Extending node protection concept of p-cycles for an efficient resource utilization in multicast traffic

Ahmed Frikha, Bernard Cousin, Samer Lahoud

Extending Node Protection Concept of P-Cycles for an Efficient Resource Utilization in Multicast Traffic

Ahmed Frikha, Bernard Cousin, and Samer Lahoud
University of Rennes 1, IRISA, 35042 Rennes Cedex, France
Email:{ahmed.frikha,bernard.cousin,samer.lahoud}@irisa.fr

Abstract—In this paper, we consider link-and-node failure recovery in dynamic multicast traffic in WDM networks. We extend the node protection concept of the p-cycle approach to achieve more efficient resource utilization. Then, we propose a novel algorithm that integrates our concept for the node protection, named node-and-link protecting p-cycle based algorithm (NPC). We also propose a second algorithm, named node-and-link protecting candidate p-cycle based algorithm (NPCC). This algorithm deploys our concept for node protection and relies on a candidate p-cycle set to speed up the computational time. We compare our proposed algorithms to the ESHN algorithm, which is reported to be the most efficient algorithm for protecting dynamic multicast sessions. Extensive simulations show that the NPC algorithm achieves the lowest blocking probability, but has the highest computational time among the NPCC and ESHN algorithms. The NPCC algorithm outperforms the ESHN algorithm in terms of resource utilization efficiency and computational time.

I. INTRODUCTION

Optical network survivability becomes indispensable with the emerging wavelength-division multiplexing (WDM) technologies such as the DWDM technology. Particularly, for optical multicast sessions, a link-or-node failure has a severe impact as it can prune several communications simultaneously. The p-cycle protection approach, introduced by W.D. Grover [1], ensures node-and-link failure recovery while maintaining a fast restoration time and an efficient use of the network capacity compared to the other protection approaches. Up to now, most of existing researches in optical multicast traffic focus on link failure recovery and rarely on node failure recovery. Although node failures are less frequent than link failures, node failures may cause the disruption of multiple communications, especially when the failed node is a splitting node for multicast sessions. In 2009, F. Zhang and W.D. Zhong proposed the efficiency-score based heuristic algorithm of node-and-link protecting p-cycle (ESHN) [2]. Although the ESHN algorithm has the lowest blocking probability among the OPP-SDP algorithm [3] and the ESHT algorithm [4] in dynamic multicast traffic, ESHN does not use efficiently the protection capacity provided by a p-cycle, especially when protecting nodes. Precisely, the ESHN algorithm does not take in consideration all nodes that a p-cycle can protect, when selecting a protecting p-cycle. This is due to the two hard constraints imposed by the concept deployed by ESHN for protecting nodes. The first constraint imposes that a node protecting p-cycle has to link all one level downstream nodes of the failed node. The second constraint imposes that the p-cycle must contain one of the upstream nodes of the failed node in the light tree. Of course this concept reduces the

computation time of the algorithm as it limits the search space of the p-cycles. However, it prevents the ESHN algorithm to achieve the best resource utilization. Furthermore, when traffic load is high, the computational time of the ESHN algorithm remains high and does not deal with a dynamic multicast traffic.

In this paper, we consider link-and-node failure recovery in dynamic multicast traffic. We extend the node protection concept of the p-cycle approach to achieve more efficient resource utilization. We propose a novel algorithm, named node-and-link protecting p-cycle based algorithm (NPC). The NPC algorithm integrates our proposed concept for the node protection. This algorithm ensures node-and-link failure recovery. We also propose a second algorithm, named node-and-link protecting candidate p-cycle based algorithm (NPCC). The NPCC algorithm deploys our concept for node protection and is based on a candidate p-cycle set to overcome the high computational time problem.

II. EXTENDING THE NODE PROTECTION CONCEPT

In this section, we first present some existing well-known concepts for node protection using p-cycles. Then, we present our novel concept for protecting nodes in multicast traffic.

A. Existing approaches for node protection using p-cycles

The node encircling p-cycle concept (NEPC) [5] has been proposed for node protection using p-cycles. This concept imposes that a protecting p-cycle of a given node must link all neighbor nodes of the failed node, to protect it. However, there are some cases where such a p-cycle does not exist. The constraint imposed by this concept is very hard and prevents the algorithms to achieve good resource utilization. Some existing works that ensure link-and-node failure recovery in multicast session simplify the node protection concept to reduce the computational time of the algorithm. For example, in the ESHN algorithm, the p-cycle has to link 1) all one level downstream nodes of the failed node and 2) one of its upstream nodes in the light tree. These two constraints make finding a protecting p-cycle for a node difficult and do not allow the protection capacity of a p-cycle to be used efficiently. Fig. 1 illustrates a simple example for protecting a node using the ESHN algorithm.

