Dynamic Dual-Homing Protection in WDM Mesh Networks

Vinod M. Vokkarane[†], **Jianping Wang**[‡], **Xiangtong Qi**[+], **Raja Jothi**[†], **Balaji Raghavachari**[†], **and Jason P. Jue**[†]
[†] Department of Computer Science, The University of Texas at Dallas, Richardson, Texas
[‡] Department of Computer Science, Georgia Southern University, Statesboro, Georgia
[+] Department of IEEM, Hong Kong University of Science & Technology, Hong Kong
E-mail: [†]{vinod, raja, rbk, jjue}@utdallas.edu, [‡]jpwang@gasou.edu, [+]ieemqi@ust.hk

***Abstract*—A fault-tolerant scheme, called *dual homing*, is generally used in IP-based access networks to increase the survivability of the network. However, dual homing itself cannot provide survivability with respect to possible failures in the Wavelength Division Multiplexed (WDM) core network. To provide survivability in the core network, *protection* and *restoration* techniques must be used. In the past, dual homing architecture and protection are studied separately. In this paper, we observe that the dual homing architecture introduces new issues for protection and restoration design, especially when providing survivability against two independent failures, one in the access network and the other in the core network. This paper provides an integrated solution and studies the protection design problem in the WDM core network, given a dual-homing infrastructure in the access network. Several algorithmic solutions are proposed, and performance of the solutions is compared.**

I. INTRODUCTION

One important issue in IP-over-WDM networks is survivability, which is the capability of the network to function in the event of node and/or link failures. There are two types of survivability that need to be considered in the Internet, one in the access network and the other in the core network.

Dual homing is generally used to increase survivability in the access network. In a dual homing architecture, a host in the access network is attached to two IP routers, called dual homes, which are connected to underlying edge optical cross connects (OXCs) of the core network, as shown in Fig. 1. The main objective of dual homing is to provide enhanced survivability to protect against access node failures caused by system malfunction, scheduled outage, or an access link failure. Dual-homing architecture design has been extensively studied in self-healing ring networks [1], [2], [3], [4], [5].

In WDM networks, survivability is usually provided to handle a link failure in the core network. A single failure in an optical fiber can dramatically degrade network performance, since a single fiber carries a large amount of traffic. Therefore, it is critical to support network survivability in WDM core networks. Survivability in WDM networks is implemented using *protection* and *restoration* techniques, which provide the survivability by setting up two disjoint lightpaths [6] between the source and the destination. One lightpath is called the primary lightpath and the other is called the backup lightpath. *Protection* is a static mechanism, which reserves resources for both primary and backup lightpaths prior to the data communication. Restoration, on the other hand, is a dynamic mechanism where the backup lightpath is not set up until the failure occurs. Existing literature on protection and restoration in WDM networks can be found in [7], [8], [9], [10].

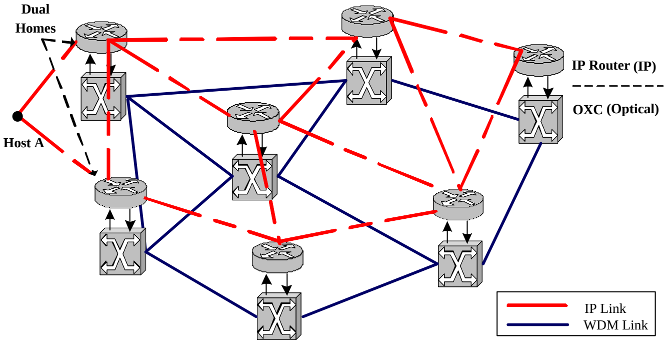


Fig. 1. IP-over-WDM Dual-homing network architecture.

There have been several efforts on providing survivability for a dual-homed IP-based access network over a WDM-based core networks [11], [12]. All these studies consider providing survivability separately at the IP layer verses the WDM layer. In [11], the authors discuss how to support dual-homing in passive optical networks; while [12] studies survivability in IP-over-WDM networks and provides different protection types (unprotected, protected, and dual homing) for each IP link in order to keep the network connected in the event of a link failure. The focus of our paper is to provide an integrated solution for providing survivability in an IP-over-WDM mesh network.

