Algorithm for FIPP *p*-cycle Path Protection in Flexgrid Networks

Helder M. N. S. Oliveira and Nelson L. S. da Fonseca
Institute of Computing - University of Campinas
Campinas 13089-971, SP, Brazil
Email: helder@lrc.ic.unicamp.br, nfonseca@ic.unicamp.br

***Abstract*—In optical networks, faults in links and nodes cause massive loss of data even if for short periods. Therefore, protection techniques have been developed to cope with failures. Among these techniques, *p*-cycle is very attractive since it provides ring-like speed of restoration in mesh topologies. In recent years, the technology of flexgrid networks has emerged as a solution for dealing with the diversity of bandwidth demands of network applications. However, very few investigations have been proposed for path protection in flexgrid networks. This paper introduces a novel algorithm to provide Failure-independent path protecting *p*-cycle for path protection in flexgrid networks. The proposed algorithm is compared to two other algorithms in the literature. Results indicate that the 100% protection for single failures can be provided by the proposed algorithm with low overhead to networks with high node connectivity.**

Keywords*—*P-cycle, Survivability, Elastic Optical Network.

I. INTRODUCTION

One of the main characteristics of the Internet architecture is to impose no constraint on the application layer which allows the fast emergence of new applications. These applications have heterogeneous bandwidth demands. Such diversity of bandwidth demands calls for a rate-flexible transport network.

The Wavelength Division Multiplexing (WDM) technique brought great capacity to the Internet link layer by allowing the multiplexing of several wavelengths in a single fiber. Traditional WDM networks employs a fixed-size frequency allocation per wavelength with a guard-band frequency separation between two wavelengths. In WDM, the fixed capacity of a wavelength accommodates demands of different sizes. This leads to underutilization of the spectrum since demands rarely match the exact capacity of a wavelength. Although multi-rate WDM introduces some flexibility in resource allocation, its coarse allocation granularity can only ameliorate the problem in a limited way.

Such rigidness has recently led to the emergence of spectrum-sliced elastic optical path networking. In this technology, (Optical) Orthogonal Frequency Division Multiplexing (OFDM) is employed. OFDM is a multi-carrier transmission technology that slits high data rate channels into a number of orthogonal channels, called subcarriers, each with (subwavelength) low data rates.

Being a cable-based medium, optical fibers are prone to cuts due to different reasons. Given the enormous capacity of an optical fiber, any disruption implies on huge loss of data. Such vulnerability has motivated the development of different protection and restoration schemes. *p*-Cycle is one of these protection techniques which has been intensively investigated in the past years due to its attractive properties. *p*-Cycles combine the properties of ring-like recovery speed and efficiency of restorable mesh networks. *p*-Cycles protect the working capacity on the span they cover, as shared protection rings, and, unlikely rings, they protect the working capacity of off-cycle spans which have their end-points on the *p*-cycle ("straddling spans"). A type of *p*-cycle of special interest is the Failure-Independent Path Protecting *p*-cycles (FIPP) *p*-cycle which provide fully pre-connected protection paths in optical networks.

However, the major difficulty in designing networks employing *p*-cycles for protection is the computational complexity of the problem which grows exponentially with the number of nodes and with the number of links. Since the network design with *p*-cycle problem is an NP-hard problem, heuristics have been developed to solve it.

This paper introduces an algorithm called FIPP-Flex for providing FIPP *p*-cycle protection in flexgrid (elastic) networks. To keep the complexity low, it is employed a Routing and Spectrum Assignment algorithm based on a multigraph representation of the spectrum. In despite of the large capacity demand for the provisioning of pre-connected 100 % path protection guarantee, numerical results indicate that it is quite advantageous to adopt the FIPP-Flex in networks with high node connectivity.The FIPP-Flex algorithm was compared to other path protection algorithms: the SPP-OFDM-Aggressive and survivable-FWDM algorithms. Results produced by the FIPP-Flex algorithm show that the overhead demanded to provide pre-connected protection pays off when compared with the other two schemes which to not provide pre-connected protection.

This paper is organized as follows. Section II review related work and Section III the concepts of *p*-cycle and NIPP. Section IV introduces the notation used in the paper. Section V introduces the RSA-FLEX algorithm and Section VI the FIPP-FLEX algorithm. Section VII evaluates the performance of the proposed algorithm and Section VIII concludes the paper.

