Journal of Theoretical and Applied Information Technology
31st October 2022. Vol.100. No 20

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

MULTICAST PROTECTION WITH GROOMING BACKUP PATH IN ELASTIC OPTICAL NETWORK

BODJRE AKA HUGUES FELIX[1], ADEPO JOEL[2], KEUPONDJO SATCHOU GILLES ARMEL[3], COULIBALY ADAMA[4], BABRI MICHEL[5]

[1-3-5]École Doctorale Polytechnique, INP-HB de Yamoussoukro, Côte d'Ivoire

[2]Univercité virtuelle, Abidjan, côte d'ivoire

[3]Universtié Félix Houphouët Boigny, Abidjan, Côte d'Ivoire

E-mail: [1]aka.bodjre@inphb.ci, [2]Jcadepo@hotmail.fr, [3]armel.keupondjo@inphb.ci [4]couliba@yahoo.fr, [5]michelbabri@gmail.com

ABSTRACT

The protection of connections in very high-speed networks such as elastic optical networks is an effective solution to limit the damage due to failures on the links in the network. We have therefore proposed a protection approach that uses backup path bundling to solve the problem of protection with connection bundling in EONs. The proposed algorithm makes it possible to build the primary path and the backup path of the connections by grooming the primary and backup paths which share links in common. Thus, this algorithm reduces the resources used such as spectral resources and transponders. The simulation results reveal that the proposed approach yields better performance in terms of blocking probability, transponder cost and spectrum utilization rate compared to the shared protection method without connection bundling.

Keywords: *Multicast, Shared Protection, traffic Grooming, Elastic Optical Networks*

1. INTRODUCTION

The emergence of multicast applications such as video conferencing, Internet Protocol Television (IP-TV) and e-learning, increases the demand for bandwidth [1]. And the wavelength division multiplexing-based optical network with fixed grid allocation can no longer efficiently keep up with these emerging and dynamic applications due to the limited number of optical channels [2]. This limitation has motivated the research community to turn to so-called elastic (or) flexible optical networks (EONs) that efficiently allocate spectrum according to user demand [3]. In elastic optical networks, implementing a multicast (i.e., a communication from one source to several destinations) application, means using a continuous spectrum optical tree on the paths leading to each destination [4].Since most multicast applications are real-time and need to transmit data from one source to several destinations, it is necessary to protect this data from any possible failure. In general, the bandwidth demand on an optical channel is enormous, so that in case of failure of a single link, it could lead to a serious interruption of the data transmission. To avoid interruptions due to link or node failures, connection protection is implemented by the network operator. Connection protection consists of finding backup paths disjoint from the primary path. There are a significant number of protection methods in EONs. These multicast protection methods include: tree protection, path protection, segment protection, ring protection and p-cycle protection [5]. These proposals take into account protection mechanisms [6] or restoration mechanisms [7]. That is, depending on whether the backup paths are calculated before the failure or dynamically based on the link state information. As a result, the protection of shared connection requests has proven to be efficient in terms of spectral [8], but requires more resources to be reserved on the backup paths in case of failures. As such, traffic grooming is an efficient technique to reduce the resources used in connection establishment (transponders, spectral resources with the reduction of additional guard bands). The basic idea of optical grooming is to groom several sub-wavelength optical paths into a single Bandwidth Variable Transmitter (BVT) [9].

In the literature, this optical grooming is called optical tunnel. Based on the orthogonal

Journal of Theoretical and Applied Information Technology
31st October 2022. Vol.100. No 20

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

characteristic of OFDM signals, traffic from the same source BVT can be groom without guard's bands between two connections requests. Using the elastic nature of BV-OXC spectrum switching, a subset of subcarriers in the optical tunnel (corresponding to a subwavelength optical path) can be dropped or optically switched at any intermediate node along the route. For traffic from different source nodes (which use different oscillators), since orthogonality cannot be guaranteed between them, they must be received separately using different receivers. When using optical grooming, it is desirable that no guard bands are needed between grooming services, as this leads to inefficient use of the transponder and spectrum[9]. Services with the same source and destination can be switched as a single optical path, so no guard band is needed between them. For services with the same source and different destinations, it is also possible to groom them together without guard bands. As shown in Figure 1, in tunnel 1 three connections requests can be groom together, namely, the red, pink, and blue connections. Then, in tunnel 2, two connection requests can be groomed, namely the pink and blue connections. Finally, at node c, each connection goes to its destination. If a sub-wavelength optical path is to be separated from the optical tunnel at an intermediate node, the original optical tunnel is divided into several optical tunnels.