In this paper, a *dual-homing protection* problem is studied, which integrates dual homing and protection by using dual homing to provide survivability against a single node/link failure in the access network, and using protection to handle a single link failure in the optical core network. We assume that the failures in the access network and the core network are independent, which means that the failure of the access node/link and the failure of the link in the core network can occur simultaneously. By considering the dual-homed IP-over-WDM architecture (Fig. 1), we observe that, at any given time, each host transmits data to the destination only through one of the dual homes. Based on this observation, we see that only one of the primary/backup paths between the dual homes and the destination will be utilized at any given time. Also, this property leads to fewer restrictions on the disjointness constraint between the two primary and two backup paths from each of the dual homes to a specific destination. We observe that by providing an integrated solution, we can obtain significant cost benefits as compared to handling survivability separately at each of the layers (IP and WDM).

The rest of the paper is organized as follows. The network architecture of dual-homing protection is described in Section II. A detailed problem description is presented in Section III. In

Section IV, we propose a number of different heuristics to solve the dynamic dual-homing protection problem. In Section V, we evaluate the performance of all the proposed algorithms. Finally, the conclusion is presented in Section VI.

II. NETWORK ARCHITECTURE

In this paper, we consider an integrated IP-over-WDM network as shown in Fig. 1, where a host in the access network is attached to two IP routers (homes) in the IP-based access network. Each IP router is connected to an optical cross connect (OXC), which in turn is linked to other OXCs that constitute the all-optical WDM core network. In a dual-homing architecture, two link-disjoint paths connect the host to its dual homes, which provides survivability against a single IP router (access node) or access link failure. The dual-homed IP routers are connected to the underlying OXCs, which convert the IP packets into optical signals and the packets are transmitted over the WDM layer to the corresponding destinations.

In the event of an access node failure, by using dual homing, the access traffic can be shifted to the other home (access node), which in turn transmits the data traffic to the destination. We observe that in the event of an access link failure, the access network is survivable with dual homing infrastructure. Hence, dual homing provides survivability against a single link or node failure in the access network. In the event of a link failure in the core, we adopt link-disjoint dedicated path protection to provide survivability [7], [8], [9]. Therefore, the dual-homing protection problem we study in this paper can provide survivability subject to a single access link/node failure as well as single core link failure simultaneously.

In our model, we assume that when the IP router fails, the OXC connected to the router continues to carry optical traffic from other OXCs in the core network. This assumption is reasonable since WDM layer is a separate layer, and switching functions are provided independently at the WDM layer.

In dual homing, we have two source OXCs, with only one source OXC transmitting data to a specific destination OXC at any given time. Therefore, we observe that, in most solutions, the primary paths between each of the two source OXCs to the destination OXCs need not necessarily be disjoint. As a matter of fact, we find that having the primary paths share the maximum number of links reduces the amount of resources reserved, which is one of the primary objectives in this work. On the other hand, the disjointness constraint between the primary paths and the backup paths has to be satisfied. The detailed description of the problem and the solution approaches are given in the following sections.

III. PROBLEM DESCRIPTION

A WDM network can be modeled as an unidirected graph $G = <V, E>$, where V is the set of OXCs and E is the set of WDM links. Let the wavelength cost of a WDM link $e \in E$ be $c(e)$. Let the maximum number of wavelengths in each link be W. Suppose the current request is given by $\{\{s_1, s_2\}, d\}$, where s_1 and s_2 are two OXCs connected to the dual-homed access routers of the current request, and d is the destination OXC that in turn is connected to an IP router that connects to the destination host of the current request. Let the primary lightpath from s_1 to d be denoted by p_a^1 and the link-disjoint backup lightpath from s_1 to d be denoted by p_b^1. Similarly, the primary lightpath from s_2 to d is denoted by p_a^2 and the link-disjoint backup lightpath from s_2 to d is denoted by p_b^2. Let L be the set of all links used in the primary and backup lightpaths for the current request, where $L = p_a^1 \cup p_b^1 \cup p_a^2 \cup p_b^2$.