II. RELATED WORK

The emergence of flexgrid networks has motivated several investigations, mainly on RSA algorithms but only recently investigations have addressed protection issues.

The authors in [1] proposed survivable transparent Flexible Optical WDM (FWDM), but the adoption of *p*-cycles was not investigated. They studied the survivable traffic grooming problem for elastic optical networks with flexible spectrum

978-1-4799-3512-3/14/$31.00 ©2014 IEEE

grid employing new transmission technologies. The authors proposed to use First-Fit to assign spectrum to the working paths, and Last-Fit to assign spectrum to the backup paths. Shao *et al.* [2] proposed and evaluated conservative and aggressive backup sharing policies in OFDM-based optical networks with elastic bandwidth allocation but *p*-cycles were not investigated. They introduced a sharing policy in which backup lightpaths with different allocated capacity can protect primary lightpaths with disjoint paths, leading to better use of resources to provide path protection.

In Liu *et al.* [3], the authors proposed a new technique for shared protection which provides spectrum sharing in the sense that a primary lightpath can share the spectrum with backup paths if the primary paths are physically disjoint. The protection approach is called elastic separate-protection-connection (ESPAC), which provides end-to-end protection at the connection level.

III. FAILURE-INDEPENDENT PATH PROTECTING *p*-CYCLES

The *p*-cycle is a protection scheme in which the spare capacity is pre-connected to form ring-like structures called *p*-cycle [4]. *p*-Cycles provide Bi-directional Line Switching Ring (BLSR) protection which is considered a generalization of the 1:1 protection scheme [5]. The main difference to conventional ring protection is that *p*-cycles provide two protection paths for each link that straddles the cycle. The straddling links can have working capacity but no spare capacity [6]. Moreover, working paths can be freely routed over a mesh structure and it is not necessary to follow ring-constrained routing topology. In networks protected by cycles, in an event of failure, only two switching actions at the end nodes of the failed span are necessary to switch the traffic to a protection path, as in conventional ring. *p*-Cycles provide fast restoration not because they are rings but because they are fully pre-connected before failure [7]. Figure 1 illustrates the concept of *p*-cycle. In Figure 1(a), *p*-cycles are represented by bold lines, the arrows represent the direction on which the path should be restored and "X" the faulting link. In Figure1(a), A-B-C-D-E-A is the reserved capacity for protection, i.e., the *p*-cycle. When the link A-B fails, the protection path is provided as shown in Figure 1(b). When the link B-D fails, the *p*-cycle protects both, providing two alternative paths as shown in Figures 1(c) and 1(d).

The major drawback of *p*-cycle is that the network design is an NP-hard problem and the exponential computational complexity depends on the number of nodes as well as the number of links. Therefore, to design *p*-cycle protected networks, heuristics need to be employed.

A special case of *p*-cycle for path protection is the so called Failure-Independent Path Protecting *p*-cycles (FIPP) [8]. FIPP *p*-cycles furnish protection to end-to-end working (primary) path with end nodes on the *p*-cycle. FIPP is an extension of the *p*-cycle concept in which the failure is not limited to be in a link or path segment immediately adjacent to the end nodes. FIPP is based on disjointness of working and backup paths, and provides the advantage that fault detection is independent of the fault location which is called failure independence. Failure independence is quite advantageous when location of fault is slow or difficult such as in transparent or translucent networks. This is an advantage over traditional path protection schemes and over the so called flow *p*-cycles.

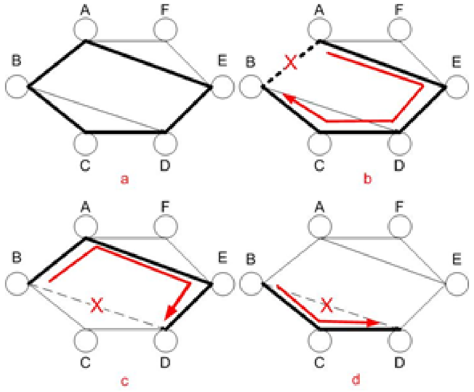


Figure 1: Example of a *P*-cycle

The Shared-Backup Path Protection (SBPP) proposed for networks based on IP signaling also has the property of failure independence. However, the major difference between SBPP and FIPP is that in SBPP the backup path needs to be determined on the fly upon failure which can adopt a restored path without the adequate transmission integrity. Thus, pre-connection of protection path is very important to assure the needed transmission quality. Moreover, SBPP demands extensive database due to the need of all nodes to have global capacity, topology and backup sharing relationship in order to furnish dynamic provisioning. The combination of failure independence and pre-connected protection paths leads to ring-like protection with minimal real time restoration of a path as well as minimal real-time signaling.