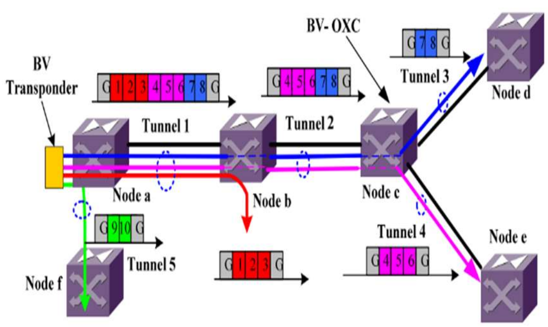

Figure 1: Example Of a Grooming Connection Demand In The EONs[9]

Guard bands should be added next to the separate optical tunnels, so that they can be switched to the subsequent BV-OXCs. In view of all the above, combining the protection method with traffic grooming before spectrum resource allocation, will lead us to minimize the used spectrum resources significantly. Some studies on multicast connection demand protection methods in elastic optical networks are presented in [10],[11]. But to the best of our knowledge, studies on shared protection for multicast connection demand and traffic grooming in EONs are not yet exploited. Therefore, in this study, we propose an abbreviated path protection algorithm with grooming and share backup path (PP-GSBP) in a multicast context.

The objective of this algorithm is to provide protection against network failure and to reduce spectrum utilization rate and transponders utilized Satisfy the new demand for multicast connection demand, by providing it with a primary and backup path while reducing the number of slots and transponders in the network by grooming backup paths sharing the same links.

Our approach in this paper, is based on shared protection which is more efficient in terms of spectral resource than dedicated protection [1]. Given the problem of protecting multicast connection demand in elastic optical networks, two main methods exist in the [12], namely shared and dedicated protection. Protection is said to be shared when the backup paths of two different connections share at least one link. And a protection is called dedicated when the backup paths of two different connections are disjoint or do not share any link. Unlike dedicated protection, a shared protection method can provide protection with less spectral resource. Therefore, in this work we have opted for a shared protection method. There are works in the literature on shared connection protection techniques. Some of these techniques are only interested in protecting connections while others, in addition to protecting connections, reduce the cost of resources used by the traffic grooming.

The rest of this paper is organized as follows, Section 2 present a state of the art on existing works, Section 3 makes a specification of the problem. A detailed presentation of our approach is made in Section 4. Section 5 presents the results of our simulations. Section 6 concludes this article by opening some perspectives. The standards laid down, will not be published.

2. STATE OF ART

There are works in the literature on shared connection protection techniques. Some of these techniques are only interested in protecting connections while others, in addition to protecting connections, reduce the cost of resources used by traffic grooming.

2.1 Protection without grooming

In [13], the authors studied the dedicated protection policy in combination with the multicast RSA problem in EON. The authors proposed an

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

integer linear programming model with the goal of minimizing the spectral resources in the small-sized network. For large size network, two heuristic algorithms are proposed: i) the two-step dedicated path protection tree (DPPT-TS) approach and ii) the dedicated path protection tree spectral window plan (DPPT-SWP) approach. The algorithms work better in EON than in WDM optical networks. In addition, for small networks, DPPT-SWP has better performance than the ILP algorithm and the DPPT-TS approach. DPPT-SWP and DPPT-TS perform better than other protection approaches [14]. In [11], the authors proposed a dedicated backup protection mechanism in EON, which uses segment-based protection for dynamic multicast connexion demands. The objective of this proposed approach is the reduction of bandwidth blocking probability while protecting against link failures in the network for unicast and multicast connection demand. In this protection scheme, only link failure is considered. Three methods are compared in this paper: i) segment-based protection, ii) shared backup path protection and iii) dedicated backup path protection. The simulation results reflect the advantages and disadvantages of the different protection policies. From this study, it found that segment-based protection performs better when the traffic load is medium in the network, and this results in better spectrum utilization efficiency. A study on partial protection shows a reduction in the blocking probability of when the QoS parameter varies. In [8], the authors proposed two heuristic approaches to solve the multicast protection problem in an elastic optical network: i) the k-tree segmented protection algorithm (KTSPA) and ii) the low spectrum segmented protection algorithm (LSSPA). The approach used in these two algorithms is a shared segment-based protection approach and both static and dynamic multicast connexion demand are considered. Each primary tree is divided into a set of working segments and there is a dedicated backup segment corresponding to each working segment. Spectrum resources are reserved in these backup segments that can be used in case of link failure. An algorithm for finding the primary tree is implemented initially and this algorithm is used by both LSSPA and KTSPA. Simulations of these algorithms are performed to study the following parameters: i) blocking rate and ii) resource utilization rate. KTSPA performs better than the other algorithms regarding the resource utilization rate. In [15], shared protection in EON is proposed by considering adaptive distance for multicast connection demands. An integer linear programming model is proposed for small networks. For large networks, a heuristic approach is proposed by using an optical tree for multicast demand routing and by using a transmission distance-based approach for spectrum allocation. The performance evaluation of the heuristic algorithm gives a result close to the optimal result obtained from the result of ILP formulation. Among the two policies, the randomized traffic request approach performs better than the connection requests that are ordered in a decreasing manner. It has been observed by the authors that some results based on certain parameters can be improved but this takes a considerably long CPU time. A summary of these methods can be found in table1.