If the core network is reliable, p_a^1 and p_a^2 are not necessarily disjoint as shown in Fig. 2(a). However, even if p_a^1 and p_a^2 are disjoint, they cannot protect simultaneous failures in the access network and the core network, as shown in Fig. 2(b). If the access node of s_1 is down, and one link in p_a^2 is also down, data cannot be sent to d. In order to provide dual-homing protected service, we need p_b^1 and p_b^2 to protect the lightpaths p_a^1 and p_a^2. We have the following observations (Fig. 2(c)):

- p_a^1 and p_b^1 must be disjoint.
- p_a^2 and p_b^2 must be disjoint.
- p_a^1 and p_a^2 are not necessarily disjoint.
- p_b^1 and p_b^2 are not necessarily disjoint.
- p_a^1 and p_b^2 are not necessarily disjoint.
- p_a^2 and p_b^1 are not necessarily disjoint.

In this paper, we study the problem to route the lightpaths p_a^1, p_b^1, p_a^2, and p_b^2 when a new request arrives, which is called *Dynamic Dual-Homing Protection*. Without loss of generalization, we assume that each connection request is for a single wavelength.

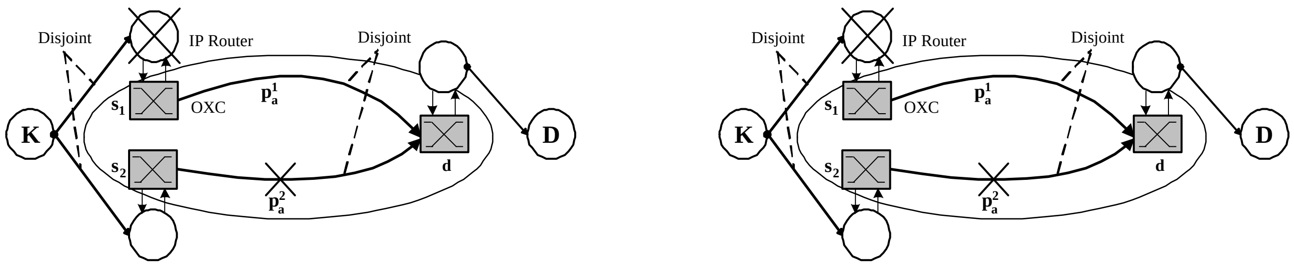
We assume that full-wavelength conversion capability is available at each OXC in the core network and that the wavelength conversion cost is not significant. We only consider the wavelength cost. Therefore, our objective in dynamic dual-homing protection is to find L for the current request such that $\sum_{e \in L} c(e)$ is minimum.

IV. DYNAMIC DUAL-HOMING PROTECTION

We now propose several heuristics for dynamic dual-homing protection. These heuristics can be classified into two categories: one category is based on a minimum cost network flow model and the other category is based on a minimum Steiner tree model. The minimum cost network flow model computes minimum-cost link-disjoint paths which satisfy the disjointness between the primary path and the backup path [14]. On the other hand, the minimum Steiner tree model considers the sharing among the primary paths and sharing among the backup paths.

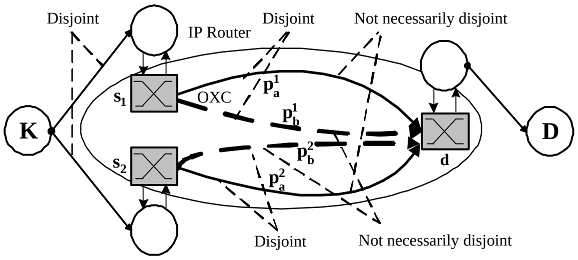
The first heuristic is based on minimum cost network flows. The heuristic finds the optimal link-disjoint primary and backup lightpaths from one of the dual homes to the destination, and then finds the optimal link-disjoint primary and backup lightpaths from the other dual home to the destination.

The second heuristic is also based on minimum cost network flows and is a generalization of the first heuristic in which we first select a new node known as the *branching node*. From each of the dual homes we compute two minimum-cost link-disjoint paths to the branching node, and from the branching node we compute two minimum cost link-disjoint paths to the destination. This process is repeated, selecting every node as



(b) Unprotected dual-homing architecture with failures.