IV. NOTATION

The following notation will be used in the paper:

s: source node;

d: destination node;

b: bandwidth demand in slots, $b = 1 \ldots N$;

$r(s, d, b)$: request from the node s to the node d with bandwidth demand b in slots;

N: number of slots between two nodes;

$G = (V, E, W)$: labeled multigraph composed by a set of nodes V, a set of edges E and a set of edge weight W, $|E| = N \cdot |V|$. The edges connecting two vertices of G represent the N slots in the link connecting two network nodes;

$E = \{e_{u,v,n}\}$: set of n edges;

$e_{u,v,n}$: the n^{th} edges connecting u and v;

$w(e_{u,v,n})$: weight of the edge $e_{u,v,n}$; $c(e_{u,v,n}) = 1$ if the n^{th} slot in the link connecting OXC u and v is free and $w(e_{u,v,n}) = \infty$ if the slot is already allocated;

$W = \{c(e_{u,v,n})\}$:set of edge weights

$\widetilde{G}_{n,b} = (\widetilde{V}, \widetilde{E}, \widetilde{C})$: the n^{th} labeled graph such that $\widetilde{E}$ is the set of edges connecting $\{\widetilde{u}, \widetilde{v}\} \in \widetilde{V}$ and $\widetilde{C}$ is the set of costs associated to $\widetilde{E}$. The edges in $\widetilde{E}$ correspond to the mapping of b edges in G starting at the $n^{th} edge$;

$\widetilde{V} = V$: set of nodes;

$\widetilde{e}_{u,v} \in \widetilde{E}$: edge connecting $\widetilde{u}$ and $\widetilde{v}$; $\widetilde{e}_{\widetilde{u},\widetilde{v}} = \{e_{u,v,n}\} \in E$ is a chain such that $e_{u,v,n}$ is the least ordered edge, $e_{u,v,n+b}$ is the greatest ordered edge and $|\widetilde{e}_{u,v}| = b$;

$\widetilde{w}_n(\widetilde{e}_{\widetilde{u},\widetilde{v}})$: weight of the edge $\widetilde{e}_{\widetilde{u},\widetilde{v}}$;

$\widetilde{W}_n = \{\widetilde{c}_n(\widetilde{e}_{\widetilde{u},\widetilde{v}})\}$: set of edge weights;

P_n: chain of $\widetilde{G}_n$ such that the source node s is the least ordered node and d is the greatest ordered node;

$W(\widetilde{P}_n)$: $\sum_{\widetilde{e}_{\widetilde{u},\widetilde{v}} \in \{\widetilde{P}_n\}} \widetilde{e}_{\widetilde{u},\widetilde{v}}$: the weight of the path $\widetilde{P}_n$ (the sum of the weights of all the edges in the chain;

$W_{s,d}$ = weight of the shortest path between s and d;

$\widetilde{c}_{u,v,b}$: p-cycle containing vertices u and v and edges corresponding to the mapping of b edges of the multigraph G;

$\widetilde{C}_{u,v,b} = \widetilde{c}_{u,v,b}$: set of all p-cycles containing vertices u and v and edges corresponding to the mapping of b edges of the multigraph G;

$\widetilde{C}$: set of all established p-cycles;

$P_1 \oplus P_2$: concatenation of paths P_1 and P_2

V. THE RSA-FLEX ALGORITHM

Similar to the routing and wavelength assignment problem (RWA) in fixed-grid WDM networks, solutions for the routing and spectrum assignment problem (RSA) in flexgrid optical networks are needed to efficiently accommodate traffic demands. Besides the spectrum continuity constraint that imposes the allocation of the same spectrum in each fiber along the route of a lightpath, in an RSA formulation, slots (carrier) must be contiguously allocated in the spectrum (the spectrum contiguity constraint).

