Journal of Information and Operations Management
ISSN: 0976–7754 & E-ISSN: 0976–7762 , Volume 3, Issue 1, 2012, pp-57-60
Available online at http://www.bioinfo.in/contents.php?id=55

A SURVEY OF P-CYCLE FOR WDM NETWORKS

MANDEEP KAUR SANDHU AND AMIT KUMAR GARG

Maharishi Markandeshwar University Mullana, Ambala, India
*Corresponding Author: Email- mandeeepcheema@gmail.com

Received: December 12, 2011; Accepted: January 15, 2012

Abstract- Most current research activities in the field of optical multicast traffic protection are mainly directed to link failure recovery and (intermediate) node failure recovery. Even with the guarantee of link failure recovery and (intermediate) node failure recovery, optical multicast traffic is still threatened by the catastrophic damage of source failures. This paper provides a comprehensive review of p-cycle-based multicast protection approaches which offer much better performance compared with other shared multicast protection approaches. Various approaches like IpC, which achieves both fast restoration and high capacity ,two novel algorithms that integrate concept for the node protection, named NPC including spare capacity optimization of p-cycle based tree protection (SOPT) and segment protection (SOPS) are presented and also reviewed that 100% node and link failure recovery can be achieved at a small amount of additional capacity.
Keywords- P-cycle, multicast routing, node failure recovery, IpC, NPC, traffic protection, SOPS, SOPT

Citation: Mandeep Kaur Sandhu and Amit Kumar Garg (2012) A Survey of P-Cycle for WDM Networks. Journal of Information and Operations Management ISSN: 0976–7754 & E-ISSN: 0976–7762, Volume 3, Issue 1, pp– 57-60.

Introduction

Optical WDM networks provide a high bandwidth as it allows hundreds of wavelengths to be multiplexed into a single fiber. Therefore, it is important to maintain WDM network survivability since a single link-or-node failure would affect a large number of communication sessions. In multicast communications, this impact is more severe as a link-or-node may carry traffic for multiple destinations. Hence, protecting multicast sessions in WDM networks is a crucial task [1]. A single link failure costs more loss for multicast traffic than for unicast traffic, because that link may carry traffic to multiple destinations. Extensive research has been done on protection / restoration for unicast traffic, but not much work has been carried out for multicast traffic. Recently, due to the rapid growth of multicast applications, the problem of provisioning of survivable optical multicast sessions has started to draw more attention and research interests. Because of the predominance of link failure, most of the previously proposed multicast protection approaches mainly focus on link failure recovery. As shown in Fig.(1), most current multicast protection schemes can be classified into five major schemes: (i) tree-based protection approaches; (ii) Ring-based protection approaches; (iii) path-based protection approaches; (iv) segment-based protection approaches; (v) p-cycle-based protection approaches. Among them, tree based protection approaches were shown to be not so capacity-efficient, and not applicable to sparse networks [2]. Path/segment based protection approaches are more cost-effective, but their complicated signalling and configuration processes make failure recovery slow. Although ring based protection approaches are fast in recovery, their disadvantage is the inefficiency of resource utilization. p-cycle based protection approaches have been shown to be highly capacity efficient and fast in failure recovery for unicast traffic protection [3].

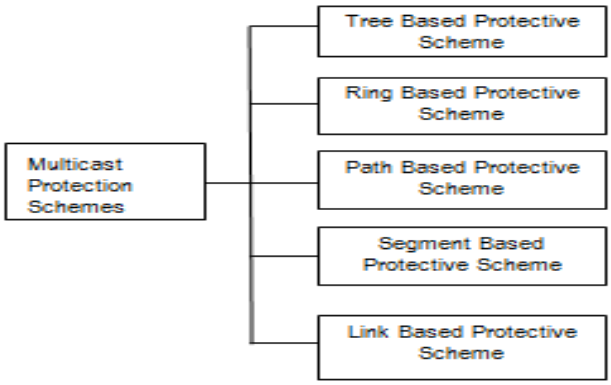


Fig. 1- Classification of Multicast protection schemes

In [4-7], p-cycle based multicast protection approaches have also been shown to be promising for link failure recovery and combined (intermediate) node and link failure recovery. Thus, most research work considered link and (intermediate) node failures but not source failures.

(intermediate) node failures, optical multicast traffic is still threatened by the catastrophic damage of source failures. In fact, source failure recovery is more important than failure recovery of any other node or link on a multicast tree, especially for real-time constrained multicast applications. Without an efficient, reliable and fast protection mechanism, a source failure can lead to severe disruption to all multicast sessions originating from the source node, and cause calamitous loss to both service providers and end customers. Thus, we recently investigated flow p-cycle based dual-source protection approach and optimal path pair based dual-source protection approach, for source failure recovery on top of combined node and link failure recovery [8]. Results showed that, the flow p-cycle based dual-source protection approach leads to lower total capacity consumption than optimal path pair based dual-source protection approach. Besides, p-cycle based approaches offer fast ring-like recovery speed because p-cycles are preconfigured [3, 6, 9].

