Protection Algorithms for Groupcast Sessions in Transparent Optical Networks with Mesh Topologies

Tania Panayiotou and Georgios Ellinas
Department of Electrical and Computer Engineering
University of Cyprus
Nicosia, Cyprus
Email:{panayiotou.tania, gellinas}@ucy.ac.cy

Neo Antoniades
Department of Engineering Science and Physics
College of Staten Island
CUNY, New York, NY, USA
Email: Neo.Antoniades@csi.cuny.edu

***Abstract*—Next-generation networks are expected to support traffic that will be heterogeneous in nature with bandwidth-intensive unicast, multicast, and groupcast applications. This paper presents two novel heuristic algorithms, namely Cycle-for-two (CFT) and Tree-for-two (TFT), for protecting groupcast sessions in mesh optical networks. The proposed schemes outperform other protection techniques that are mainly extensions of known multicast protection algorithms with the CFT heuristic algorithm performing the best amongst all of them.**

I. Introduction

As networks evolve to support more bandwidth-intensive applications, and as rich multimedia and real-time services become more popular, next-generation networks are expected to support traffic that will be heterogeneous in nature with unicast, multicast, and groupcast applications. There are several potential groupcast applications in optical networks, where optical multipoint-to-multipoint sessions are set-up in wavelength-routed networks. Many applications that require groupcast are widely deployed, such as grid-computing, multi-party teleconferencing, distributed interactive simulations, virtual private network (VPN) services, and Ethernet LAN (E-LAN) services. In next-generation optical networks it is expected that groupcast applications will be even more commonly utilized to serve multipoint-to-multipoint bandwidth intensive sessions. However, for such applications to be viable, it is important that the groupcast traffic is not only routed efficiently through the optical network but it is also protected against any possible link failures in the network. Since groupcast sessions may carry traffic to multiple destinations, the impact of a link failure is even more severe compared to a link failure on a unicast or multicast session.

In transparent optical networks, a light-forest is constructed to serve a groupcast session, which is a set of light-trees or light-paths [1]. This is equivalent to finding a set of multicast trees or point-to-point paths in such a way that every node in the groupcast session can send to every other node in the session and receive from every other node in the session simultaneously. Since the light-tree approach performs better than the light-path approach, as was shown in [1], throughout this work we consider only the former case. Specifically, in the point-to-point (path) based approach [1], if the groupcast set is consisting of k nodes, then $k \times (k-1)$ point-to-point paths need to be computed. For example, the groupcast set $GC(d_1, d_2, d_3)$ consisting of three nodes, is decomposed into six point-to-point (unicast) sets $U_1(d_1, d_2)$, $U_2(d_1, d_3)$, $U_3(d_2, d_1)$, $U_4(d_2, d_3)$, $U_5(d_3, d_1)$, and $U_6(d_3, d_2)$. Then, for each point-to-point set a specified routing algorithm (e.g., Dijkstra's shortest path algorithm) can be used for the calculation of each path. In the light-tree approach [1], if the groupcast set consists of k nodes, then k multicast trees need to be routed. For example, for a groupcast set $GC(d_1, d_2, d_3)$ consisting of three nodes, three multicast trees need to be computed; one for each multicast set $MC_1(d_1, d_2, d_3)$, $MC_2(d_2, d_1, d_3)$, and $MC_3(d_3, d_1, d_2)$, where the first node in the multicast set corresponds to the source node of the tree and the rest of the nodes in the multicast set correspond to the destination nodes. In transparent optical networks, optical splitters can be used in network nodes to split the incoming signal to multiple outputs, thus enabling the establishment of connections with multiple destinations [2]. Finding the multicast tree corresponds to solving the Steiner Minimum Tree (SMT) problem that is NP-complete, and therefore several heuristics have been developed to approximately solve the problem [2], [4].

Subsequently, in order to solve the wavelength assignment subproblem for the light-forest found, several heuristics have been developed on assigning wavelengths to the routes (or trees). Fig. 1 shows a light-tree based connection for the groupcast set $GC(1, 2, 3, 4)$. In this example, four light-trees are required for supporting the session, utilizing three wavelengths. In general, to arbitrate wavelength contentions among lightpaths/light-trees, a random node sequence is generated for the multicast group. The first node generates its route and requests optical channel(s) for its route, publishing them to the second node. The second node generates its route and considers optical channels available, excluding the requested channels from the first node; the third node considers channels excluding the first and second route requests. For the $k \times (k-1)^{th}$ path or k^{th} tree, wavelength channels available are only those left after $[k \times (k-1) - 1]$ paths or $k-1$ trees respectively, reserve their channels [1].