It has been proved that the Routing and Spectrum Allocation problem is an NP-hard problem and heuristics are needed to solve the problem. The proposed algorithm models the spectrum availability in the network as labeled multigraph. A multigraph is a graph which can have multiple edges (also called "parallel edges"), that is, edges that have the same end vertice. In this auxiliary graph, vertices represent OXCs and edges the slots in the link connecting OXCs. All vertices are connected by N edges which is the number of slots in the spectrum of each network link. The label on an edge represent the slot availability. An ∞ value means that the slot is already allocated whereas the value 1 means that the slot is available for allocation. These values were defined to facilitate the employment of traditional shortest path algorithms.

The multigraph is transformed into $N-b+1$ graphs where b is the bandwidth demand in slot of the requested channel. These graphs are generated by fixing an edge of the multigraph and considering the b consecutive edges to the fixed edge. This set of b edges of the multigraph are mapped onto a single edge of the generated graph. Its weight is given by applying a specific weight function that considers the b edges. Figure 2 illustrates the multigraph representing the spectrum and one of the generated graph. For each of the generated graphs, a shortest path algorithm is executed and the chosen path is the one that has the lowest weight among all shortest paths found.

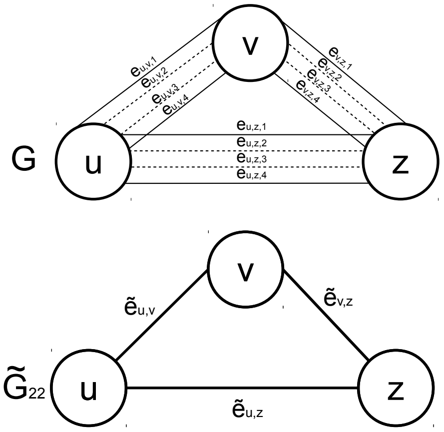


Figure 2: Multigrapgh representation of the network spectrum

For a demand of b slots, $N-b+1$ graphs of type $\widetilde{G}_{n,b}$ will be generated, each edge of the $\widetilde{G}_{n,b}$ graph corresponds to the mapping of b edges of G starting on the n^{th} edge of G. Since the same ordered edges connecting any two nodes in G are mapped onto edges of $\widetilde{G}_{n,b}$, the spectrum continuity is assured.

Algorithm 1 RSA-Flex

```
1: $\forall n = 1 ... N-b$
2:     $(W(P_n), P_n) = ShortestPath(\widetilde{G}_{n,b}, r(s,d,b))$
3: $W_{s,d} = W(P_n) | \ \forall i \ W(P_n) \leq W(P_i)$
4: if $W_{s,d} = \infty$ then
5:     $block \ r(s,d,b)$
6: else
7:     $W(e_{u,v,i}) = \infty \quad \forall \{u,v\} \in \widetilde{P}_i \quad n = n ... i+b-1$
8: end if
```

Algorithm 1 details the RSA-Flex Algorithm. In this algorithm, Line 1 establishes all the set of edges that will be mapped onto $\widetilde{G}_{n,b}$ edges. Line 2 solves a shortest path algorithm for the graph $\widetilde{G}_{n,b}$ and provides the path and its weight. If the weight of the shortest path is ∞, it was not possible to find a path under the contiguity constraint for the demand b with allocation starting with the n^{th} slot. Line 3 selects the path among the $N-b+1$ shortest paths that has the lowest weight value. In case the weight of all shortest path is ∞ (Line 4), there is no path in the network that satisfies the request of b slots under the contiguity constraint. Therefore, the request has to be blocked (Line 5). Otherwise, the shortest path with the lowest value is chosen (Line 7) and the corresponding edges in the multigraph G have their weight changed to ∞ (Line 8) meaning that the slots were allocated to the newly established lightpath.

Since the RSA-Flex Algorithm executes a shortest path algorithm $N - b$ times and considering the use of the Djkstra Shortest Path algorithm, the computational complexity of the proposed algorithm is $N \cdot (|V| + |E|) \cdot \log(|V|)$.

VI. FIPP-FLEX ALGORITHM

The algorithm introduced in this section, called FIPP-Flex decides on the establishment of lightpaths in an FIPP p-cycle protected network. A lightpath is established if and only if it can be protected by an FIPP p-cycle which can have both on-cycle and straddling links. An FIPP p-cycle protects disjoint primary paths. Requests to lightpath establishment arrive dynamically and for each request an existing p-cycle is searched to protect the potential lightpath. In case no existing p-cycle can protect the potential lightpath then a path is searched to create a new p-cycle for the request. If no path can protect the lightpath then it is not established. The FIPP-Flex algorithm assures a protection path for each established lightpath and the protection is guaranteed for single failures.