B. The proposed concept for node protection using p-cycles

Let us introduce some notations before presenting our concept. Let T be a multicast light tree to be protected, N_f be an intermediate node in T, and $D = \{d_1, d_2, .., d_i\}$ be the set of
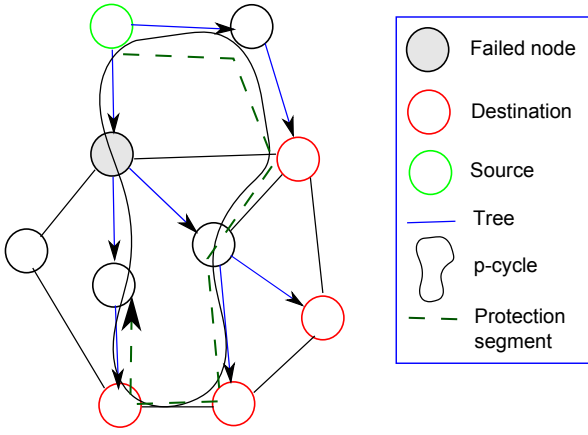
Fig. 1.   Protecting a node using the ESHN algorithm

destinations of T that are affected when a failure occurs on the node N_f. A p-cycle C of the network can protect the node N_f if and only if it exists a protection segment $[N_a, N_e] \in C$ such that:

1) N_a is not affected by the failure of N_f.
2) $\forall d_j \in D, \exists N_j \in [N_a, N_e]$ and $N_j \in]N_f, d_j]$, where $]N_f, d_j]$ is a segment of T.
3) $N_f \notin [N_a, N_e]$.

Note that N_a is the node which activates the p-cycle when a failure on the node N_f occurs. This node must inject the muticast traffic in the p-cycle upon the failure of N_f. Therefore, this node must not be affected by the failure of N_f, i.e. N_a continues to receive the multicast traffic even if a failure occurs on node N_f. Constraint 2) ensures that all destinations affected by the failure of N_f continue to receive the multicast traffic through the protection segment $[N_a, N_e]$. The protection segment can route the multicast traffic directly to the affected destinations in D or through an intermediate node N_j ancestor of the destination and descendant of N_f in the ligh tree T. Constraint 3) ensures that the protection segment $[N_a, N_e]$ is not affected by the failure of N_f. Fig.2 illustrates an example of a p-cycle that can protect the node N_f using our concept.
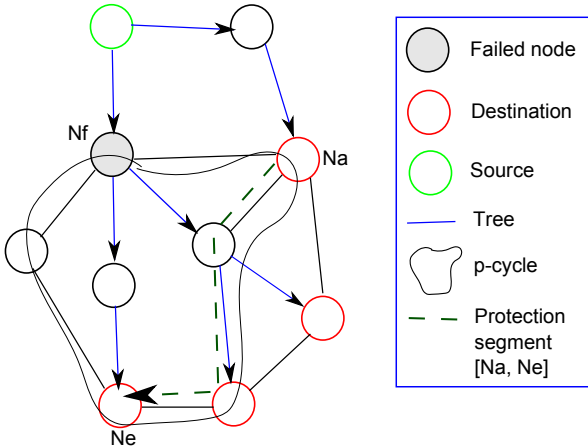

Fig. 2.   Protecting a node using the proposed concept

III. THE PROPOSED ALGORITHMS

In this section, we present two novel algorithms for combined node-and-link failure recovery. Our algorithms deploy the afore-mentioned concept for node protection.

A. The NPC algorithm

Fig. 3 presents the flow chart of the NPC algorithm. Let us introduce some notations before detailing the operation performed by this algorithm. Let us consider a multicast request and its corresponding light-tree T. Let L denote the unprotected working link capacity of T, N denote the unprotected intermediate node transit capacity of T. The amount of working link capacity that can be protected by the existing p-cycles in the network is subtracted from L and the amount of protected node transit capacity is subtracted from N. Note that the existing p-cycles are previously established to protect other light trees in the network. If $L \neq \phi$ or $N \neq \phi$, the algorithm computes new p-cycles to protect the remaining unprotected link capacity in L as well as the remaining unprotected node transit capacity in N. To select a new protecting p-cycle, the algorithm uses the ES-based unity-p-cycle procedure. In this procedure, we deploy the same efficiency-score (ES) used in the ESHN algorithm to measure the efficiency of the p-cycles in the network. Note that this score adapts the efficiency-ratio based unity-p-cycle heuristic algorithm (ERH) [6] to deal with node-and-link failures in multicast traffic. This score takes in consideration the largest amount of unprotected node transit capacity as well as the largest amount of unprotected working link capacity of the multicast tree that a unity-p-cycle can protect. A unity-p-cycle is a p-cycle in the network that reserves only one bandwidth unity (e.g. one wavelength) on each traversed link. Let C_j be a unity-p-cycle in the network. The score ES of C_j is given by equation (1), where $W_{j,L}$ is the largest amount of unprotected link capacity in L that C_j can protect, $W_{j,N}$ is the largest amount of unprotected node transit capacity in N that C_j can protect, and $|C_j|$ is the spare capacity required for setting up a unity-p-cycle C_j. $|C_j|$ is given by the number of links traversed by C_j.

