level multicast requests protection in networks with limited and unlimited port resources respectively. As the conclusions hold for networks with either un-limited or limited port resources, we present only the results obtained in port-limited networks.

Figure 12 compares LF-SSP and CL-SSP in the port-limited NSFnet topology for SMTG. Simulation results show that LF-SSP outperforms CL-SSP: when the average size of the multicast sessions is small, e.g., $E(N) < 4.5$, LF-SSP is superior to CL-SSP by more than one order of magnitude; when the size of the multicast session increases, the performance difference between these two methods decreases. This observation can be understood: when the size of the average multicast-session is small, the network resources are relatively abundant and thus the performance superiority of LF-SSP is more significant. When the average session size is large, however, the network resources become relatively scarce, which decreases the performance superiority of LF-SSP method, as we discussed earlier.

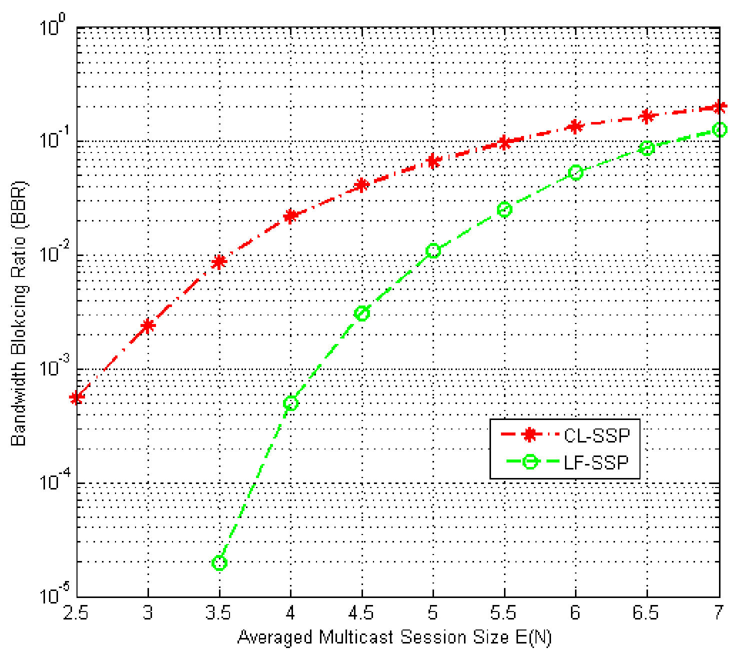

Figure 12: LF-SSP compared to CL-SSP for sub-wavelength-level multicast request protection in the NSFnet topology ($r = 0.6, \rho = 60 Erlangs$).

Figure 13 compares LF-SSP versus the SPT and LP methods for the protection of wavelength-level multicast requests in the port-limited NSFnet topology. It is evident that LF-SSP achieves better BBR performance than both SPT and LP in the simulated cases. Specifically, when the multicast-session size is small, i.e., $E(N) < 4$, LF-SSP outperforms LP by about an order of magnitude. Even when the average multicast-session size is larger, i.e., $E(N) > 4.5$, it still outperforms LP by 54% averaged over all the simulated cases. When compared to the SPT method, LF-SSP also achieves much better performances in different cases: when $E(N) < 4$, it outperforms SPT by more than 60%; while when $E(N) > 4.5$, its performance is still slightly better over that of SPT. As we have discussed earlier: more redundant network resources allow the LF-SSP method to achieve more significant improvements over the existing methods.