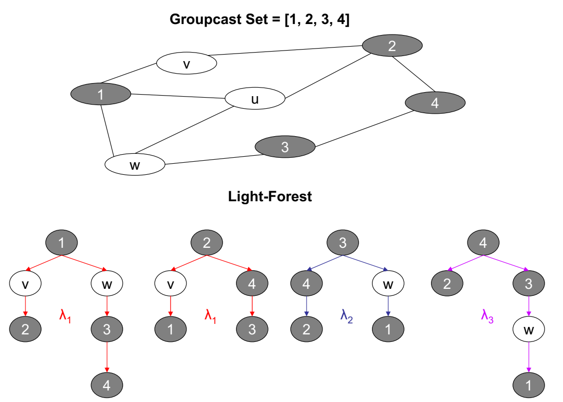

Fig. 1. Light-tree based optical groupcast.

Protecting a groupcast session against a link failure requires finding an alternate light-forest for all failure scenarios prior to the fault. According to the above, a solution to this problem corresponds to finding a set of alternate light-trees for each primary multicast tree in the light-forest. Thus, known multicast protection algorithms could be directly adapted for solving the groupcast protection problem. This work investigates the groupcast protection problem by examining the performance of several such multicast-based protection heuristic algorithms (such as the Arc-Disjoint Trees (ADT), the Modified Conventional Segment-Based Protection (MCSP), the Modified Segment-Based Protection With Sister Node First (MSSNF), and the Level Protection (LP) algorithms described in [3], [5]–[8]) and by also comparing them to two novel groupcast protection algorithms, namely the Cycle-for-two (CFT) and Tree-for-two (TFT) heuristic algorithms. The rest of the paper is organized as follows: Section II describes the proposed techniques, Section III discusses the provisioning of protected groupcast sessions, while Section IV shows the performance results for the proposed heuristics, followed by some concluding remarks in Section V.

II. Groupcast Protection

The mesh optical network is denoted as a graph $G(N, E)$, where N denotes the optical node set and E denotes the set of optical fibers. Each link $l \in E$ is assigned a positive weight to represent the cost between each pair of nodes. We assume the presence of optical splitters in each node, directional connections, W wavelengths per fiber, and a network with no wavelength converters. A groupcast request with n members is denoted as $GC(d_1, d_2, ..., d_n)$ and its primary light-forest as $LF(T_1, T_2, ..., T_n)$, where T_i is the primary light-tree for multicast set $MC_i(d_i, D_i)$. Note that d_i is the source node of the i^{th} multicast tree while the rest $n-1$ member nodes are included in the destinations set D_i. If a primary light-forest LF can be provisioned and can also be protected, the

TABLE I
Basic steps of the CFT heuristic for multicast sets MC_1 and MC_2 of groupcast session GC.

Step 1	In G, compute a linear light-tree c_1 starting from any node in groupcast set GC and visiting exactly once every other node in set GC, using the MC-CR (minimum cost collapsed ring) heuristic [9].
Step 2	Remove the arcs of c_1 from G and create graph G'.
Step 3	In G', compute shortest path c_2 connecting the end-points of c_1 and starting from the node last added to c_1, using a shortest path (Dijkstra's) algorithm.
Step 4	Merge paths c_1 and c_2 onto protection cycle C.
Step 5	Remove the arcs of c_2 from G' and create graph G''.
Step 6	In G'', find two primary arc-disjoint trees T_1 and T_2 for MC_1 and MC_2, using the Steiner Tree (ST) heuristic.

groupcast request is accepted in the network; otherwise it is blocked. Thus, the objective of this work is to devise protection algorithms that minimize the resources that are used to protect the primary light-forest and therefore the blocking probability in the network.

The key objective of a groupcast protection algorithm is to ensure that every affected destination can receive the information from the source via the backup path(s) after the failure. One solution to the groupcast protection problem is to directly use known multicast-based protection schemes [3], [5]–[8] for the creation of the backup light-forest $LF'(T'_1, T'_2, ..., T'_n)$, where T'_i corresponds to the backup paths of the primary light-tree T_i. This approach however, does not consider the unique characteristics of the groupcast sessions, as is done in the proposed techniques. The basic idea behind both proposed heuristics relies on the fact that between any multicast set in a forest the member nodes are the same. Thus, if any two multicast trees can be packed in the same wavelength and protected via the same backup path, then the number of resources used for protecting the entire light-forest is reduced, and thus so is the blocking probability.