Table 1 : Summary Of Works About Shared Protection Without Grooming

Author	Type	Domain	Brief summary
In (2016) [15]	Shared Protection	EON	Protection with distance adaptive multicast RSA without grooming
In (2015) [8]	Shared Protection	EON	Segment-based protection without grooming for multicast traffic
In (2017) [13]	Dedicated Protection	EON	Protection based multicast RSA without grooming
In (2016) [11]	Dedicated Protection	EON	Segment-based protection without grooming for multicast traffic

2.2 Protection with grooming

In [16], the authors proposed a shared segment protection method and a grooming algorithm for WDM optical networks. This approach deals with multicast connection demands in the case of a single link failure. The proposed algorithm generates a primary tree for a multicast connection demand and a backup tree disjoint from the primary tree. Each primary segment has a set of backup segments. The traffic grooming allows efficient use of the wavelength channel capacity since multiple sub-wavelength connections can use one wavelength channel. In [17], the authors proposed a protection approach called Elastic Separate Protection-at-Connection (ESPAC). This protection approach emphasizes sharing the backup path and relies on

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

two constraints. Hence, connection requests can share resources on a backup path if: i) their corresponding primary paths have disjointed links, and ii) their backup paths are adjacent to each other on a fiber link and can share spectrum resources. Spectrum is allocated on the primary paths, with the First-Fit (FF) spectrum allocation technique and the Last-Fit (LF) spectrum allocation technique on the backup paths. In [18], the authors proposed a traffic grooming with energy optimization in EON, using the Software Defined Network (SDN) principle. They propose a ILP model and a heuristic algorithm to solve the problem of grooming, routing, and slot allocation in EONs. The objective is to meet a demand with adequate bandwidth ensuring the existence of a backup path. The results of the proposed approach are better than the non-grooming approach in terms of energy efficiency, blocking probability and spectral resource gains. Choudhury et al. [19], proposed a segment-based protection approach with traffic grooming in EON. The proposed grooming heuristic is typical for static connection requests and allows first to groom connections, then to protect them from link failure and finally to allocate spectrum to connection requests. They use a dedicated protection approach and divide the primary path into certain segments and provide a backup segment set for each primary segment. Choudhury et al.[20], proposed a path protection approach combined with traffic grooming problem in EONs. The proposed heuristic is specific to dedicated multicast connection demands but unlike the previous method [19] this approach uses dynamic connection requests. A summary of these methods can be found in Table2.

Table 2: Summary Of Works About Shared Protection With Grooming

Author	Type	Domain	Brief summary
In [16]	Shared Protection	WDN	Segment base protection with grooming for unicast application
In [17]	Dadicated Protection	EON	Protection elastique separated at connection with grooming for unicast application
In [18]	Shared Protection	EON-SDN	Power efficient protection with grooming for unicast application
In [19]	Dedicated Protection	EON	Segment-based protection with grooming for multicast application
In [20]	Dedicated Protection	EON	Path-based protection with grooming for dynamic multicast application

The multicast connection demand protection methods with the above traffic grooming problem are dedicated protection methods (unicast and multicast) and shared protection methods (unicast only).

Given the above, the existing methods show that only a few works have studied the survivability problem the network which supports the methods of protection with connection grooming in the EON.

Therefore, it is necessary to carry out further investigations to consider the problem of protection with bundling of shared multicast connections in elastic optical networks.

3. SPECIFICATION OF PROBLEM

To solve the formulated problem, in this section, we define our problem known as multicast connection protection with traffic grooming in elastic optical networks. In the following, network model, assumption, the problem description, and problem formulation are given.

3.1 Network Model

- The elastic optical network is represented by a graph $G = (V; E)$ where $V = \{v_{1,} v_{2,} \dots v_n\}$ is the set of network nodes with n number of nodes and $E = \{e_{1,} e_{2,} \dots e_m\}$ the set of optical links with m the number of links.
- In each link, we have an ordered set of frequency slots $fs = \{\mathrm{fs}_1, \mathrm{fs}_2, \dots, \mathrm{fs}_\mathrm{M}\}$, with M, the maximum number of slots.
- Consider a multicast connection demand $\mathrm{Mcr} = (\mathrm{s}; \mathrm{D}; \mathrm{b})$ where s is the source node, $\mathrm{D} = \{\mathrm{d}_1, \mathrm{d}_2 \dots \mathrm{d}_{|\mathrm{D}|}\}$ is the set of destinations $|\mathrm{D}|$ the number of destinations) and b the bandwidth required for the connection request.
- T is the primary tree of the multicast connection demand, formed by a set of

primary paths w_{Li} and $B = \{b_{Li} / i \in \mathbb{N}\}$ a set of links, called backup path disjoints to the working path w_{Li} .

