Electronic Traffic Grooming in Dedicated Path Protected IP over Elastic Optical Network

Fengxian Tang, Gangxiang Shen*, Lian Xiang, Mingyi Gao
School of Electronic and Information Engineering, Soochow University, Suzhou, Jiangsu Province, P. R. China
*Correspondence email: shengx@suda.edu.cn

Abstract: We propose different electronic traffic grooming schemes for IP over elastic optical networks with dedicated path protection. Simulation results show that the proposed approaches can significantly improve network capacity utilization and reduce the number of transponders.

OCIS codes: (060.4250) Networks; (060.4256) Network, network optimization

1. Introduction
In recent years, elastic optical network (EON) has emerged as a new technology to achieve better fiber spectrum utilization [1]. In this type of network, optical channels provide huge bandwidth, so it is important to provide an efficient way to aggregate low speed IP traffic flows onto the optical channels. Such an aggregation process is called traffic grooming [2]. Meanwhile, network protection is important for an optical transport network which combats fiber failures through simultaneously establishing a pair of working and protection paths between each pair of nodes. In this study, we focus on electronic traffic grooming in the IP over EON with dedicated path protection. We propose and compare different electronic traffic grooming schemes for dedicated path protected IP over EON. A scheme with IP traffic flow splitting in the grooming process is also proposed, which allows multiple paths in a virtual topology to serve the bandwidth request between each node pair. The schemes using dedicated and non-dedicated optical channels to accommodate working and protection IP traffic flows are also evaluated and compared. We aim to minimize the maximal number of used frequency slots (FSs) and optical transponders when all the IP traffic requests are served. Though there are works on traffic grooming of IP over EON without protection [3][4] and IP over WDM with protection [5], to the best of our knowledge, this is the first work that considers electronic traffic grooming in dedicated path protected IP over elastic optical network with different modulation formats.

2. Traffic grooming with dedicated path protection
In the elastic optical network, a lightpath may traverse multiple fiber links. The failure of a network component such as a fiber cable cut can lead to the failure of all the lightpaths that traverse the link and therefore cause a huge data loss. Dedicated path protection provides backup resources on a protection path that has no links shared with the primary path between the source and destination nodes. In this study, we focus on dedicated path protection in the IP layer, i.e., establishing a pair of working and protection IP traffic flows between each node pair. In the context of this type of protection, we next introduce the concept of electronic traffic grooming in the IP over EON.

Fig. 1 shows an example of traffic grooming in IP over EON with dedicated path protection. In Fig.1 (a), three working paths A-B, B-C, A-C are established respectively for the requests between corresponding node pairs, and their backup paths are also dedicatedly established between the node pairs. Without traffic grooming, 12 transponders are required to establish all these 6 lightpaths. In contrast, Fig. 1(b) shows the case with traffic grooming, where low speed traffic flows can be aggregated onto common optical channels. In this example, the traffic flow between node pair (A, C) are aggregated onto the working and protection lightpaths established between node pairs (A, B) and (B, C). As a result, there are only 4 lightpaths and 8 transponders required.

In the example, an important assumption is made that the same type of IP traffic flows should be aggregated onto the same types of optical channels. That is, protection traffic flows are aggregated onto optical channels dedicated to protection traffic and working traffic flows are aggregated onto optical channels dedicated to working traffic. We call these two types of optical channels “working” and “protection” optical channels. In the context of a virtual topology for IP traffic grooming, they are also called “working” and “protection” virtual links, respectively, and the corresponding virtual topologies are called “working” and “protection” virtual topologies, respectively.