A. Cycle-for-two Heuristic Algorithm

In the CFT approach, a single cycle that passes through every member in the groupcast request is computed to support two multicast trees in the case of a single link failure. The constraint is that primary trees must be arc-disjoint from each other and from their backup paths as well. Table I describes the basic steps of the CFT heuristic, between any two multicast sets of a groupcast session. Note that the protection cycle is calculated first, since in this way the savings of network resources are increased.

Fig. 2 is used as an illustrative example of the CFT heuristic for groupcast set $GC(a, b, c, d)$. Specifically, Fig. 2 shows only the two of the four multicast trees that must be created for the groupcast session, originating from source nodes a and b. In the same figure, multicast trees $MC(b, a, c, d)$ and $MC(a, b, c, d)$, computed by the Steiner Tree (ST) heuristic [3], are protected via the same cycle in such a way that both trees and the protection cycle are arc-disjoint from each other. Fig. 3 shows how the two light-trees are reconfigured upon the failure of link (a, b) by using the appropriate arcs of the protection cycle. Similar to any other protection scheme in which backup paths are shared between several primary paths, the protection arcs that will be utilized are not known prior to the failure and therefore an automatic protection switching (APS) protocol is required for setting-up the new light-trees after a link failure has occurred.

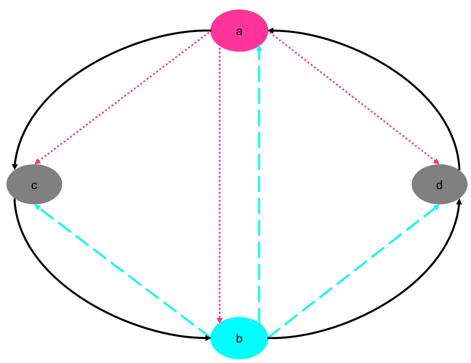

Fig. 2. A cycle passing through every node in $GC(a, b, c, d)$ supports multicast sets $MC(a, b, c, d)$ and $MC(b, a, c, d)$.

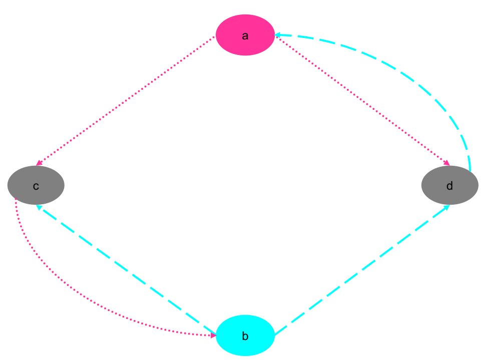

Fig. 3. Protection paths upon failure of link (a, b) in Fig. 2.

B. Tree-for-two Heuristic Algorithm

In the TFT approach a new tree is computed to support two multicast trees. The constraint again is that primary trees must be arc-disjoint from each other and from their backup paths as well. Table II describes the basic steps of the TFT heuristic, between any two multicast sets of a groupcast session. Again, the protection tree is calculated first, since in this way the savings of network resources are increased.

Figs. 4 and 5 are used as an illustrative example of the basic idea of the TFT heuristic for groupcast set $GC(a, b, c)$. Specifically, Fig. 4 shows only two of the three multicast trees that must be created for the groupcast session, originating from source nodes a and b. In the same figure, multicast trees

TABLE II
BASIC STEPS OF THE TFT HEURISTIC FOR MULTICAST SETS MC_1 AND MC_2 OF GROUPCAST SESSION GC.

Step 1	In G, calculate two arc-disjoint shortest paths p_1 and p_2 using a shortest path (Dijkstra's) algorithm, connecting the source nodes of multicast sets MC_1 and MC_2 in both directions.
Step 2	Remove from set GC the source nodes of multicast sets $MC1$ and $MC2$, and the arcs of paths p_1 and p_2 from G to create graph G'.
Step 3	In G', calculate a multicast tree T_1 using the ST heuristic, starting from any node in paths p_1 and p_2 and spanning every node in set GC.
Step 4	Identify the source node s' of tree T_1. If $s' \in p_j$, where $j = 1$ or 2, then calculate shortest path p_3 from any node in path p_i, where $i = 1$ or 2 and $i \neq j$ to node s'.
Step 5	Remove arcs of tree T_1 and path p_3 from graph G' to create graph G''.
Step 6	Merge tree T_1 and paths p_k, where $k = 1, 2, 3$ onto protection tree T.
Step 7	In G'', find two primary arc-disjoint trees T_2 and T_3 for MC_1 and MC_2 respectively, using the ST heuristic.