3.2 Assumptions

- Network links are bidirectional and consist of two unidirectional fiber.
- All network nodes have multicast capability but no wavelength conversion capability.
- Each connection established in the network must correspond to a primary path and its backup path.
- Any failure of the primary path affects a single link on the tree.

3.3 Description of problem

Consider an optical network of 6 nodes and 9 links. We consider two multicast connexion Mcr1 and Mcr2 requiring respectively 2 and 1 frequency slots designed by Mcr1=(s4,{d2;d6},2) and Mcr2=(s1,{d2;d6},1) figure 2. These demands share the backup frequency slots on the link 3-6 with Mcr3 demand (Figure 2).

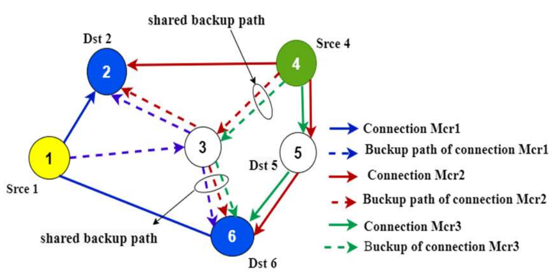

Figure 2 : Grooming Protection

One of the possible backup slot allocations can be represented in figure3.

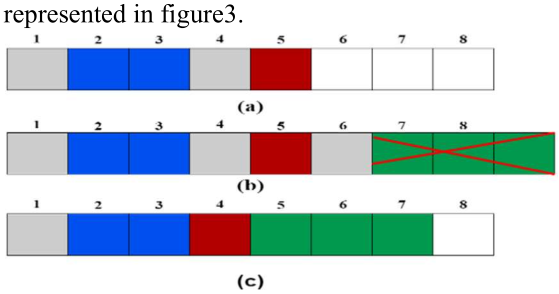

Figure 3: Resource Allocation Spectrum: (a)Link 3-6 Allocation Of The Two First Connection (b) Allocation Of The New Connection Without Grooming (c) Allocation Of The New Connection By The Grooming Method.

If Mcr3 with a set of three contiguous slots marked in green and a guard band arrives, then we observe on the shared backup link (link 3-6) that the free frequency slots on the link between node 3 and node 6 are not sufficient to accommodate the slots of Mcr3 (figure 3-b). Therefore, Mcr3 must be blocked because there are no unoccupied frequency slots for Mcr3. However, once the traffic grooming is done, the guard band is no longer needed; we can observe that the approach of Fig.3 (c) uses less frequency.

3.4 Formulation of problem

Data:

An elastic optical network represented by a graph $G = (V; E)$;

- $MCR = \{Mcr_1,\ Mcr_2, \dots, Mcr_n\}$ a set of multicast connexion demand with

$Mcr_i = (s, D, b)$, where **s** representing the source node, D as the set of destinations nodes and b the bandwidth required.

- FS, the number of spectrum frequency slots.

Objective is to provide protection against network failure and to reduce spectrum utilization rate and transponders utilized.

The constraints are as follows:

- Spectrum continuity constraint.

This constraint means that all the links of the primary tree of a multicast connection demand should be allocated the same range of frequency slots.

- Spectrum non-overlapping constraint.

This constraint indicates that if a link is common to two primary path of a multicast connection demand, the same frequency slots must not be assigned.

- Spectrum contiguity constraint.

This constraint indicates that the spectrum frequency slots allocated to a multicast connection demand must be adjacent to each other in the frequency domain.

- The primary path and the backup path must be disjoint.

This constraint indicates that the only link can be used either by the primary path or by the back path, but it cannot be used for both paths.

4. PROPOSED APPROACH

To solve the formulated problem, a path protection algorithm with grooming and sharing of backup paths for multicast connection demands, abbreviated as PP-GSBP, is proposed. The PP-GSBP takes as input a graph G, multicast connection demands already established and a connection arriving to be established. The result is a multicast tree (primary path) and a backup path for multicast connection demands. The PP-GSBP first checks if there are similar connection in the set of connection requests already established. That is, if two requests have the same source, then their destination sets are matched, and if their destination sets are identical, then they are groomed (thus forming a single connection) and switched together. Then, for a particular traffic request, Dijkstra's algorithm is applied on the graph G to form the primary path. If the primary path can be found on G, then it is allocated a range of bandwidth required in terms of the number of slots required. Then, for each primary path, a disjoint backup path on G is found for the protection of the primary path. If a backup path is found for each primary path on G, then the required bandwidth is allocated to it in terms of the number of slots required. For all primary paths in the multicast tree, if all backup paths can be found on G then, the multicast connection demand can be established. Spectrum is allocated using the Resource First-Fit allocation technique[21].