The separation of working and protection traffic flows in different types of optical channels can simplify network control and management. However, this can create some low efficiency situation as the working and protection IP traffic flows cannot be multiplexed onto a common optical channel that may be underutilized. Thus, in this study we also consider a mixed scenario that allows the working and protection IP traffic flows between different node pairs to share common optical channels. Such multiplexing is possible as long as the condition of route disjointness between pairs of working and protection paths can be ensured. In this case, we do not distinguish working and protection optical channels, but generally call them “mixed” optical channels.
For traffic grooming, we also propose a scheme called “flow splitting,” which allows the IP traffic flow between a node pair to be split and routed over different paths. This can increase the flexibility of traffic grooming and improve capacity utilization. Fig. 2 shows an example of traffic grooming with flow splitting, in which lightpaths A-B, B-D, A-C, and C-D are established for the requests between node pairs. For the request of A-D, we may split the 50-Gb/s request into a 30-Gb/s and 20-Gb/s flow, and route the first flow via A-B and B-D and the second flow via A-C and C-D (see Fig. 2(b)). Obviously the flow splitting process can save lightpath A-D and its corresponding transponders, thereby improving spectrum efficiency and decreasing system cost.

3. Heuristic algorithm

We develop several schemes for traffic grooming in dedicated path protected IP over EON. However, due to the page limit, we only present the key steps for the scheme with dedicated “working” and “protection” optical channels and without flow splitting (called “fundamental scheme”). All the other schemes will be further briefed based on the fundamental scheme.

**Step 1** For each demand request $R$ (with bandwidth $B_R$) between a node pair, create empty virtual topologies $G_w$ and $G_p$ for working and protection virtual links (optical channels), respectively.

**Step 2** Route working traffic flow of $R$ in $G_w$: remove all the virtual links whose remaining bandwidth is smaller than $B_R$ from $G_w$; employ Dijkstra’s algorithm to find a shortest route in $G_w$. If failed, move to Step 3; otherwise, move to Step 4.

**Step 3** Establish a working optical channel between the node pair of $R$: establish a working optical channel $C_w$ along the shortest route between the node pair in the physical topology; assign the most efficient modulation format and just sufficient number of FSs (in the first-fit way) to $C_w$; accommodate the traffic demand of $R$; add $C_w$ as a new virtual link to $G_w$.

**Step 4** Route protection traffic flow of $R$ in $G_p$: remove all the virtual links whose remaining bandwidth is smaller than $B_R$ from $G_p$; remove all the virtual links that have shared (physical) links with the working flow of $R$ from $G_p$; employ Dijkstra’s algorithm to find a shortest route in $G_p$. If failed, move to Step 5; otherwise, $R$ is served.

**Step 5** Establish a protection optical channel between the node pair of $R$: remove all the links that are traversed by the working flow of $R$ from the physical topology; establish a protection optical channel $C_p$ along the shortest route between the node pair in the physical topology; assign the most efficient modulation format and just sufficient number of FSs (in the first-fit way) to $C_p$; accommodate the traffic demand of $R$; add $C_p$ as a new virtual link to $G_p$.

Based on the above fundamental scheme, we further have the following extended schemes: (1) fundamental scheme with flow splitting, in which all the steps are the same except that in Step 2 and 4 the flow splitting strategy is applied; (2) scheme with mixed optical channels, in which each optical channel is allowed to carry both working and protection traffic flows as long as the condition of route disjointness between them is ensured. For this case, we also have two sub-cases, i.e., with and without flow splitting.

4. Simulation and performance analyses

To evaluate the performance of the proposed traffic grooming schemes, we consider the 14-node, 21-link NSFNET network as the test network (see Fig. 3). The traffic demand between each node pair follows a random distribution within the ranges from 5 to 50 Gb/s, to 100 Gb/s, and maximally to 300 Gb/s. For each range, we average the results of 15 randomly generated traffic matrixes. We assume that four modulation formats (i.e., BPSK, QPSK, 8 QAM, and 16 QAM) are employed in the study. For each of the modulation formats, we assume a maximal optical reach as shown in Table I, in which the bandwidth of each FS is assumed to be 12.5 GHz and each row shows the FS...
capacity and transparent reach of the corresponding modulation format. In this test study, as there is no shortest route longer than 4000 km, no signal regeneration needs to be considered.