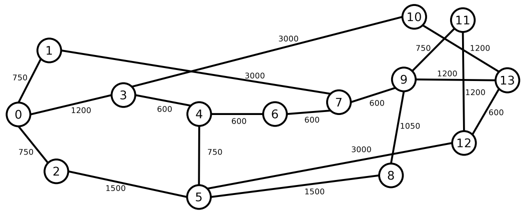
Algorithm 2 FIPP-Flex

```
1:  $(W(P_n), P_n) = RSA - Flex(G, s, d, b)$
2:  if $W_{s,d} = \infty$ then
3:      $block\ r(s, d, b)$
4:  else
5:      if $C_{u,v,i} \neq \emptyset \forall i \geq b$ then
6:          establish $r(s, d, b)$ as $P_n$
7:      else
8:          $(W(P_1), P_1)$ = RSA-Flex $(G, r(s, d, b))$
9:          $(W(P_2), P_2)$ = RSA-Flex $(G, r(s, d, b))$ | $P_1 \bigcap P_2 = \emptyset$
10:         if $W(P_1) = \infty$ or $W(P_2) = \infty$ then
11:             block $r(s, d, b)$
12:         else
13:             establish $r(s, d, b)$ as $P_n$
14:             establish $P_1$ and $P_2$
15:             $\widetilde{c}_{u,v,b}$ = $P_1 \oplus P_2$
16:         end if
17:     end if
18: end if
```

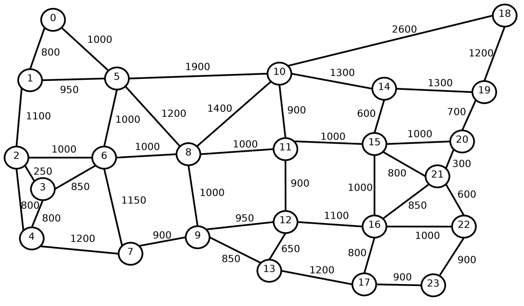
Line 1 tries to find a path to establish the request $r(s, d, b)$. If there is no path available (Line 2) then the request is blocked (Line 3). Otherwise, a p-cycle to protect the lightpath to be established is searched (Line 5). In case, there exists a p-cycle, the lightpath is established. Otherwise, a p-cycle to protect the lightpath to be established should be created (Lines 8 and 9). In case, no p-cycle can be created to protect the lightpath then the request is blocked (Line 1), otherwise the lightpath (Line 13) as well as the p-cycle (Lines 14 and 15) are established to satisfy the request.

VII. PERFORMANCE EVALUATION

To assess the performance of the FIPP-Flex algorithm, simulation experiments were employed and results compared to those of networks without any protection scheme as well to those produced by SPP-OFDM-Aggressive and survivable-FWDM protection algorithm. Both FIPP-Flex and SPP-OFDM-Aggressive provide shared backup path protection. The difference between the results given by these two algorithm can be attributed to the advantage of having a pre-connected scheme (FIPP-Flex). The FlexGridSim [9] simulator was used. In each simulation, 100,000 requests were generated and simulations for each algorithms used the same set of seeds. Confidence intervals with 95% confidence level were generated. The NSF (Figure 3a) and the USA (Figure 3b) topologies were used. The NSF topology has 16 nodes and 25 links whereas the USA topology has 24 nodes and 43 links. In the simulated network, the spectrum was divided in 240 slots of 12,5 GHz each.