4.1 Proposed algorithm

The following table 3 presents algorithm 1

Table 3 : Path Protection With Grooming And Share Backup Algorithm

- Input: a graph $G = (V; E)$, $MCR = \{Mcr_i = (s_i, D_i, b_i)\}$ a set of multicast connexion demands
- Output: a primary path and a backup path for each connection demand

1: **for** each multicast connexion demand $Mcr_i = (s_i, D_i, b_i)$ **do**
2: run the shortest path (Dijkstra's) algorithm on the graph G to find the primary path

3: ***if*** the primary path existing ***then***,
3 ***if*** grooming is ***true***
4: construire le chemin de secours disjoint au chemin primaire

5: ***if*** step 4 is successful ***then***,
6: For each link of primary path and the backup path, assigned b_i contiguous spectrum on the links of primary path and backup path *// using FIRST FIT Algorithm*
And
8: ***else***
9: Find a backup path for the non-grooming demand request on G // *using Dijkstra*
10: For each link of backup path, assigned b_i contiguous spectrum on the links of backup path *// using FIRST FIT Algorithm*
11: Add a guard band
12: Update transponder status
13: e***nd if***
14: ***else***
15: this request is blocked
16 : e***nd if***
17: Run the shortest path (Dijkstra's) algorithm on the graph G to find the link -disjoint backup path
18: ***if*** the backup path is found ***then***,
19: The backup path is Groomed with another existing backup path if they share at least one link
20: ***if*** *S*tep 19 is successful ***then***,
21: For each link of backup path, assigned b_i contiguous spectrum on the links of backup path *// using FIRST FIT Algorithm*
22: Remove Guard band
23: Update transponder status to free
24: ***else***
25 : Find another backup path for the non-grouped backup part on G // *using Dijkstra*
26: For each link in the backup path, assigned b_i contiguous spectrum on the links of backup path *// using FIRST FIT Algorithm*
27: add guard band
28: Update transponder status to occuped
29: e***nd if***
30 : ***else*** this demand request is blocked
31 : ***end if***
32: e***nd for***
33: Return primary paths and backup paths

4.2 Illustration

Figure 4 represents the graph of an elastic optical network. On the network graph, three multicast connection demands, namely: Mcr1 = $(1\,;\{4{,}6\};4)$, Mcr2 = $(1\,;\{4{,}6\};6)$ et Mcr3 = $(2\,;\{5{,}7\};3)$.

We note that, both requests Mcr1 and Mcr2 have the same source and same destination.

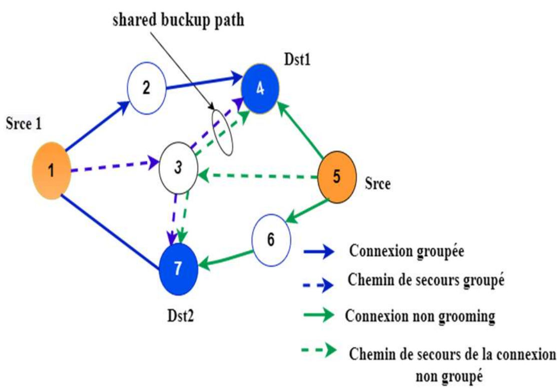

Figure 4: Example of Physical Network Topology With Connection Requests

As these two requests have common links, we group them so that the slot requests are added. Thus, the new request becomes a new request Mcr1.2= (1;{4,6};10). If the primary path contains paths 1→ 2 → 4 and 1→ 7, then the backup path contains path 1→ 3→ 4 and 3→7.

Now, the traffic groomed is routed, and slots are assigned to the primary paths as well as the backup paths. Mcr3, has the same destinations with Mcr1 and Mcr2 but does not share any links. It cannot be groomed with the other connection requests. Thus, if the primary tree contains paths 5→ 4 and 5→ 6→ 7 then, the backup path contains path 5→ 3→4 and 3→7 (Figure 4). Now, only Mcr3 is routed and slots are assigned to the primary paths as well as the backup paths. The following table 3 gives a comparison of the two methods in terms of spectral gain.