$$ES(C_j) = \frac{W_{j,L} + W_{j,N}}{|C_j|} \qquad (1)$$

The ES-based unity-p-cycle procedure calculates the score ES of each unity-p-cycle and selects the p-cycle with maximum ES. The amount of working link capacity protected by the selected unity-p-cycle is subtracted from L and the amount of protected node transit capacity is subtracted from N. This process is iterated until the amount of working link capacity in L and the amount of node transit capacity in N are protected, i.e. $L = \phi$ and $N = \phi$. The selected unity-p-cycles are configured and the corresponding wavelengths are reserved. Note that the reserved p-cycles may serve to protect next coming multicast requests. This is why after routing a multicast tree, we compute the amount of working link capacity in L and the amount of node transit capacity in N that can be protected by the existing p-cycles in the network. Note that the reserved capacity of an existing p-cycle in the network is released when the p-cycle does not protect any working link capacity and any node transit capacity in the network.
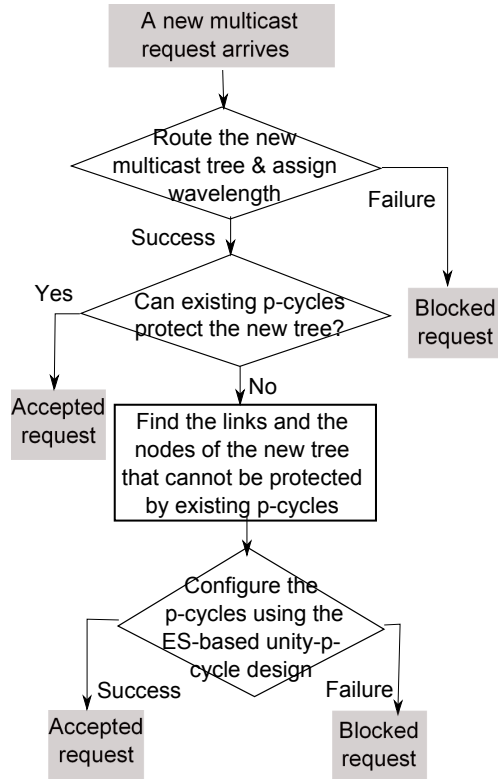
Fig. 3. Flow chart of the NPC and the NPCC algorithms for combined link-and-node failure recovery in dynamic multicast traffic

B. The NPCC algorithm

The NPCC algorithm has the same flow chart of the NPC algorithm, except that it applies the ES-based unity-p-cycle procedure on a candidate p-cycle set instead of applying it on the total p-cycle set. At each iteration of the ES-based unity-p-cycle procedure, the algorithm selects the p-cycle with maximum ES among the candidate p-cycle set. This will reduce considerably the computational time of the algorithm. In fact, when the number of p-cycles in the network is high, computing the score ES of each p-cycle in the network is a very long task and affects the computational time of the procedure. Therefore, we select a set of candidate p-cycles to reduce the computational time of the procedure.

To select a candidate p-cycle set, we define a new score, named protection capacity PC, for each p-cycle in the network. This score is computed in advance for each p-cycle before routing the requests. The score PC of a unity-p-cycle C_j, specified by equation (2), is defined as the ratio of the largest amount of link capacity on the network LC_j that C_j can protect over the sum of spare capacity required by C_j.

$$PC(C_j) = \frac{LC_j}{|C_j|} \qquad (2)$$

A p-cycle with a high PC, is useful as it maximizes the amount of protected capacity while reserving less spare capacity. The l p-cycles with highest PC are selected as candidate p-cycle set, where l is a parameter for the algorithm. The goal of selecting this set is to maximize the capacity that can be protected on the network, and this will help to protect the next

coming requests. The NPCC algorithm consists in using the l selected p-cycles as a candidate p-cycle set instead of using all p-cycles in the network.