(a) NSF Topology



(b) USA Topology

Figure 3: Topology

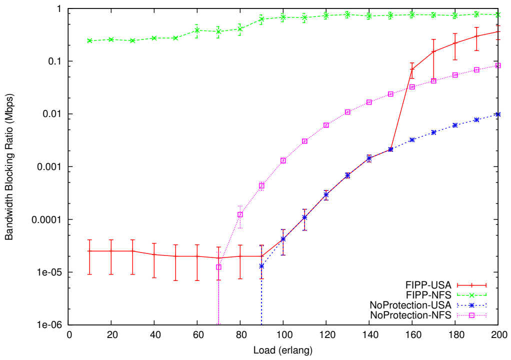


Figure 4: Bandwidth Blocking Ratio

Figure 4 plots the bandwidth blocking ratio (BBR) for networks without any protection and networks with p-cycle protection. The label "NoProtection" means there is no protection scheme in the network and the labeled "FIPP" means network protected by a p-cycle scheme. For the USA topology, the BBR is quite low until loads of 90 erlangs when the network with no protection starts blocking. The BBR for the two networks are very similar until loads of 140 erlangs. This low overhead for the provisioning of 100% protection is due to the large number of available paths in the USA topology. Therefore, up to this load protection is guaranteed with minimal overhead. After that, the difference in BBR starts increasing and it can be of two orders of magnitude for highly loaded networks. For the NSF network, the picture looks quite different since the difference in BBR can be of four order of magnitude under moderately loaded networks. Under heavy loads this difference drops to less than two orders of magnitude due to the large blocking in the NSF topology.

Figure 5 compares the number of p-cycles and primary paths established. It can be seen that the number of primary paths in the USA topology is one order of magnitude higher than the number of p-cycles while such relation is of two orders of magnitude for the NSF networks. Since blocking in the NSF network is high, there is a tendency to establish protected lightpaths only for a reduced number of p-cycles. This tends to increase the sharing of p-cycles. In the USA topology, a higher number of p-cycles with heterogeneous capacity is established and p-cycles tend to be shared by a lower number of primary paths.

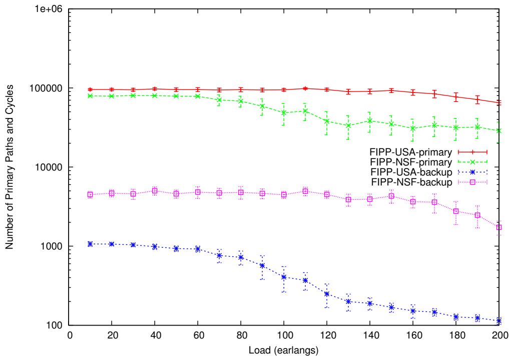


Figure 5: Number of Primary Paths and Cycles

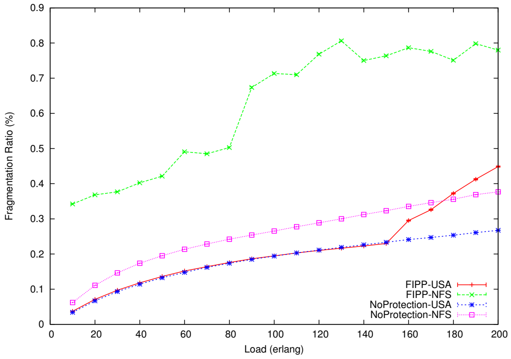
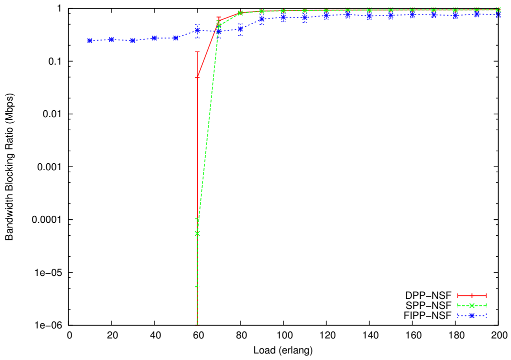


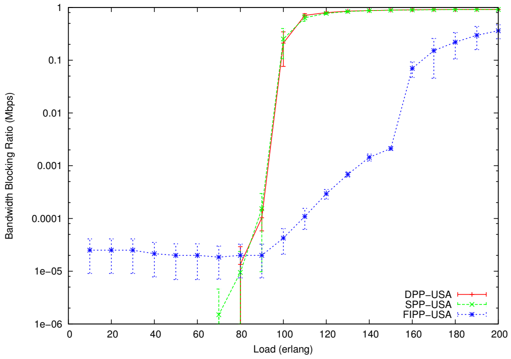
Figure 6: Fragmentation Ratio (%)

Figure 6 depicts the Fragmentation Ratio as function of the load. In flexgrid networks, the establishment and tear down of lightpaths leads to the fragmentation of the spectrum which is a state in which there are available slots, but not gathered in a way that can be used to accept new requests. The fragmentation ratio is defined as the average ratio between the number of types of demands that cannot be accepted to the total number of types of demands. For the USA topology, there is not much difference between the fragmentation ratios for networks with and without protection. The difference arises only under heavy load. However, for the NSF topology, the difference in fragmentation ratio is quite significant and this is a consequence of blocking due to the low number of alternative paths.