Table 4 : Illustration Of The Advantage Of Protection With Grooming And Share Backup Path

Link	Protection with grooming	Protection without grooming	slot Gain per Link
3-4	14	16	2
3-7	14	16	2
TOTAL	28	32	4

5. SIMULATION

This section presents the results of the algorithm considering the network shown in Figure 5. The network topology consists of 14 nodes and 21 links which are assumed to be bi-directional.
All simulations were run on a personal computer with Intel i5-2540M / 2.6 GHz processor, 4.0 GB RAM and with Linux distribution.
Each frequency slot has a value of 12.5 GHz, and the corresponding spectrum width to 25, 50, 75 GHz carry the traffic for data rates of 40, 100, 400 Gbit/s line-rates, respectively with varied MFs.

All network nodes can be selected as a source or as a destination. The number of destinations for each connection is random and, in the range [2;3]. Only one link failure is allowed.

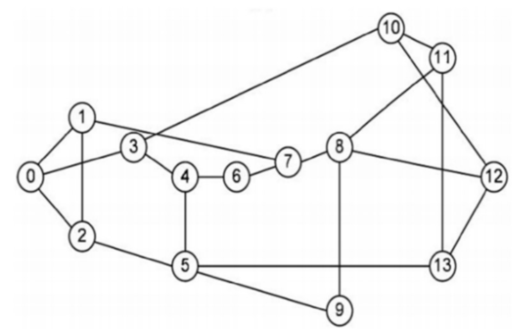

Figure 5: NSFNET Topology Used For The Evaluation Of Our PP-GSBP Algorithm

The following results were evaluated in terms of the following metrics:

1. the blocking probability (BP) which is defined by Equation 1

$$BP = \frac{number\ of\ blocked\ demands}{number\ of\ arriving\ demands} \quad (1)$$

2. the cost of transponders (CT) which is defined as the number of transponders used by all connection requests.

3. Spectrum Utilization Rate (SUR) which is defined by Equation 2,

$$SUR = \frac{occupied\ frequency\ slots}{total\ frequency\ slots} \quad (2)$$

The BP performance of the proposed approach with respect to network load is shown in Figure 6

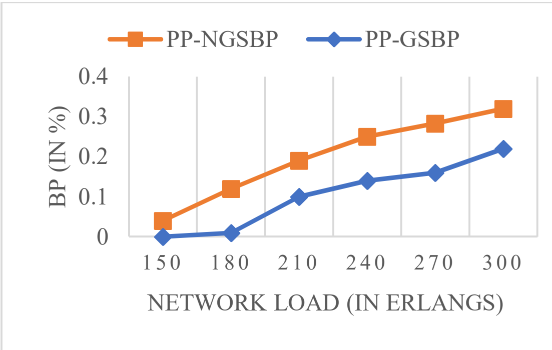

Figure 6 : Comparison Of The BP Of PCP-GCS And PC-SGCS According To The Network Load

From the results, it is evident that the integrated protection approach with grooming based on shared backup path protection performs better than other non-grooming standard approaches.

It can be observed from Fig.6 that with an increase in the number of incoming connection requests, the BP also increases for both approaches because, with the increasing network load, for the following requests, there is a decrease in the number of free resources and therefore more subsequent requests will need to be blocked. However, the BP for PP-GSBP is better than that of PP-NGSBP because PP-GSBP can economize on guard band slots. And this saving on the spectrum provisions service for many subsequent demands.

Then, the CT performances of the proposed approach regarding the number of transponders are illustrated in Figure 7.

We then compare the CT performance of the PP-GSBP and PP-NGSBP approaches, and show the result obtained in Figure 7. We observed that there is no connection request blocking for a network load equal to 150 Erlang. Therefore, to find the CT, we assumed that the network load is less than 150 Erlang.