(b) Unprotected dual-homing architecture with failures.



(c) Protected dual-homing architecture.

Fig. 2. Dual homing and protection architectures.

the branching node, and then choosing the minimum cost solution. The first heuristic is a special case of second heuristic in which the destination is chosen as the branching node.

The third heuristic is also based on minimum cost network flow model and is motivated by the fact that the two dual homes are usually located close to each other. Here, we find the shortest link-disjoint paths from each of the dual homes to the destination, and also two minimum cost link-disjoint paths between the dual homes. These four paths make up the primary and backup lightpaths.

The last heuristic is based on the minimum Steiner tree. The heuristic finds a low-cost Steiner tree that connects the two homes to the destination and the primary paths are covered by the minimum Steiner tree. The heuristic then provides path protection from each home to the destination.

We now describe each of the heuristics in detail and compare their relative performance.

A. Minimum Cost Network Flow Heuristic (MCNFH)

The *minimum cost network flow heuristic* (MCNFH) first finds the minimum cost link-disjoint primary and backup lightpaths from one of the dual homes to the destination, then changes the cost of the these links to zero (in order to encourage sharing) and finds the minimum cost link-disjoint primary and backup lightpaths from the other dual home to the destination.

We can use the minimum cost network flow (MCNF) algorithm to find the minimum-cost link-disjoint primary and backup lightpaths from one home to the destination. Initially, we set the capacity of link to be unity in order to force the primary and the backup lightpaths from s_1 to d as well as from s_2 to d to be disjoint. Note that the order in which the paths are computed has a bearing on the total cost. Hence, we first find the primary and backup lightpaths from one dual home to the destination, and then find the primary and backup lightpaths from the other dual home to the same destination. Then we exchange the order and repeat the same process. Finally, we select the solution having the minimum cost.

It is proved that any solution obtained by MCNFH is at most 4/3 times the cost of the optimal solution under the additional assumption that links are bi-directional. The proof can be found in [15].

B. Minimal Disjoint Segment-Pair Heuristic (MDSPH)

The minimal disjoint segment-pair heuristic (MDSPH) is based on the observation that the two primary paths are either disjoint or there is a branching node which connects the two homes and the destination. As a matter of fact, if two primary paths are disjoint, it can still be considered as if there is a branching node located at the destination. Obviously, the position of the branching node will affect the total cost of the primary lightpaths and backup lightpaths.

The MDSPH tries to find the right branching node such that the total wavelength cost used in both primary paths and backup paths is minimum. Let S_i be the set of links used in the primary paths and backup paths, when Node $v_i \in V$ is chosen as the branching node. MDSPH make efforts on finding v_b such that $S_b = \min_{v_i \in V} \{S_i\}$.

MDSPH always finds a solution if a feasible solution exists. The solution obtained is no worse than MCNFH, since MCNFH is a special case of MDSPH where the destination serves as the branching node.

C. Minimum Cost Shortest Path Heuristic (MCSPH)

In the minimum cost shortest path heuristic (MCSPH), we obtain link-disjoint shortest paths from the dual homes to the destination, and then compute two link-disjoint paths with minimum cost between the dual homes themselves.The solution obtained is composed of two minimum cost link-disjoint primary paths from the dual homes OXCs to the destination, p_a^1 and p_a^2. The backup path for the first home is composed of the path from the first home to the second home and the path from the second home to the destination. The backup path for the second home is composed of the path from the second home to the first home and the path from the first home to the destination. Since the backup paths from a dual home to the destination go through the other dual home, in the case of an access node failure, we assume that the underlying OXC can continue to forward all-optical traffic seamlessly.

D. *Minimum Steiner Tree Heuristic (MSTH)*

The minimum Steiner tree heuristic uses the fact that a minimum Steiner tree is the best approach to connect three nodes with minimum cost. The idea behind the minimum Steiner tree heuristic (MSTH) is to find a minimum cost tree which is designated as the primary tree and then provides path protection to the dual homes.