$MC(b, a, c)$ and $MC(a, b, c)$ computed by the Steiner Tree (ST) heuristic are protected via the same multicast tree that originates from a random node v in the network, in such a way that all three trees are arc-disjoint from each other. Fig. 5 shows how the two light-trees are reconfigured upon the failure of link (a, b) by using the appropriate arcs of the protection tree. As before, an APS protocol is required for rerouting the traffic after the failure has occurred. Note that the protection tree starts from a random node in the network and spans every other node in the groupcast set. Since performing an exhaustive search for finding the best source for the protection tree increases the computational complexity of the algorithm, the TFT heuristic, as shown in Table II, tries to identify a convenient source node v in a few algorithmic steps.

Note that in cases where there is an odd number of members of a groupcast set, then in both the CFT and TFT heuristics the remaining multicast set is protected separately utilizing the ADT protection technique.

III. PROVISIONING OF PROTECTED GROUPCAST SESSIONS

For each groupcast request GC consisting of k members, the protected groupcast routing and wavelength assignment (PGC-RWA) algorithm breaks the GC set into k MC sets. For each MC_i set the protected multicast routing and wavelength assignment (PMC-RWA) algorithm [8] is solved. Specifically, for the protected multicast routing subproblem, a primary light-tree T_i and its backup paths T_i' on the same wavelength are found. The Steiner-tree heuristic is used for the computation of the primary light-trees while for the computation of their backup paths one of the ADT, MCSP, MSSNF or LP [3],

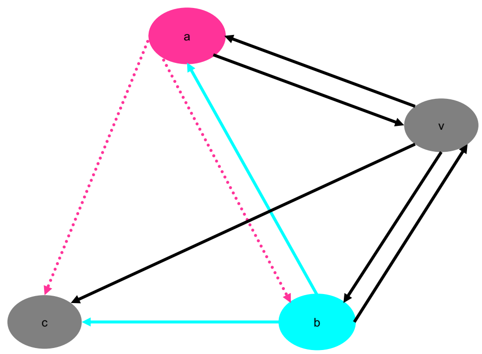

Fig. 4. A tree originating at a random source v and spanning all nodes in $GC(a, b, c)$ supports multicast sets $MC(a, b, c)$ and $MC(b, a, c)$.

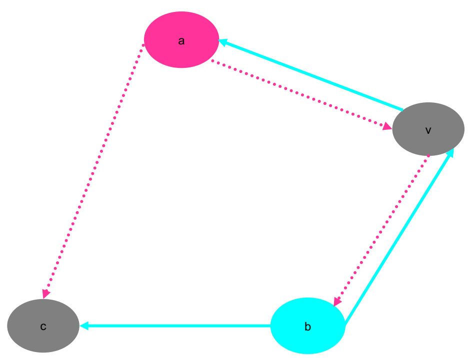

Fig. 5. Protection paths upon failure of link (a, b) in Fig. 4.

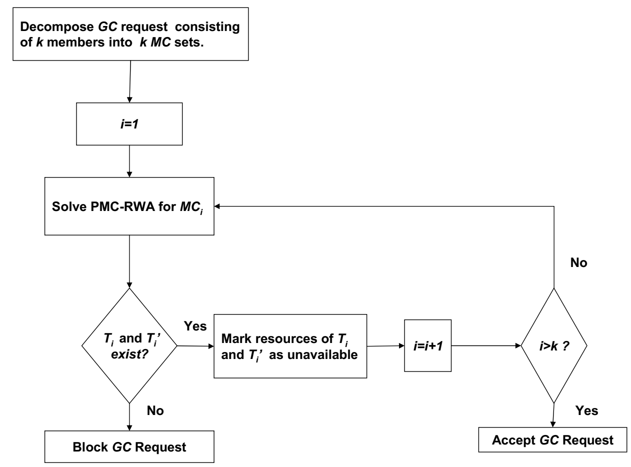

Fig. 6. Flowchart of the protected groupcast routing and wavelength assignment (PGC-RWA) algorithm when one of the ADT, MCSP, MSSNF or LP [3], [5]–[8] heuristic algorithms is used.