Next, results produced by the FIPP-Flex algorithm will be compared with those given by the survivable-FWDM algorithm and with those produced by the SPP-OFDM-Aggressive algorithm. The SPP-OFDM-Aggressive algorithm also provide SBPP protection and the difference of results given by this algorithm and those given by FIPP-Flex is due the pre-connected protection provided by the FIPP-Flex algorithm. The SPP algorithm uses a k-shortest path algorithm and the First-Fit policy to allocate subcarriers. The subcarriers allocated to the primary path are removed from the auxiliary graph and the k-shortest path is executed to determine the backup paths. The DPP algorithm construct an auxiliary graph in which edges represent available slots. It finds k pairs of disjoint paths and chooses a pair to be the primary and backup paths. In the figures, curves labeled "DPP" show the results for networks using the survivable-FWDM algorithm [1], while curves labeled "SPP" display the results for networks using the SPP-OFDM-Aggressive algorithm [2]. The curves labeled "FIPP" plots results for the network using the FIPP-Flex algorithm described in section VI.



(a) NSF Topology

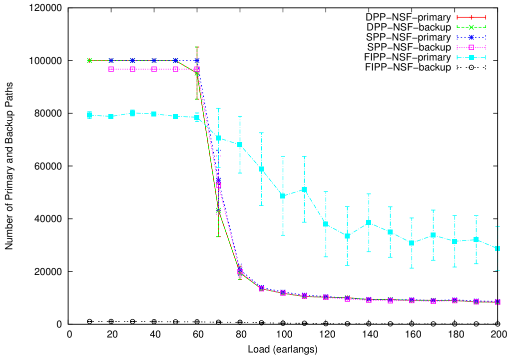


(b) USA Topology

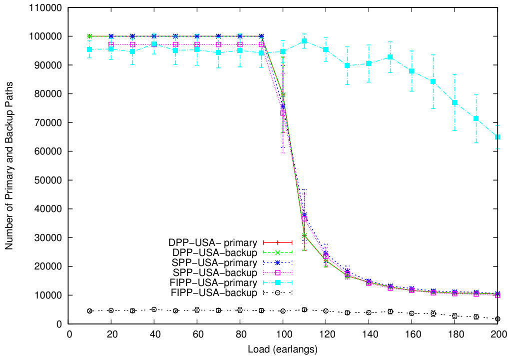
Figure 7: Bandwidth Blocking Ratio

Figure 7 shows the bandwidth blocking ratio as a function of the load. SPP and DPP produce similar BBR values, which have a typical pattern: whenever the network saturates the BBR reaches its maximum value. While there was no blocking until loads of 60 erlangs in the NSF network, for higher loads the BBR is a slightly higher than that given by FIPP-Flex with the disadvantage that the backup path is not pre-connected. For the USA topology, the behavior of SPP and DPP is quite similar to that of the NFS network. However, FIPP-Flex takes advantage of the high connectivities of nodes in the USA topology and the BBR increases smoothly as a function of the load increase. The BBR values produced by FIPP-Flex is lower than those given by SPP and DPP after the network saturates.

Figure 8 shows the number of primary and backup paths allocated by using different algorithms. The number of primary paths allocated by the FIPP-Flex algorithm is one order of magnitude higher than the number of backup paths due to the capacity of sharing paths promoted by the FIPP-Flex algorithm. Actually any paths connecting a pair of nodes along the backup path can share the backup path. The number of primary and backup paths produced by the other two algorithms are quite similar and shows low capacity of sharing paths.