P-Cycle Based Multicast Protection Scheme

In this study, all light trees and p-cycles are unidirectional, i.e., they are directed. We define one unit of capacity as one wavelength on a span (link), and denote a unity p-cycle as a directed p-cycle with one unit of capacity on every span [4]. A directed unity-p-cycle can protect one working unit in the opposite direction for every on-cycle span and two working units (one in each direction) for every straddling span. We extend all three strategies in [5] to dynamic provisioning of survivable multicast traffic. In strategy 1, all the existing p -cycles are released and then reconfigured upon the arrival of a new multicast request arrival Strategy 2 attempts to maximize the number of working units that can be protected by existing p-cycles and reconfigure new ones if the new multicast tree cannot be protected by the existing ones. Strategy 1 achieves a better blocking performance, while strategy 2 requires much less computational time. In Strategy 3, shown in Fig. 1, if the routing of a new light tree fails, it follows strategy 1; if succeeds, it follows strategy 2 (see [5] for more details). Strategy 3 achieves the best blocking performance and the computational time is close to that of Strategy 2. Hence, it is selected as our dynamic *p*-cycle design model for multicast traffic protection.

Flow P-Cycle Based Dual-Source Multicast Protection Approach

The flow p-cycle based dual-source multicast protection approach is divided into two steps: dual-source tree routing and flow p-cycle protection. In our study, a dual-source optical multicast session Φi is denoted as {si1, si2, di1 , di2 ,…, dik}, where si1 is the primary source, si2 is the backup source, di1 , di2 ,…, dik are the destinations, k (k ∈[1, N −2]) is the multicast group size. Dual-source tree routing is more complicated than single-source tree

routing, because five possible different types of dual-source multicast trees may be routed, as shown in Fig. 1. s 1 is the primary source, s2 is the backup source, d1, d2 , d3 and d4 are the destinations, and nodes 1, 2, 3 and 4 are intermediate nodes. A dual-source tree is referred as a parallel-dual-source tree, if the information flows from the two sources are parallel. The two trees shown in Fig. 1(a) and Fig. 1(b) are parallel-dual-source trees. The tree shown in Fig. 1(a) is referred as Type a, in which, there is a bridge node (B) which delivers the information flows from the two sources to the destinations. The tree shown in Fig. 1(b) is referred as Type b, where a bridge node cannot be identified but one or more bidirectional links can be set up such that the destinations can receive the information from either the primary source or the backup source via the bidirectional link(s). In contrast, a dual-source tree is referred as a serial-dual-source tree, if the information flow from one source to the destinations traverses the other source. The two trees shown in Fig (2) and are serial-dual-source trees. In the serial-dual-source tree, the terminal source is defined as the source without incoming flow; whereas the intermediate source is defined as the source at the downstream of the terminal source. The difference between the tree of Type and the tree is that, the primary source is the terminal source for the Type c tree while the backup source is the terminal source for the Type d tree. It is noted that, in serial-dual-source trees, the intermediate source should be on the main stem (the stem from the terminal source to the splitting node, e.g., s1 -1-s2, so that all destinations are the downstream nodes of both the terminal backup sources. If the two sources are too far apart, else if the routing is constrained by the network topology, a dual-source link-disjoint tree, which consists of two link-disjoint single source trees, may be routed for a dual-source multicast session, as shown in Fig. (2). This depicts a 1+1 dedicated protection approach, in which, no p-cycles are required to protect the link, intermediate node and source multicast session, as shown in Fig.(2).

Fig. 2- Types of dual-source multicast trees[4]

This depicts a 1+1 dedicated protection approach, in which, no p-cycles are required to protect the link, intermediate node and source failures, because the backup tree originated from the backup source can cope with all failures mentioned.