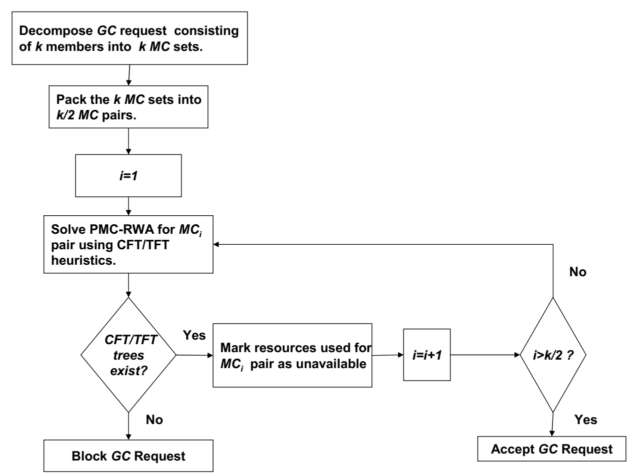

Fig. 7. Flowchart of the protected groupcast routing and wavelength assignment (PGC-RWA) algorithm when one of the CFT or TFT heuristic algorithms is used.

[5]–[8] heuristics is used. For the wavelength assignment procedure the *first-fit* algorithm is utilized. Groupcast requests are blocked if there is no available wavelength for the entire primary tree and its backup paths. The flowchart of Fig. 6 describes in detail the PGC-RWA algorithm used in this work.

The aforementioned approach is slightly modified when the CFT and TFT heuristics are used, in order to pack multicast sets into pairs in a random fashion before the computation of the primary tree and its backup paths. Specifically, for each groupcast request GC consisting of k members, the PGC-RWA algorithm breaks the GC set into k MC sets. Subsequently, it randomly packs the multicast sets into $\frac{k}{2}$ MC pairs and for each MC pair the PMC-RWA algorithm is solved. For the protected multicast routing subproblem, one of the proposed CFT and TFT heuristic algorithms is used while for the wavelength assignment procedure the *first-fit* algorithm is again utilized. Groupcast requests are blocked if there is no available wavelength for the entire CFT or TFT trees. The flowchart of Fig. 7 describes in detail the modified PGC-RWA algorithm used for the CFT and TFT heuristic algorithms. Note that, the flowchart of Fig. 7 assumes that the number of the k members included in the GC set is even. However, if k is an odd number, then one more algorithmic step is required for the remaining MC set. For the remaining MC set, the PMC-RWA algorithm is used, during which the ADT heuristic is utilized during the protected multicast routing subproblem and the *first-fit* algorithm is utilized during the wavelength assignment procedure.

IV. Performance Evaluation

To evaluate the performance of the different groupcast protection techniques described above, a metropolitan area optical network was considered with statistics as shown in Table III.

Groupcast requests arrive into the system dynamically according to a Poisson process and the holding time is exponentially distributed with a unit mean. In each simulation, $2,000$ requests were generated for each groupcast group size for a total of $22,000$ groupcast requests, and the results were averaged over five simulation runs. One hundred and twenty eight (128) wavelengths per link were utilized to evaluate the blocking probability versus the groupcast group size for a network load of 50 Erlangs.

Fig. 8 shows the blocking probability versus the groupcast group size for a number of groupcast routing algorithms. Results show that CFT heuristic outperforms all other schemes,

TABLE III
NETWORK STATISTICS

Number of nodes	50
Number of links	98 (196 arcs)
Average nodal distance	60 Km
Maximum link length	100 Km
Minimum link length	20 Km
Average node degree	3.92
Minimum node degree	3
Maximum node degree	6
Network diameter	305 Km (6 hops).

especially for large groupcast group sizes. The TFT heuristic only slightly outperforms the rest of heuristic algorithms that were initially developed for multicast connections especially for small group sizes.

Furthermore, from the description of the heuristics, it is clear that both the CFT and TFT heuristics achieve much lower redundant capacity for protecting the groupcast sessions compared to the other multicast-based heuristics, as in these two cases each cycle found protects all the links for a pair of multicast trees. This is true as the CFT and TFT heuristics by default share their backup resources and this sharing approach is much simpler compared to global cross-sharing techniques [10] that could be used for the multicast-based protection approaches. Thus, for the implementation of the CFT or TFT protection techniques, simpler APS protocols will be required to arbitrate the common resources in case of a link failure, compared to the case where cross-sharing is performed. In the latter case, cross-sharing of the resources in general increases the computation complexity of the protection heuristic algorithms, as well as the implementation of the protection techniques since a more complex mechanism is now required in the network in order to keep information of the reserved resources and their capabilities of being shared.