(a) NSF Topology



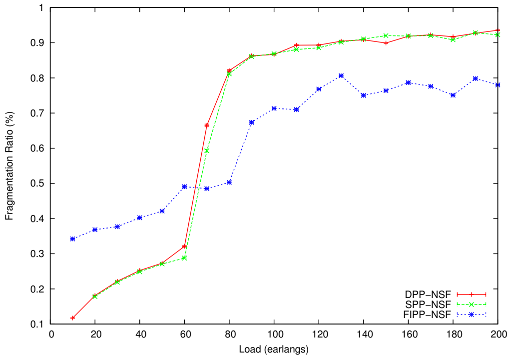
(b) USA Topology

Figure 8: Number of Primary and Backup Paths

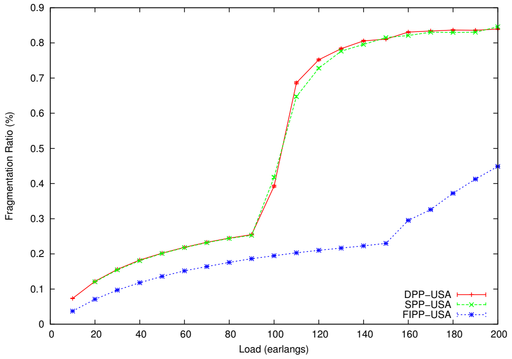
Figure 9 shows the fragmentation ratio as a function of the load. The fragmentation ratio of SPP and DPP have a similar trend than that of the bandwidth blocking ratio which was already expected since the fragmentation ratio influence the blocking of request. FIPP produces considerable lower fragmentation ratio for the USA topology due to the higher number of available paths.

VIII. CONCLUSIONS

This paper introduced an algorithm to support the establishment of lightpaths in flexgrid networks protected by FIPP p-cycles. The p-cycle method benefits from the fast restoration of ring-like protection and high capacity efficiency of mesh protection. The algorithm was evaluated for different topologies and loads. The FIPP-Flex algorithm provides 100% protection for single failures. Results indicated that the overhead demanded by the FIPP-Flex algorithm is quite acceptable for networks with high node connectivities (USA) but it is not so attractive to networks with low node connectivities (NSF). Moreover, when compared to the SPP-OFDM-Aggressive and survivable-FWDM algorithms, the FIPP-Flex algorithm produce more attractive results specially for the USA topology besides being a pre-connected scheme. As future work different modulation schemes and physical impairments will be considered in the RSA-Flex algorithm.



(a) NSF Topology



(b) USA Topology

Figure 9: Fragmentation Ratio (%)

REFERENCES

[1] A. Patel, P. Ji, J. Jue, and T. Wang, "Survivable transparent flexible optical WDM (FWDM) networks," in *Optical Fiber Communication Conference and Exposition (OFC/NFOEC), 2011 and the National Fiber Optic Engineers Conference*, 2011, pp. 1–3.

[2] X. Shao, Y.-K. Yeo, Z. Xu, X. Cheng, and L. Zhou, "Shared-path protection in OFDM-based optical networks with elastic bandwidth allocation," in *Optical Fiber Communication Conference and Exposition (OFC/NFOEC), 2012 and the National Fiber Optic Engineers Conference*, 2012, pp. 1–3.

[3] M. Liu, M. Tornatore, and B. Mukherjee, "Survivable traffic grooming in elastic optical networks shared protection," *Lightwave Technology, Journal of*, vol. 31, no. 6, pp. 903–909, 2013.

[4] R. Asthana, Y. Singh, and W. Grover, "p-cycles: An overview," *Communications Surveys Tutorials, IEEE*, vol. 12, no. 1, pp. 97 –111, quarter 2010.

[5] M. Kiaei, C. Assi, and B. Jaumard, "A survey on the p-cycle protection method," *Communications Surveys Tutorials, IEEE*, vol. 11, no. 3, pp. 53 –70, quarter 2009.

[6] D. Schupke, W. Grover, and M. Clouqueur, "Strategies for enhanced dual failure restorability with static or reconfigurable p-cycle networks," in *Communications, 2004 IEEE International Conference on*, vol. 3, june 2004, pp. 1628 – 1633.

[7] Schupke, "Analysis of p-cycle capacity in wdm networks," *Photonic Network Communications*, pp. p. 41–51, 2006.

[8] A. Kodian and W. Grover, "Failure-independent path-protecting pcycles: efficient and simple fully preconnected optimal-path protection," *IEEE J. Lightwave Technol.*, vol. 23, pp. 3241–3259, Oct. 2005.

[9] P. M. Moura and A. C. Drummond, "FlexGridSim: Flexible Grid Optical Network Simulator," http://www.lrc.ic.unicamp.br/FlexGridSim/.