Although the minimum Steiner tree problem is NP-hard in the general case, it is polynomial-time solvable when there are only three terminal nodes. We observe that a tree with only three terminal nodes will have at most one branching (or splitting) node. Once the branching node is determined, the minimum cost Steiner tree is obtained by finding shortest paths from the branching point to each of the end nodes (the dual homes and the destination). In order to find the optimal branching node in a network with N nodes, we can consider each Node $v_i \in V$ to be the branching point and then T_i, which consists of the shortest paths from s_1 to v_i, from s_2 to v_i, and from v_i to d, resulting in N different trees. The optimal minimum Steiner tree, T_{opt}, is given by the minimum cost tree of the N different enumerated trees. Two primary lightpaths are provided in T_{opt}. Then a link-disjoint backup lightpath is constructed from each source to the destination.

E. *Heuristic Algorithms Comparison*

We observe that MCNFH and MDSPH can always find a solution, if one exists, since finding a disjoint pair of paths from one home router to the destination does not interfere with the choice of the disjoint pair of paths from the other home router to the destination. However, MSTH may not be able to find such a feasible solution, even if there is such a solution, since there may not be link-disjoint backup lightpaths (or a disjoint tree) after the primary lightpaths (or tree) are computed. For MCSPH, it is also possible that the heuristic cannot find the feasible solution, even if such a solution exists, since there may not be link-disjoint paths between the dual homes.

The MCNFH and MCSPH have a worst-case time complexity $O(N^2)$, the generalized MDSPH has a worst-case time complexity $O(N^3)$, and the MSTH has a worst-case time complexity $O(N^3)$.

V. SIMULATION RESULTS

In this section, we analyze the performance of proposed algorithms for dynamic dual-homing protection. We are interested in comparing the performance of MCNFH, MDSPH, MCSPH, and MSTH. We compare our solutions for the integrated dual-homing protection with a baseline solution obtained by providing protection without being aware of the dual-homing architecture.

We are interested in comparing the average total cost of the solutions obtained using MCNFH, MDSPH, MCSPH, and MSTH under the bidirectional network topology as well as unidirectional network topology. The important simulation parameters include the network size, N, the maximum outgoing degree at each node, D. Given a group of parameters $<N, D>$, we randomly generate a network with N nodes. The outgoing degree of each Node i, is uniformly distributed in $[1, 2, \ldots, D]$. The cost of each link is set to unity. For the selection of dual homes, we consider two approaches, in one of the approaches we consider two random nodes to be the dual homes connected to the host and in the other approach we consider the two closest nodes connected to the host (IP routers) to be the dual homes. Based on the approach used for selecting the dual homes, we observe the performance of different heuristics. Once the dual homes are selected, we randomly select a destination and assume the current connection request is from the selected dual homes to the selected destination.

For each group of parameters, problem instances are generated until 1000 instances have feasible solutions by using MCNFH. All these instances are also solved by MDSPH, MCSPH, MSTH, and the baseline solution (where in sharing between any of the primary and backup paths is not allowed).

Fig. 3-6 plots of average cost for the proposed algorithms

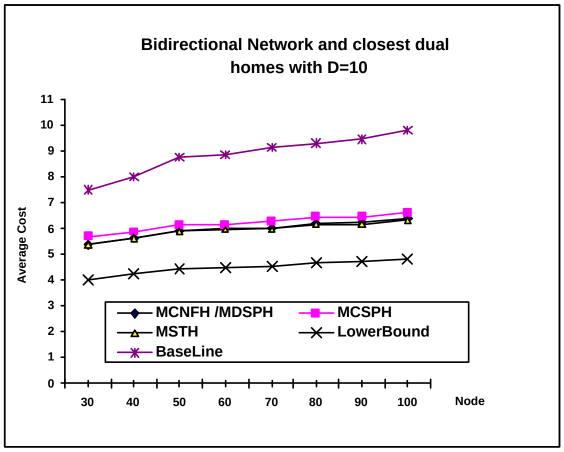


Fig. 3. The average cost versus number of nodes (N) in bidirectional networks with closest dual homes