The Proposed Algorithms

a. Overview of lpC Scheme

A WDM optical network is represented by a graph *G*= (*V*, *E*), where *V* and *E* represent the sets of nodes and links, respectively. A multicast session *R* is de-noted as {*s*,*d*1,...,*dk*},where *s* is the source and *di* is the *i*th destination denotes the multicast tree associated with multicast session *R*. The set of all links on *T* is denoted as E_T and the set of all nodes on *T* is de-noted as *VT*. We use directed *p*-cycles to protect a multicast tree since multicast traffic is directed. A directed *p*-cycle can protect a directed link $u \rightarrow v$ if $u \rightarrow v$ is a straddling link of the *p*-cycle or the directed link $v \rightarrow u$ (not *uv*!) is on the *p*-cycle. In either case, the *p*-cycle segment from u to v can be used to route the traffic around the link uv when it fails. Given a multicast tree *T* and a *p*-cycle *c* that can protect some link (s) on *T*, we define the efficiency ratio (ER) of *c* as the ratio of |*PE* (*c*) |to |*c*|, where *PE (c*) denotes the set of links in E_T *that* are protected b *c*

and |c| denotes the number of links on *c*.Note that |*c* |is equal to the number of wavelength channels used by *c*. Clearly, the larger is ER, the more efficient is *c* in protecting the tree links. Given a multicast tree T, our Ipc algorithm, for-mally presented in Algorithm 1, is used to find a set PC of p-cycles to protect T so that every link in E_T is protected by some p-cycle in PC.The framework of the algorithm is as follows:

(1) For every link in E_T, there are two options to protect it: finding a new *p*-cycle for it, or extend-ing an existing *p*-cycle in *PC* to protect it.Hence, we can find at most 2*|*ET*| *p*-cycles for all links in E_T.

(2) Let *p* be the *p*-cycle with the maximum ER among all the *p*-cycles found in (1).We add *p* to *PC* and remove all links in *ET* that can be protected by *p*.

(3)We combine *p* with the other *p*-cycles in *PC* to reduce the wavelength usage of the *p*-cycles.

(4) If E_T becomes empty, PC is returned; otherwise, the above steps are repeated.

Three algorithms are used by I*p*C algorithm.Algorithm 2 and Algorithm 3 are used in Step(1) to com-pute a new *p*-cycle and an extended *p* cycle to protect a link in *ET* ,respectively. Algorithm 4 is used in Step (3) to combine *p* with the other *p*-cycles in PC.

b. The NPC algorithm

Fig. (3) presents the flow chart of the NPC algorithm. Some notations before detailing the operation performed by this algorithm is introduced. Then considered 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 φ or N =φ, 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 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) to deal with node-and-link failures in a 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 Cj be a unity-p-cycle in the network. The score ES of Cj is given by equation (1), where Wj,L is the largest amount of unprotected link capacity in L that Cj can protect, Wj,N is the largest amount of unprotected node transit capacity in N that Cj can protect, and |Cj| is the spare capacity required for setting up aunity-p-cycle Cj. |Cj| is given by the number of links traversed by Cj.

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

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 =φ and N =φ. 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 Land the amount of node transit capacity in N that can be protected by the existing p-cycles in the network. Note that there served 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.

c. 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[8].

$$PC(C_j) = (LC_j) \div |C_j| \quad (2)$$

A p-cycle with a high PC is useful as it maximizes the amount of protected capacity while reserving less spare capacity. The I p-cycles with highest PC are selected as candidate p-cycle set where 1 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 I selected p-cycles as a candidate p-cycle set instead of using all p-cycles in the network

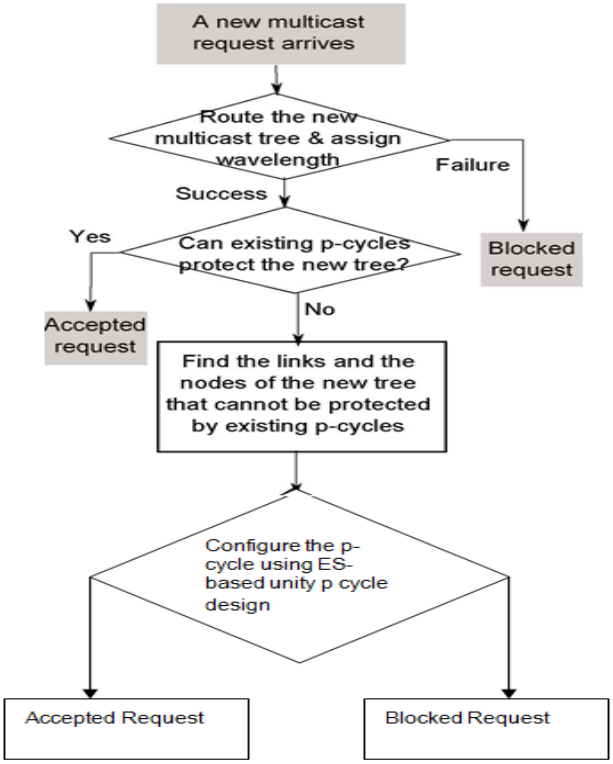
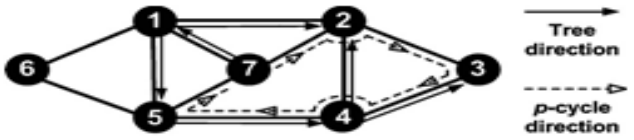


