A Novel Distributed Destination Routing-Based Availability-Aware Provisioning Framework for Differentiated Protection Services in Optical Mesh Networks

Emad M. Al Sukhni, Student Member, IEEE and Hussein T. Mouftah, Fellow, IEEE
School of Information Technology and Engineering SITE
University of Ottawa
Emad.Alsukhni@uottawa.ca, mouftah@site.uottawa.ca

Abstract

In optical mesh networks, different protection schemes can be used to satisfy the service availability against network failures. However, in order to satisfy a connection's service-availability requirement in a distributed controlled WDM with dynamic traffic and no wavelength converters, we need a framework to manage the provisioning process and to select a proper protection scheme. In this paper, we propose a novel distributed Availability-Aware provisioning framework based on intelligent destination routing to assign and manage the working and the protection paths as well as their wavelength(s) of each connection. Our proposed framework probes the k most reliable paths in parallel. The probing technique used in this framework is the first probing technique that probes each path as both a candidate working path and a candidate shared protection path at the same time. Moreover, we propose to use connection availability as a metric for providing differentiated protection services in WDM mesh networks. Based on the availability information collected, our provisioning strategy selects an appropriate level of protection to each connection. The effectiveness of our provisioning approaches is demonstrated through simulation results.

Index Terms— distributed controlled optical network, distributed k-Alternative paths, *Availability-Aware routing, connection provisioning, differentiated services, destination routing, protection, service reliability.*

1. Introduction

Driven by the rapid growth of the Internet, increasing demand, and the nature of traffic, WDM is now beginning to expand from a network core technology toward metropolitan and access networks. It is envisioned that fibers will be extended to homes and small businesses, thereby making efficient use of the increasing number of wavelengths available, and dynamic lightpath establishment is thus essential to respond quickly and economically to customer demands. Due to the huge amount of data that can be lost and the large number of users that can be disrupted as a result of a fiber cut or node failure, network survivability has become a key issue during the RWA process. The working lightpath and the backup lightpath must be link-disjoint in order to protect against fiber cuts or node-disjoint to protect further against node failure. In order to achieve the service reliability required, a network operator needs to provision a customer's connection requests by considering the network components' failure probabilities, failure repair times, and connection restoration times. Connection availability is determined by the network components' availabilities along its route [1]. To increase service reliability against network failures; extra resources for each connection request, *protection, can* be used. A variety of protection schemes have been studied in the literature, such as dedicated vs. shared, link-rerouted vs. path-rerouted, etc. [2, 3].

Several works have been done on availability-Aware provisioning. Some of these works focused on the analysis and evaluation of connection availability in WDM [4– 6]. While other works focus on availability aware routing for static traffic in centralized systems [7, 8]. There is no previous work that provides a distributed signaling protocol for availability-aware provisioning in distributed controlled WDM mesh networks. In this paper, we propose a new framework for cost-effective connection provisioning to satisfy the connections' availability requirements defined in the SLA for distributed managed WDM mesh networks with dynamic traffic. In this framework, we use the availability analysis for different protection schemes in WDM mesh networks, and efficiently provision the connection using the availability analysis to provide appropriate protection based on a customer's SLA. Moreover, we describe the signaling process of this framework.

The rest of this paper is organized as follows. In Section 2, we present the availability analysis of WDM mesh networks. In Section 3, we present our proposed framework. In Section 4, we carry out a simulation study to evaluate the performance of the proposed framework. Section 5 concludes this paper.

2. Availability analysis in WDM mesh networks

In this section we present the availability analysis of the system that we found in the literature. A system could be a

978-1-4244-2703-1/08/$25.00 ©2008 IEEE

component, path, or connection in a mesh network. For any component, there are "up" times (or Mean Time To Failure, MTTF) and repair times (or Mean Time To Repair, MTTR), and these are independent processes with known mean values. The availability of a system is the portion of time that the system is "up" during the whole service time. A network component's availability can be estimated based on its failure attributes. Upon the failure of a component, it is repaired and restored to operation. This procedure is known as an alternating renewal process. Consequently, the availability of a network component (denoted as a_j) can be calculated as in [9]:

$$a_j = \frac{MTTF}{MTTF + MTTR} \qquad (1)$$

Component failure parameters can be usually obtained from the network operators. In particular, the MTTF of a fiber link is distance related and can be derived according to measured fiber-cut statistics.