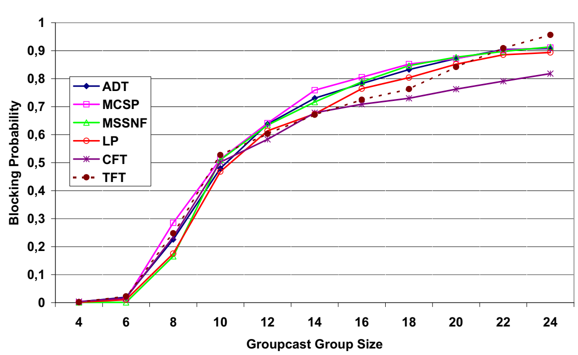

Fig. 8. Blocking probability vs. groupcast group size.

V. CONCLUSION

The performance of several groupcast protection schemes initially proposed for multicast traffic, were extended to support groupcast connections and also two new protection schemes, namely the CFT and TFT heuristics, that consider the unique characteristics of groupcast connections, were developed. Performance results showed that the CFT heuristic algorithm outperforms all the other approaches for the protection of groupcast connections. In addition, these two new approaches provide an inherent simple sharing capability, compared to more general multicast-based cross-sharing protection techniques that require more complex protection heuristics and protocols.

ACKNOWLEDGMENT

This work was supported by the Cyprus Research Promotion Foundation's Framework Programme for Research, Technological Development and Innovation (DESMI 2009-2010), co-funded by the Republic of Cyprus and the European Regional Development Fund, and specifically under Grant TPE/EPIKOI/0311(BIE)/11.

REFERENCES

[1] T. Rahman, G. Ellinas, and M. Ali, "Lightpath- and Light-Tree-Based Groupcast Routing and Wavelength Assignment in Mesh Optical Networks," *IEEE/OSA Journal of Optical Communications and Networking*, 1(2):A44-A55, 2009.

[2] L. H. Sahasrabuddhe and B. Mukherjee, "Multicast Routing Algorithms and Protocols: A Tutorial", *IEEE Network*, 14(1):90-102, 2000.

[3] N. K. Singhal, L.H. Sahasrabuddhe, and B. Mukherjee, "Provisioning of Survivable Multicast Sessions against Single Links Failures in Optical WDM Mesh Networks", *IEEE/OSA Journal of Lightwave Technology*, 21(11):2587-2594, 2003.

[4] Y. Sun, J. Gu, and D. H. K. Tsang, "Multicast Routing in All-optical Wavelength-routed Networks," *SPIE Optical Networks Magazine*, 2(4):101-109, 2001.

[5] N.K. Singhal, L.H. Sahasrabuddhe, and B. Mukherjee, "Protecting a Multicast Session Against Single Link Failures in a Mesh Network," *Proc. IEEE International Conference on Communications (ICC)*, Anchorage, Alaska, May 2005.

[6] X. Wang, L. Guo, L. Pang, J. Du, and F. Jin, "Segment Protection Algorithm with Load Balancing for Multicasting WDM Mesh Networks," *Proc. 10th International Conference on Advanced Communication Technology (ICACT)*, Phoenix Park, Korea, February 2008.

[7] H. Luo, L. Li, and H. Yu, "Algorithm for Protecting Light-trees in Survivable Mesh Wavelength-division-multiplexing Networks," *OSA Journal of Optical Networking*, 5(12):1071–1083, 2006.

[8] T. Panayiotou, G. Ellinas, and N. Antoniades, "Segment-based Protection of Multicast Connections in Metropolitan Area Optical Networks with Quality-of-transmission Considerations," *IEEE/OSA Journal of Optical Communications and Networking*, 4(9):692-702, 2012.

[9] T. Rahman and G. Ellinas, "Protection of Multicast Sessions in WDM Mesh Optical Networks," *Proc. Optical Fiber Communications Conference (OFC)*, Anaheim, CA, March 2005.

[10] N.K. Singhal, C. Ou, and B. Mukherjee, "Cross-sharing vs. Self-sharing Trees for Protecting Multicast Sessions in Mesh Networks," *Elsevier Computer Networks*, 50(2):200–206, 2006.