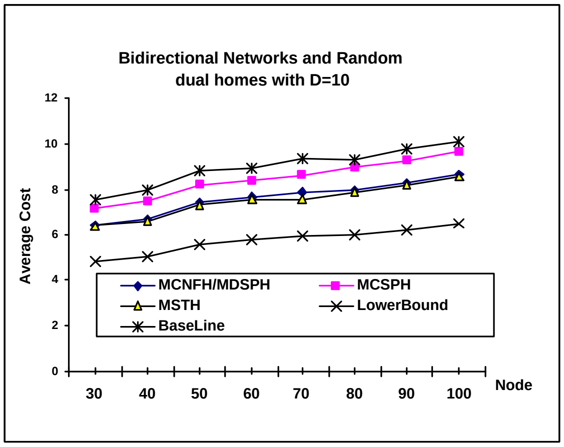


Fig. 4. The average cost versus number of nodes (N) in bidirectional networks with random dual homes

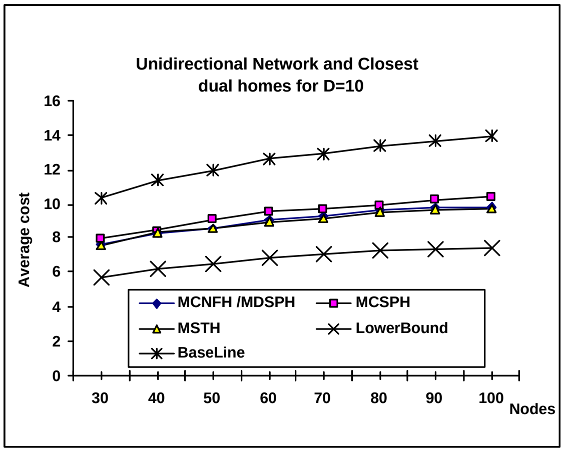


Fig. 5. The average cost versus number of nodes (N) in unidirectional networks with closest dual homes

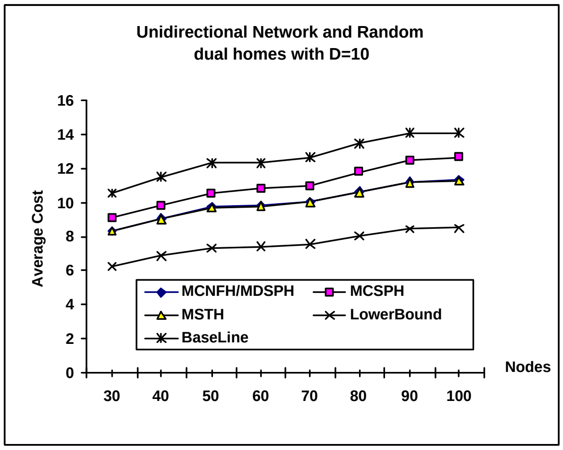


Fig. 6. The average cost versus number of nodes (N) in unidirectional networks with random dual homes

versus different values of N, when D is set to 10 considering both bidirectional and unidirectional networks with the two different approaches of assigning dual homes (closest/random). In order to show the advantage of the integrated solution, we compare the algorithms with the baseline case. By considering that a dual-homed IP layer exists above the WDM core network, we can see that the cost of providing protection in the core network using MCNFH, MDSPH, MCSPH, and MSTH is significantly lower than the baseline case. We also observe that MCNFH and MDSPH incur the same cost for the network scenarios considered. The performance of MSTH is slightly better than that of the network flow-based algorithms. Also, using the result that MCNFH is 4/3 times the optimal solution, we also plot a tight lower-bound for the dynamic dual-homing protection problem.

For all these cases in Fig. 3-6, the performance of MCSPH is worse than network flow-based algorithms. However, we observe that if the paths from the closest dual homes to the destination for the current connection request is long, MCSPH works better than the other heuristic algorithms, since only two long paths need to be found. In other words, the average cost of MCSPH is lower than other heuristic algorithms in a large sparse network where the dual homes are close to each other and the paths from the dual homes to the destination are long.