Fig. 3- Flow chart of the NPC and NPCC algorithms for combined link-and node failure recovery

d. SOP Design of p-Cycle-Based Tree Protection (SOPT)

In our SOPT design, only mutually link-disjoint trees can be protected by the same copy of a unity-p-cycle,as long as they are arc-disjoint with the cycle and their source, destination nodes are all on-cycle.This is to ensure that there is no contention for the same reserved spare capacity among the multicast trees. Upon detecting a single link failure in a multicast tree, node and the destination nodes of the disrupted tree perform the protection switching.As shown in fig. 4,the unity –p-cycle follows the direction of 2→3→4→5→7→2;the source,destination nodes of tree a and tree b can share this unity-p-cycle,because they are mutually link-disjoint with each other,and are also arc-disjoint with the cycle.Upon the failure on link 1-7,the traffic on tree a from node 7 to node 2 and 5 is disrupted,but the current p-cycle provides a protection path 7→2→3→4→5,which covers both the destination nodes of a tree a.



Tree	Tree topology	Source	Destinations
Tree *a*	$7 \rightarrow 1 \rightarrow \begin{cases} 2 \\ 5 \end{cases}$	7	{2,5}
Tree *b*	$5 \rightarrow 4 \rightarrow \begin{cases} 2 \\ 3 \end{cases}$	5	{2,3,4}

Fig. 4- Example of p-cycle-based tree protection

e. SOP Design of P-Cycle-Based Segment Protection (SOPS)

In SOPS, we define a splitting node to be an intermediate node (other than the source and destination nodes) with anode degree greater than 2.For instance, there are 5 intermediate nodes in the multicast shown in fig.6 but only node 2 is qualified for a splitting node. Here a segment of a tree is defined as a portion of a path, connecting critical nodes. Critical nodes include source destination nodes and splitting nodes. Splitting nodes or desti-nation nodes can only be the end nodes but not the intermediate nodes of the segments.

There are be six possible scenarios of segments:

1) From the source node to a destination node;
2) From the source node to a splitting node;
3) From a splitting node to another splitting node;
4) From a splitting node to a destination node;
5) From a destination node to a splitting node;
6) From a destination node to another destination node.

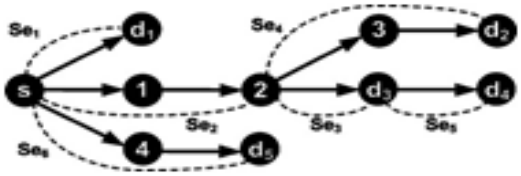


Fig. 5- An example of the segmentation of a tree

For the multicast tree in Fig.(5), we can identify 6 segments.

Conclusions

In this paper a comprehensive literature review is provided to discuss the current effort to extend the security approaches for source failure recovery on top of the combined node and link failure recovery for optical multicast traffic protection. Studies showed that, the total capacity is increased by up to 14%, if source failure recovery is required on top of the combined node and link failure recovery. This implies that the additional capacity required for source failure recovery can be more than capacity required for single intermediate node failure recovery. This finding verifies that, source failure recovery is more important than failure recovery of any other node or link on a multicast session. The flow p-cycle based dual-source protection approaches like IpC and NPCC, SOPS was also more capacity efficient than the optimal path pair based dual-source approach.

References

[1] Zhong W.D. and Zhang F. (2011) *Optical Switching and Networking*.
[2] Singhal N.K., Sahasrabuddhe L.H. and Mukherjee B. (2003) *IEEE/OSA J. Lightw. Technol.,* vol. 21, no. 11, pp. 2587-2594.
[3] Grover W.D. (2004) *Mesh-Based Survivable Networks - Options and Strategies for Optical, MPLS, SONET, and ATM Networking: Prentice Hall.*
[4] Zhang F. and Zhong W.D. (2008) *"Photonic Netw. Commu.*, vol. 16, no. 2, pp. 127-138.
[5] Zhang F., Zhong W.D. and Jin Y.H. (2008) *IEEE/OSA J. Lightw. Technol.,* vol. 26, no. 19, pp. 3298-3306.
[6] Zhang F. and Zhong W.D. (2009) *IEEE Commun. Lett.,* vol. 13, no. 1, pp. 40-42.
[7] Zhang F. and Zhong W.D. (2009) *IEEE/OSA J. Lightw. Technol.,* vol. 27, no. 18, pp. 4017-4025.
[8] Zhang F. and Zhong W.D. (2010) *IEEE/OSA J. Opt. Comm. & Netw.,* vol. 2, no. 10, pp. 831-840.
[9] Shen G.X. and Grover W.D. (2003) *IEEE J. Sel. Areas. Commun.,* vol. 21, no. 8, pp. 1306-1319.