The simulation results are shown in Fig. 4, in which legend “TG” means traffic grooming based on dedicated path protection, “w/o” means word “without,” “FS” means “flow splitting,” “Dedicated” and “Mixed” mean whether optical channels are dedicated to working and protection traffic flows or support them in a mixed way. Based on the results, we have the following key observations. (1) Compared with the case without traffic grooming (i.e., the curve “w/o TG”), the traffic grooming schemes can significantly reduce the number of required FSs by up to 45% and the number of transponders by up to 15% at a low bandwidth request. However, when the bandwidth request increases, the performance improvement decreases. Specifically, when the bandwidth request is 300 Gb/s, the performance difference between the schemes with traffic grooming and without traffic grooming becomes very small. This is reasonable because when the bandwidth request is low, there are more opportunities for an established optical channel to have sufficient remaining capacity to accommodate a traffic flow between a node pair. In contrast, when the bandwidth request is high, such an opportunity becomes very low; there is a high chance of requiring a direct lightpath between a node pair, which is just the case of without traffic grooming. (2) Comparing the schemes with dedicated and mixed optical channels, we see that the mixed case requires smaller numbers of FSs and transponders. This is also reasonable as the mixed case is more efficient to allow working and protection traffic flows to share a common optical channel. (3) Comparing the cases with and without flow splitting, we see that flow splitting does help reduce the numbers of FSs and transponders. This is also reasonable since traffic grooming with flow splitting is more flexible to route portions of bandwidth request on multiple routes, thereby better utilizing the remaining capacity in each optical channel.

5. Conclusions
We proposed different schemes for electronic traffic grooming in IP over EON with dedicated path protection. We aim to minimize the total numbers of used frequency slots and transponders in the EON. Simulation results show that compared to the case without traffic grooming, the proposed approaches are efficient to significantly reduce the total numbers of required FSs and transponders. Also, the scheme of allowing working and protection IP traffic flows to share common optical channels is efficient to improve network capacity utilization.

Acknowledgment: This work was jointly supported by National Natural Science Foundation of China (NSFC) (61322109, 61172057), Natural Science Foundation of Jiangsu Province (BK20130003, BK2012179), and Science and Technology Support Plan of Jiangsu Province (BE2014855).

Table I: FS Capacities and Optical Reaches of Different Modulation Formats

<table>
<thead>
<tr>
<th>Modulation Format</th>
<th>FS Capacity (Gbit/sec)</th>
<th>Transparent Reach (km)</th>
</tr>
</thead>
<tbody>
<tr>
<td>BPSK</td>
<td>12.5</td>
<td>4000</td>
</tr>
<tr>
<td>QPSK</td>
<td>25</td>
<td>2000</td>
</tr>
<tr>
<td>8 QAM</td>
<td>37.5</td>
<td>1000</td>
</tr>
<tr>
<td>16 QAM</td>
<td>50</td>
<td>500</td>
</tr>
</tbody>
</table>

Fig. 3. 14-node, 21-link NSFNET network

Fig. 4. Performance comparison between different traffic grooming schemes

(a) Used frequency slots

(b) Used transponders

(a) Used frequency slots

(b) Used transponders

5. Conclusions
We proposed different schemes for electronic traffic grooming in IP over EON with dedicated path protection. We aim to minimize the total numbers of used frequency slots and transponders in the EON. Simulation results show that compared to the case without traffic grooming, the proposed approaches are efficient to significantly reduce the total numbers of required FSs and transponders. Also, the scheme of allowing working and protection IP traffic flows to share common optical channels is efficient to improve network capacity utilization.

Acknowledgment: This work was jointly supported by National Natural Science Foundation of China (NSFC) (61322109, 61172057), Natural Science Foundation of Jiangsu Province (BK20130003, BK2012179), and Science and Technology Support Plan of Jiangsu Province (BE2014855).