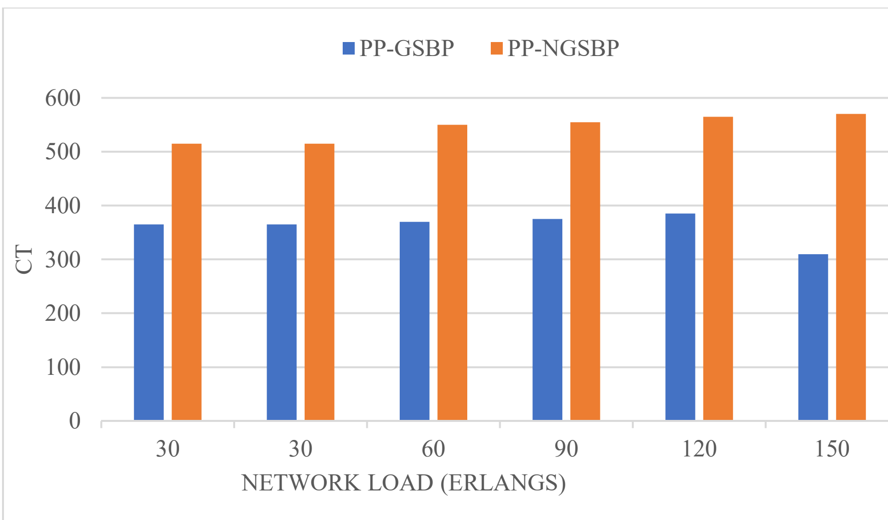

Fig. 7: Comparison Of CT Of PP-GSBP And PP-NGSBP As a Function Of Network Load

It can be observed from Figure 7, that the CT for the PP-GSBP scheme is much lower than that of the PP-NGSBP because less transponder resource consumption results in higher utilization of the existing optical path.

in conclusion, the grooming of several connections can be done in PP-GSB contrary to PP-NGSB which allows i) to establish new ones ii) allows a lower TC compared to the one obtained by PP-NGSB.

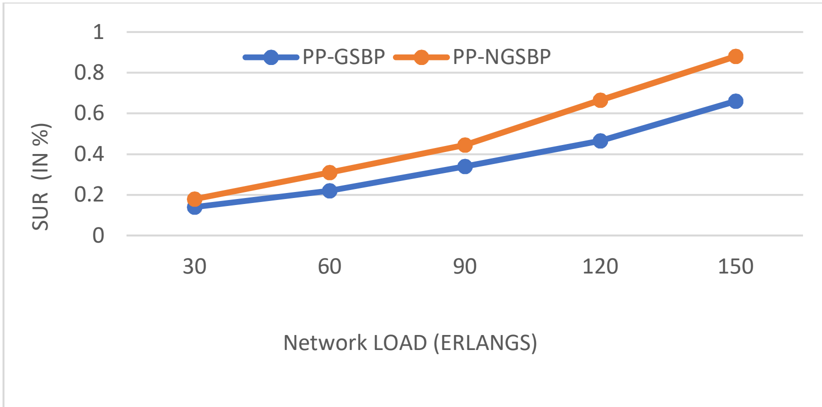

Fig. 8 : Comparison Of SUR Of PP-GSBP And PP-NGSBP As a Function Of Network Load.

We finally compare, in Figure 8, the SUR performance of the PP-GSBP and PP-NGSBP approaches. In this figure, it can be observed that the SUR increases with the number of requests, because the incoming multicast connexion more spectral resources to accommodate. It can also be seen that the SUR of the PP-GSBP approach is much lower than the PP-NGSBP approach. since PP-SGBP uses grooming which allows it to save more spectral resources and thus reduce transponder costs. Saving more spectral resources therefore means minimizing the total achievable spectrum, which reduces the SUR.

6. CONCLUSION

In this article, we performed a literature review on different optical connection protection methods. Then, we showed the advantage of using protection with traffic grooming. Finally, we described that the existing protection methods with traffic grooming are all based on a dedicated unicast or multicast protection scheme. In addition, we proposed a protection with traffic grooming for the shared multicast protection scheme. The simulation results showed that the proposed PP-GSBP protection with traffic grooming is better than the protection methods without traffic grooming in terms of blocking probability, number of transponders used, and resource utilization rate.

REFERENCES

[1] Der-Rong Din, « Survivable routing problem in EONs with FIPP p-cycles protection », in *2017 IEEE International Symposium on Local and Metropolitan Area Networks (LANMAN)*, Osaka, Japan, juin 2017, p. 1-2. doi: 10.1109/LANMAN.2017.7972133.

[2] J. Thangaraj, « Review and analysis of elastic optical network and sliceable bandwidth variable transponder architecture », *Optical Engineering*, vol. 57, p. 19, 2018.

[3] L. Velasco, A. P. Vela, F. Morales, et M. Ruiz, « Designing, Operating, and Reoptimizing Elastic Optical Networks », *J. Lightwave Technol.*, vol. 35, nº 3, p. 513-526, févr. 2017, doi: 10.1109/JLT.2016.2593986.

[4] X. Li, L. Zhang, Y. Tang, T. Gao, Y. Zhang, et S. Huang, « On-demand routing, modulation level and spectrum allocation (OD-RMSA) for multicast service aggregation in elastic optical networks », *Opt. Express*, vol. 26, nº 19, p. 24506, sept. 2018, doi: 10.1364/OE.26.024506.

[5] P. D. Choudhury, S. Bhadra, et T. De, « A brief review of protection based routing and spectrum assignment in elastic optical networks and a novel p-cycle based protection approach for multicast traffic demands », *Optical Switching and Networking*, vol. 32, p. 67-79, avr. 2019, doi: 10.1016/j.osn.2018.12.001.