2.1. End-To-End Path Availability

Given the route of a path ***i***, the availability of ***i*** (denoted as A_i) can be calculated based on the availabilities of the network components along the path. Path ***i*** is available only when all of the network components along its route are available. Let a_j denote the availability of the j^{th} network component in the route of ***i*** (G_i). A_i can be computed as follows [6]:

$$A_i = \prod_{j \in G_i} a_j \qquad (2)$$

2.2. Availability of Dedicated-Path-Protected Connection

In path protection, connection ***c*** is carried by one primary path and protected by one backup path that is link disjoint with ***P***. By link disjoint, we mean that the backup path for a connection has no links in common with the primary path for that connection. In this study, we require the primary and backup of a connection to be link-disjoint and only consider link failures in the availability analysis.

If the wavelength(s) of the backup path ***b*** are dedicated to connection **c**, then, when primary path ***P*** fails, traffic will be switched to ***b*** if ***b*** is available; otherwise, the connection becomes unavailable until the failed component is restored. ***c*** is "down" only when both paths are unavailable, so it can be computed straightforwardly as follows [6]:

$$A_c = 1 - (1 - A_P) \times (1 - A_b) = A_P + (1 - A_P) \times A_b \qquad (3)$$

Where A_P and A_b denote the availabilities of paths ***P*** and ***b***, respectively.

2.3. Availability of Shared-Path-Protected Connection

In shared-path protection, connection ***c*** is carried by primary path ***P***, and protected by a link-disjoint backup path ***b***; however, the reserved wavelength on each link of ***b*** can be shared by other connections as long as Share Risk Link Group SRLG constraints can be satisfied. Let ***SRLGc*** contains all the connections that share some backup wavelength on some link with ***c***. We denote as ***SRLGc*** the sharing group of ***c***.

The availability of connection ***c*** is affected by the size of ***SRLGc*** and the availabilities of the connections in ***SRLGc***. When one or more primary paths of the connections fail together with ***c***, either ***c*** or some of the failing connections in can acquire the shared backup wavelengths. With the values of ***SRLGc*** connection availabilities, we can compute the availability of a shared-path-protected connection now. Connection will be available if: 1) path ***P*** is available; or 2) ***P*** is unavailable, ***b*** is available, and other primary paths of connections in sharing group also available. Therefore, A_c can be computed as follows [6]:

$$A_c = A_P + (1 - A_P) \times A_b \times \prod_{t_i \in SRLG} A_{t_i} \qquad (4)$$

Where A_P and A_b denote the availabilities of paths ***P*** and ***b*** respectively, and A_{t_i} is the availability of the primary path of the connection in SRLG.

3. Our proposed framework

Our proposed framework uses efficiently a probing mechanism, fixed alternative routing [10- 12], destination routing that intelligently selects the working and protection paths, if necessary, with backward reservation, and a distributed local information signaling algorithm for connection management. In the following subsections, we discuss the details of the control and management protocols used to set up and tear down connections and determine restoration capacity shareability in a distributed manner.

3.1. Compute the K Most Reliable Paths

In order to meet the SLA availability requirement, each node in our proposed framework computes the *k* most reliable paths (KMRPs), the paths with the highest availability, to each other node. The node then saves these paths into the local database in order to use them in the routing process as fixed alternative paths. In our proposed framework we set *k* equal to three as is recommended in the literature. To compute the most reliable paths we used Multiplication-to-Summation conversion technique [7]. Suppose that a single path *P* is used to carry connection ***c***. The availability of ***c*** is equal to the multiplication of the availabilities of the components it traverses. Suppose that path *P* traverses links ***l1,l2,…,ln*** :

$$A_P = A_{l_1} \times A_{l2} \times A_{l_3} \times \ldots \times A_{l_n} \qquad (5)$$

Where A_{l_i} is the availability of link ***i***. If we compute the logarithm of both sides of (5), we can convert the multiplication to summation and obtain

$$\log A_P = \log A_{l_1} + \log A_{l2} + \log A_{l_3} + \ldots + \log A_{l_n} \qquad (6)$$

Since A_P and A_{l_i} are between 0 and 1, log A_P and log A_{l_i} have negative values. Multiplying both sides by -1, we get

$$-\log A_P = -\log A_{l_1} - \log A_{l2} - \log A_{l_3} - \ldots - \log A_{l_n} \qquad (9)$$

Now we can observe that, if the cost of link is defined as a function of its availability (i.e. -log A_{li}), the cost is additive and the path with the minimum cost will be the path with maximum availability (i.e., the most-reliable path). Through this Multiplication-to-Summation conversion technique, a

standard modified shortest-path algorithm (such as a modified Dijkstra or Bellman-Ford algorithm) can be applied to compute the KMRPs. Each node saves each of the KMRPs into the local database with its availability by computing the exponential of -1 multiplied by the cost of the path (i.e. e -(-log A_P)).