IV. PERFORMANCE EVALUATION

In this section, we evaluate our proposed algorithms NPC and NPCC for combined link-and-node failure recovery in dynamic multicast traffic, by comparison with the ESHN algorithm. As mentioned before, the ESHN algorithm was reported to be the most efficient algorithm for dynamic multicast traffic protection in terms of resource utilization efficiency and blocking probability. For simulating dynamic multicast traffic, we assume that the multicast request arrival follows a Poisson process with an average arrival rate λ, and the multicast request holding time follows an exponential distribution with an average holding time μ. Hence, the network offered traffic load is given by $\lambda\mu$. We run simulations on the following well known European optical topologies:

- The COST-266 core topology [7]: contains 16 nodes and 23 links. The total number of p-cycles in this topology equals 236 (118 p-cycles in each direction).
- The COST-239 topology [8]: contains 11 nodes and 26 links. The total number of p-cycles in this topology equals 5058 (2029 p-cycles in each direction).

Without lack of generality we assume in our study that each link has two fibers. The two fibers transmit in opposite directions; 16 wavelengths are available on each fiber. The source and the destinations of each multicast session are randomly selected among any node in the network (uniform distribution law). We choose the number of destinations in each multicast request $D = 5$ as the total number of nodes in the used topologies is lower than 16 nodes. We compare the performance of the algorithms according to the blocking probability (BP) as well as the average computational time (CT) required for routing and protecting a traffic request. Performance criteria BP and CT are computed function of the traffic load. For each traffic load value, 10^5 requests are generated. This number of requests is enough to measure BP and CT, with a 95% confidence interval.

First, we consider the COST-266 topology. The total number of p-cycles in this topology equals 236 p-cycles. We choose the number of candidate p-cycles $l = 100$ for the NPCC algorithm. Fig. 4 illustrates the blocking probability measured in the COST-266 network. The ESHN algorithm has a blocking probability very high compared to that of our proposed algorithms NPC and NPCC. The NPCC algorithm has a blocking probability very close to that of the NPC algorithm. This is due to the number of candidate p-cycles which is not very low compared to the total number of p-cycles in the network.

The blocking probability comparison measured on the COST-239 network is represented in Fig. 5. Note that, for the NPCC algorithm, we select the number of candidate p-cycles $l = 500$ in the COST-239 network. This number is very low compared to the total number of p-cycles in the COST-239 network which is equal to 5058 p-cycles. The figure illustrates the variation
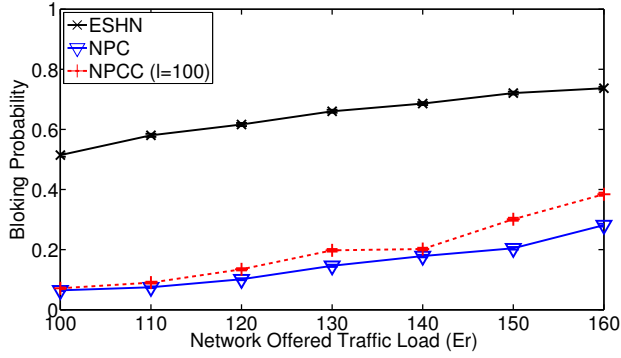
Fig. 4. Comparison of the blocking probability BP in COST-266 network.

Fig. 6. Comparison of the average computational time CT for setting up a multicast request in COST-239 network.

of blocking probability of each algorithm according to the network offered traffic load. For all the algorithms, the blocking probability of the algorithms increases when the traffic load is high. The NPC algorithm has a blocking probability very low compared to the ESHN algorithm. The blocking probability of our algorithm NPC does not exceeds 20% when traffic load is lower than 190 Erlang, while the ESHN algorithm has a blocking probability higher than 60% for the same traffic load value. The NPCC algorithm outperforms the ESHN algorithm having a blocking probability very low, especially when traffic load is not very high. The NPC algorithm has a blocking probability lower than that of NPCC. This is due to the low number of candidate p-cycles considered for the protection in the NPCC algorithm.
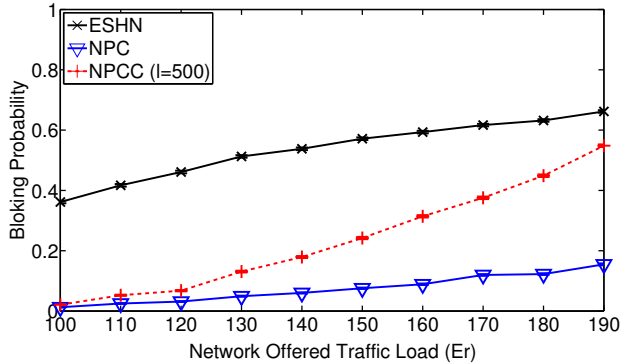

Fig. 5. Comparison of the blocking probability BP in COST-239 network.