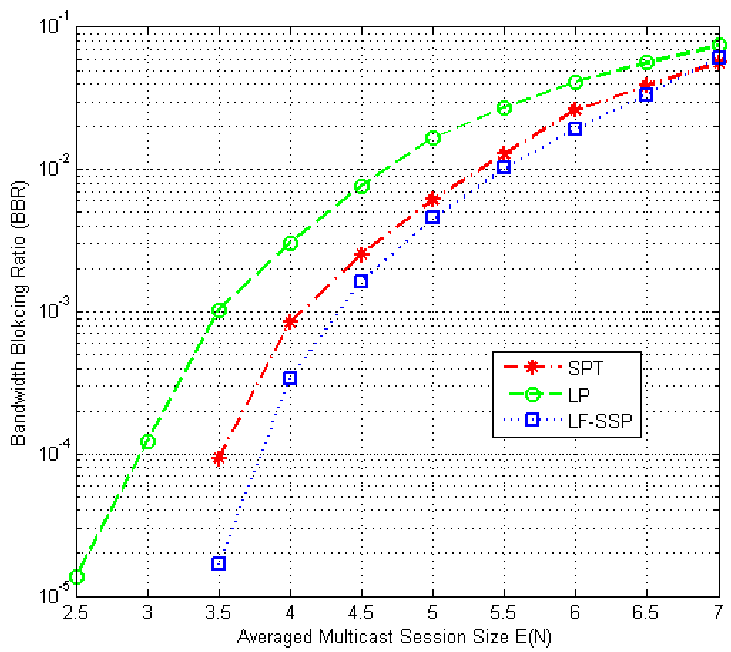

Figure 13: LF-SSP compared to SPT and LP for wavelength level multicast request protection in the NSFnet topology ($r = 0.6, \rho = 30Erlangs$).

It is worth noting that the LF-SSP method is designed for sub-wavelength level request protection. For wavelength-level request protection, there may still be nontrivial space for further improving the performance of the algorithm. For example, the three parameters defined in (4) – (6) may be optimized to further improve the network resources sharing for wavelength-level request provisioning. Detailed discussions on such possible improvements, however, are out of the scope of this paper and hence, have to be left to a future report.

5. Conclusion

In this paper, we addressed the problem of protecting sub-wavelength-level multicast requests against single link failure in dynamic traffic grooming process. An efficient mechanism, namely, lightpath-fragmentation based segment shared protection (LF-SSP), was proposed. LF-SSP attempts to minimize the network BBR by adopting the LF method to properly split the primary/backup lightpaths to improve resource sharing. Extensive simulations have been conducted to evaluate the performances of LF-SSP in various cases. Results demonstrated that LF-SSP is capable of achieving satisfactory BBR performances for either sub-wavelength- or wavelength-level multicast request protection in networks with limited or unlimited transceiver resources under various traffic loads; performance superiority of LF-SSP compared to the existing methods is more significant when the network resources are relatively more abundant. The influences of variations in the number of add/drop ports and average multicast destination numbers per request on the performances of LF-SSP were also evaluated.

Our future studies may include optimizing the algorithm for wavelength-level multicast protection, and extending the algorithm to handle the case with certain kinds of node failures, etc.

References

[1] B. Mukherjee, *Optical WDM Networks.* New York, USA: Springer Science+Business Media, Inc., 2006.

[2] I. Chlamtac, A. Ganz, and G. Karmi, "Lightpath communications: an approach to high bandwidth optical WAN's," *IEEE Trans. Commun.*, vol. 40, no. 7, pp. 1171–1182, Jul. 1992.

[3] G. N. Rouskas and H. G. Perros, "A tutorial on optical networks," *NETWORKING 2002 Tutorials, LNCS 2497*, pp. 155–193, May 2002.

[4] L. H.Sahasrabuddhe and B. Mukherjee, "Light-trees: Optical multicasting for improved performance in wavelength-routed networks," *IEEE Commun. Mag.*, vol. 37, no. 2, pp. 67–73, Feb. 1999.

[5] K. Zhu and B. Mukherjee, "Traffic grooming in an optical WDM mesh network," *IEEE J. Sel. Areas Commun.*, vol. 20, no. 1, pp. 122–133, Jan. 2002.

[6] N. K. Singhal, L. H.Sahasrabuddhe, and B. Mukherjee, "Optimal multicasting of multiple light-trees of different bandwidth granularities in a WDM mesh network with sparse splitting capabilities," *IEEE/ACM Trans. Netw.*, vol. 14, no. 5, pp. 1104–1117, Oct. 2006.

[7] A. E. Kamal, "Algorithms for multicast traffic grooming in WDM mesh networks," *IEEE Commun. Mag.*, vol. 44, no. 11, pp. 97–105, Nov. 2006.

[8] R. Lin, W.-D. Zhong, S. K. Bose, and M. Zukerman, "Light-tree configuration for multicast traffic grooming in WDM mesh networks," *Photonic Netw. Commun.*, vol. 20, no. 2, pp. 151–164, Oct. 2010.

[9] X. Yu, G. Xiao, and T.-H. Cheng, "Dynamic multicast traffic grooming in optical wdm mesh networks: Lightpath vs light-tree," *IEEE/OSA J. OPT. COMMUN. NETW.*, vol. 5, no. 8, pp. 870–880, Aug. 2013.

[10] S. Ramamurthy and B. Mukherjee, "Survivable WDM mesh networks. II - restoration," in *Proc. IEEE International Conference on Communications '1999*, vol. 3, Jun. 1999, pp. 2023 – 2030.