VI. CONCLUSION

We investigate the survivability issue in IP-over-WDM networks when a dual-homing architecture is provided in the access network. Our goal is to provide survivability for such an infrastructure subject to two independent failures, one failure from the access network and one from the core network. We proposed four new heuristics, namely MCNFH, MDSPH, MCSPH, and MSTH for the dynamic dual-homing protection problem. These heuristics can be classified into two categories: those based on the minimum cost network flow model and those based on the minimum Steiner tree model. For a dense network, MCNFH is the best choice which achieves a good balance between the running time, average cost, and the capability to find a feasible solution. For a large sparse network, MCSPH is the best candidate to solve the dynamic dual-homing protection problem due to its faster running times and its ability to find low cost solutions. We observe that by following an integrated approach that considers the dual-homed IP-over-WDM architecture as compared to an independent solution at each layer (IP and WDM), we can significantly reduce the cost incurred to provide protection in the WDM core network.

REFERENCES

[1] C. Lee and S. Koh, "A Design of the Minimum Cost Ring-Chain Network with Dual-homing Survivability: A Tabu Search Approach," *Computers Operations Research*, vol. 24, no. 9, pp. 883-897, 1997.

[2] M. Willebeek-LeMair and P. Shahabuddin, "Approximating Dependability Measures of Computer Networks: An FDDI Case Study," *IEEE-ACM Transactions on Networking*, vol. 5, no. 2, pp. 311-327, April 1997.

[3] F. Farahmand, A.F. Fumagalli, and M. Tacca, "Near-Optimal Design of WDM Dual-Ring with Dual-Crossconnect Architecture," *Proceedings, SPIE Optical Networking and Communication Conference (OptiComm) 2002*, Boston, MA, vol. 4874, pp.286-297, July 2002.

[4] A. Proestaki and M. Sinclair, "Design and Dimensioning of Dual-Homing Hierarchical Multi-Ring Networks," *IEE Proceedings-Communications*, vol. 147, no. 2, pp. 96-104, April 2000.

[5] J. Shi and J. Fonseka, "Analysis and Design of Survivable Telecommunications Networks," *IEE Proceedings-Communications*, vol. 144, no. 5, pp. 322-330, Oct. 1997.

[6] I. Chlamtac, A. Ganz, and G. Karmi, "Lightpath Communications: An Approach to High Bandwidth Optical WANs," *IEEE Transactions on Communications*, vol. 40, no. 7, pp.1171-1182, 1992.

[7] E. Modiano and A. Narula, "Survivable Lightpath Routing: A New Approach to the Design of WDM-Based Networks," *IEEE Journal on Selected Areas in Communications*, vol. 20, no. 4, pp. 800-809, May 2002.

[8] F. Ricciato, S. Salsano, and M. Listanti, "Optimal Routing for Protection and Restoration in an Optical Network," *Photonic Network Communications*, vol. 4, no. 3-4, pp. 409-422, Jul. -Dec. 2002.

[9] D. Zhou and S. Subramaniam, "Survivability in Optical Networks," *IEEE Network* , vol. 14, no. 6, pp. 16-23, Nov/Dec. 2000.

[10] S. Yuan and J.P. Jue, "A Shared Protection Routing Algorithm for Optical Networks," *SPIE Optical Networks Magazine*, vol. 3, no. 3, pp. 32-39, May/June 2002.

[11] A. Phillips, J. Senior, R. Mercinelli, M. Valvo, P. Vetter, C. Martin, M. Deventer, P. Vaes, and X. Qiu, "Redundancy Strategies for a High Splitting Optically Amplified Passive Optical Network," *IEEE Journal of Lightwave Technology*, vol. 19, no. 2, pp. 137-149, Feb. 2001.

[12] G. Sasaki and C. Su, "The Interface between IP and WDM and its Effect on the Cost of Survivability," *IEEE Communications Magazine*, vol. 41, no. 1 , pp. 74-79, Jan. 2003.

[13] A. Orda and R. Rom, "Multihoming in Computer Networks: a Topology-design Approach," *Computer Networks ISDN*, vol. 18, no. 2, pp. 133-141, Feb. 28, 1990.

[14] J. W. Suurballe, "Disjoint Paths in a Network,"*Networks*, vol. 4, pp. 125-145, 1974.

[15] J. Wang, V.M. Vokkarane, R. Jothi, X. Qi, B. Raghavachari, and J.P. Jue, "Dual-Homing Protection in WDM Mesh Networks", *UTD Technical Report UTDCS-40-03*, Sept. 2003.