To assess the rapidity of our proposed algorithms, we focus on the average computational time CT for setting up a multicast request. Fig. 6 illustrates the value of CT of each algorithm, measured in COST-239 network according to the network traffic load. As shown in this figure, the NPCC algorithm has the lowest computational time among the NPC and the ESHN algorithm, this is due to the low number of p-cycles considered for the protection. The average computational time CT of the NPCC algorithm is lower than 25 ms, while it is higher than 35 ms for the ESHN algorithm. The NPCC algorithm outperforms the ESHN algorithm in terms of Blocking probability and computational time. The computational time of the NPC algorithm is higher than that of ESHN. However, the NPC algorithm has a very low blocking probability compared to ESHN.
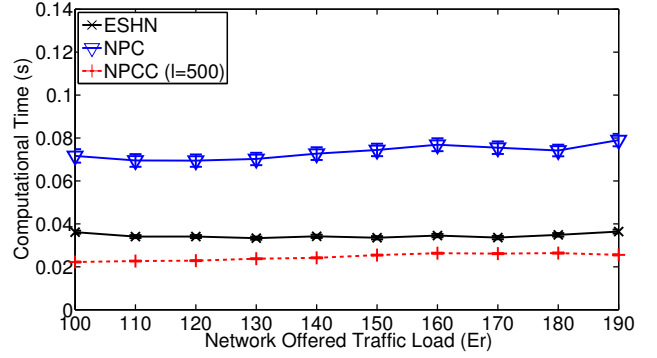
V. CONCLUSION

In this paper, we extended the concept of node protection of p-cycle approach in optical multicast traffic. Our novel concept allows the protection capacity provided by a p-cycle to be used efficiently. We proposed a novel algorithm, named NPC, which deploys our concept for the node protection. The NPC algorithm ensures both link and node failure recovery for a dynamic multicast traffic. We also proposed a second novel algorithm, named NPCC, based on our concept for the node protection. This algorithm speeds up the computational time of setting up a multicast traffic request by enumerating a set of candidate p-cycles. We compared our proposed algorithms with the ESHN algorithm, which was reported to be the most efficient algorithm for node-and-link failure recovery in dynamic multicast traffic. Extensive simulations showed that the NPC algorithm achieves the lowest blocking probability, but has the highest computational time among the NPCC and ESHN algorithms. The NPCC algorithm outperforms the ESHN algorithm in terms of resource utilization efficiency and computational time.

REFERENCES

[1] W. D. Grover and D. Stamatelakis, Cycle-oriented distributed preconfiguration: ring-like speed with mesh-like capacity for self-planning network restoration, *in proceedings of IEEE ICC,* 1998.
[2] F. Zhang and W. D. Zhong, Performance evaluation of optical multicast protection approaches for combined node and link failure recovery, *J. Lightw Technol.,* vol. 27, no. 18, pp. 4017-4025, 2009.
[3] N. K. Singhal, L. H. Sahasrabuddhe, and B. Mukherjee, Provisioning of survivable multicast sessions against single link failures in optical WDM mesh networks, *J. Lightw. Technol.,* vol. 21, no. 11, pp. 2587-2594, 2003.
[4] F. Zhang, and W. D. Zhong, p-Cycle based tree protection of optical multicast traffic for combined link and node failure recovery in WDM mesh networks, *IEEE Commun. Lett.,* vol. 13, no. 1, pp. 40-42, 2009.
[5] J. Doucette, P. A. Giese, W. D. Grover, Combined Node and Span Protection Strategies with Node-Encircling p-Cycles, *in proceedings Workshop on Design of Reliable Communication Networks (DRCN), Ischia (Naples), Italy,* pp. 213-221, 2005.
[6] Z. R. Zhang, W. D. Zhong, and B. Mukherjee, A heuristic method for design of survivable WDM networks with p-cycles, *IEEE Commun. Lett.,* vol. 8, pp. 467-469, 2004.
[7] S. De Maesschalck and al., Pan-European Optical Transport Networks: an Availability based Comparison, *Photonic Network Communications,* Vol. 5, no. 3, pp. 203-226, 2003.
[8] P. Batchelor et al.: Ultra High Capacity Optical Transmission Networks. *Final report of Action COST 239,* 1999.