[11] S. Ramamurthy and B. Mukherjee, "Survivable WDM mesh networks. part I-protection," in *Proc. Eighteenth Annual Joint Conference of the IEEE Computer and Communications Societies INFOCOM '99*, vol. 2, Mar. 1999, pp. 744 – 751.

[12] H. Drid, B. Cousin, M. Molnar, and S. Lahoud, "A survey of survivability in multi-domain optical networks," *Computer Communications*, vol. 33, no. 8, pp. 1005–1012, May 2010.

[13] N. K. Singhal, L. H.Sahasrabuddhe, and B. Mukherjee, "Provisioning of survivable multicast sessions against single link failures in optical WDM mesh networks," *IEEE/OSA J. Lightw. Technol.*, vol. 21, no. 11, pp. 2587–2594, Nov. 2003.

[14] H. Luo, L. Li, and H. Yu, "Algorithm for protecting light-trees in survivable mesh wavelength-division-multiplexing networks," *Journal of Optical Networking*, vol. 5, no. 12, pp. 1071–1083, Dec. 2006.

[15] H. Luo, L. Li, H. Yu, and S. Wang, “Achieving shared protection for dynamic multicast sessions in survivable mesh WDM networks,” *IEEE J. Sel. Areas. Commun.*, vol. 25, no. 9, pp. 83–95, Dec. 2007.

[16] X. Wang, L. Guo, L. Pang, J. Du, and F. Jin, “Segment protection algorithm with load balancing for multicasting WDM mesh networks,” in *10th International Conference on Advanced Communication Technology 2008. (ICACT 2008.)*, vol. 3. IEEE, 2008, pp. 2013–2016.

[17] F. Zhang and W.-D. Zhong, “Performance evaluation of optical multicast protection approaches for combined node and link failure recovery,” *IEEE/OSA J. Lightw. Technol.*, vol. 27, no. 18, pp. 4017–4025, Sep. 2009.

[18] L. Long and A. E. Kamal, “Tree-based protection of multicast services in WDM mesh networks,” in *Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE.* IEEE, Nov. 2009, pp. 1–6.

[19] T. Panayiotou, G. Ellinas, and N. Antoniades, “Segment-based protection of multicast connections in metropolitan area optical networks with quality-of-transmission considerations,” *IEEE/OSA J. OPT. COMMUN. NETW.*, vol. 4, no. 9, pp. 692–702, Sep. 2012.

[20] C. Lu and L. Li, “Dynamic multicast traffic grooming for survivable WDM mesh networks,” in *Proc. International Conference on Communications, Circuits and Systems 2008*, May 2008, pp. 567–571.

[21] C. Ou, K. Zhu, H. Zang, L. H. Sahasrabuddhe, and B. Mukherjee, “Traffic grooming for survivable WDM networks-shared protection,” *IEEE J. Sel. Areas. Commun.*, vol. 21, no. 9, pp. 1367–1383, Nov. 2003.

[22] X. Yu, G. Xiao, and T.-H. Cheng, “Connection-level segment shared protection for dynamic multicast traffic grooming,” in *Proc. IEEE ICICS ’2013*, Dec. 2013.

[23] D. Xu, Y. Xiong, and C. Qiao, “Novel algorithms for shared segment protection,” *IEEE J. Sel. Areas. Commun.*, vol. 21, no. 8, pp. 1320–1331, Oct. 2003.

[24] P.-H. Ho, J. Tapolcai, and T. Cinkler, “Segment shared protection in mesh communications networks with bandwidth guaranteed tunnels,”

IEEE/ACM Transactions on Networking, vol. 12, no. 6, pp. 1105–1118, Dec. 2004.

[25] N. K. Singhal, C. Ou, and B. Mukherjee, "Cross-sharing vs. self-sharing trees for protecting multicast sessions in mesh networks," *Computer Networks*, vol. 50, no. 2, pp. 200–206, 2006.

[26] H. Takahashi and A. Matsuyama, "An approximate solution for the steiner problem in graphs," *Math. Japonica*, vol. 24, no. 6, pp. 573–577, 1980.

[27] X. Yu, G. Xiao, and T.-H. Cheng, "Historical data learning based dynamic LSP routing for overlay IP over WDM networks," *Optical Fiber Technology*, vol. 19, no. 4, pp. 308–319, Aug. 2013.

[28] E. A. Doumith and M. Gagnaire, "Impact of traffic predictability on WDM EXC/OXC Network performance," *IEEE J. Sel. Areas. Commun.*, vol. 25, no. 5, pp. 895–904, Jun. 2007.