[6] H. M. N. S. Oliveira et N. L. S. da Fonseca, « Routing, spectrum and core assignment algorithms for protection of space division multiplexing elastic optical networks », *Journal of Network and Computer Applications*, vol. 128, p. 78-89, févr. 2019, doi: 10.1016/j.jnca.2018.12.009.

[7] « OSA | On Spectrum Efficient Failure-Independent Path Protection p-Cycle Design in Elastic Optical Networks ». https://www.osapublishing.org/jlt/abstract.cfm?uri=jlt-33-17-3719 (consulté le 19 août 2021).

[8] D.-R. Din et I.-R. Lai, « Multicast protection problem on elastic optical networks using segment-base protection », in *2015*

International Conference on Informatics, Electronics & Vision (ICIEV), Fukuoka, Japan, juin 2015, p. 1-6. doi: 10.1109/ICIEV.2015.7334038.

[9] G. Zhang, M. De Leenheer, et B. Mukherjee, « Optical Traffic Grooming in OFDM-Based Elastic Optical Networks [Invited] », *J. Opt. Commun. Netw.*, vol. 4, nº 11, p. B17, nov. 2012, doi: 10.1364/JOCN.4.000B17.

[10] T. Feng, L. Ruan, et W. Zhang, « Intelligent p-Cycle Protection for Dynamic Multicast Sessions in WDM Networks », *J. Opt. Commun. Netw., JOCN*, vol. 2, nº 7, p. 389-399, juill. 2010, doi: 10.1364/JOCN.2.000389.

[11] M. Aibin et K. Walkowiak, « Different strategies for dynamic multicast traffic protection in elastic optical networks », in *2016 8th International Workshop on Resilient Networks Design and Modeling (RNDM)*, sept. 2016, p. 174-180. doi: 10.1109/RNDM.2016.7608284.

[12] R. Zou, H. Hasegawa, M. Jinno, et S. Subramaniam, « Link-protection and FIPP p-cycle designs in translucent elastic optical networks », *IEEE/OSA Journal of Optical Communications and Networking*, vol. 12, nº 7, p. 163-176, juill. 2020, doi: 10.1364/JOCN.382561.

[13] A. Cai, Z. Fan, K. Xu, M. Zukerman, et C.-K. Chan, « Elastic versus WDM networks with dedicated multicast protection », *Journal of Optical Communications and Networking*, vol. 9, nº 11, p. 921-933, nov. 2017, doi: 10.1364/JOCN.9.000921.

[14] C. K. Constantinou, G. Ellinas, et K. Manousakis, « Survivability of multicast requests in mesh optical networks », in *2014 International Conference on Optical Network Design and Modeling*, mai 2014, p. 7-12.

[15] A. Cai, J. Guo, R. Lin, G. Shen, et M. Zukerman, « Multicast Routing and Distance-Adaptive Spectrum Allocation in Elastic Optical Networks With Shared Protection », *J. Lightwave Technol.*, vol. 34, nº 17, p. 4076-4088, sept. 2016, doi: 10.1109/JLT.2016.2592999.

[16] A. K. Pradhan, S. Ghose, et T. De, « Multicast protection and grooming scheme in survivable WDM optical networks », *Optical Switching and Networking*, vol. 19, p. 42-57, janv. 2016, doi: 10.1016/j.osn.2015.06.003.

[17] M. Liu, M. Tornatore, et B. Mukherjee, « Survivable Traffic Grooming in Elastic Optical Networks—Shared Protection », *J. Lightwave Technol.*, vol. 31, nº 6, p. 903-909, mars 2013, doi: 10.1109/JLT.2012.2231663.

[18] S. Iyer, « Traffic grooming with survivability and power-efficiency in software defined elastic optical networks », *J Opt*, vol. 47, nº 3, p. 351-365, sept. 2018, doi: 10.1007/s12596-018-0469-7.

[19] P. D. Choudhury, S. Bhadra, et T. De, « Incorporating grooming in protection based elastic optical network », *CSI Transactions on ICT*, vol. 6, nº 2, p. 155-160, juin 2018, doi: 10.1007/s40012-018-0195-y.

[20] P. D. Choudhury, K. Ishwarya Reddy, et T. De, « A Path Based Protection and Traffic Grooming Approach in Flex-Grid Optical Networks », in *2019 21st International Conference on Transparent Optical Networks (ICTON)*, Angers, France, juill. 2019, p. 1-3. doi: 10.1109/ICTON.2019.8840221.

[21] A. Rosa, C. Cavdar, S. Carvalho, J. W. Costa, et L. Wosinska, « Spectrum allocation policy modeling for elastic optical networks », *High Capacity Optical Networks and Emerging/Enabling Technologies*, 2012, doi: 10.1109/HONET.2012.6421472.