3.2. Availability-Aware distributed signaling control Protocol

In a wavelength-routed WDM network, a lightpath must be established between a pair of source and destination nodes before the data can be transferred. A lightpath is a unidirectional end-to-end connection between a pair of source and destination nodes, which may span multiple fiber links and use a single or multiple wavelengths. To establish a lightpath under distributed control, the network must first decide on a route for the connection and then reserve a suitable wavelength on each link along the chosen route.

In our distributed framework, each node in the network is required to maintain a routing table that contains an ordered list of KMRPs to each destination node. In addition to the static routing table, each node also maintains another local database for dynamic information. This database reflects the local resource usage at that node, e.g. the status of wavelength usage, as well as sharing information that contains information about the lightpaths whose shared backup paths traverse that node (see figure 1). This information is required to assist our framework in determining whether a wavelength on the outgoing link is shareable and to compute the availability in the case of shared protection.

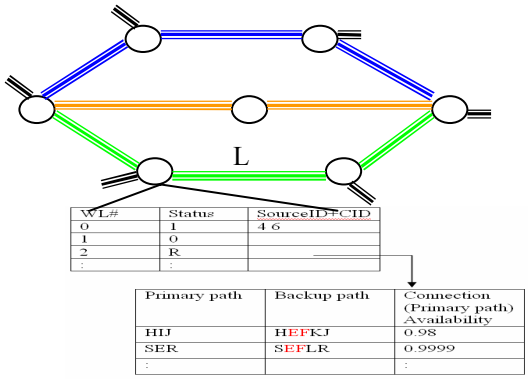

Figure 1: Local database for outgoing link "L"

The major procedures involved in the establishment of a lightpath can be described as follows:

- When a new connection request arrives in the network, the source node prepares a probe message (PROB) for each candidate path (i.e. for each MRP). These messages contain information about candidate the paths including the connection ID, the requested availability level of the connection, the availability of the path, the link state of outgoing links, and the other two alternative paths each with vector of values (say, WP2SH and WP3SH) for the purpose of probing the path as a shared protection path for other candidate. Each value of the vector belongs to one of the outgoing wavelengths and represents the multiplication of the availabilities of the working paths of the connections protected by that wavelength. After preparing the PROB messages, the source node sends these three PROB messages toward the destination node through the three KMRPs link-disjoint k-shortest paths in parallel to collect the recent link state information from the local databases in visited intermediate nodes.
- Upon receiving the PROB message, the intermediate nodes examine the local link-state information and update the request message as follows:

  They check the free wavelengths in the outgoing links, and intersect them with the set of free wavelengths in the last link included in the received PROB. They update the shareability information in the received PROB by examining the shareability of each channel along the probed path with the shared protection path for each one of the other probed paths (i.e. the other candidates). This is done by checking each wavelength in the outgoing probed link; if it is sharable to the candidate working path then the node increases the value belonging to that wavelength in the received vector by one. Otherwise, if the wavelength is not sharable, the node sets the value of that wavelength to zero. It then writes the results into the PROB message and transmits it to the next node in the candidate path.

  By updating the PROB message fields at each intermediate node, the destination node receives the latest information about the usage of each wavelength along each candidate path so that it can select the working or protection path(s). Each intermediate node determines the shareability of the wavelength by retrieving the candidate working path of the current connection from the received PROB packet and checks with its shareability database to see whether the candidate working path belongs to the same SRLG of the working paths of the connections protected by this wavelength. If it is not belong to the same SRLG, it is sharable, then multiplies the value belonging to that wavelength in the received vector by the availabilities of the working paths of the connections protected by that wavelength, excluding the redundant connection. Otherwise, if it is not sharable, the node sets the value of that wavelength to zero.
- When receiving the three connection probes, the destination node first examines the sets of the remaining wavelengths that are free. If all of the sets are empty, it is indicated that none of the wavelengths could be utilized in the three candidate paths. Therefore, a Negative Acknowledgement (NAK) message will be sent back to the source in the reverse direction through the primary route. Upon receiving a NAK, the source node blocks the request. Otherwise, the destination node must pick one free wavelength from the three results if one or more sets are not empty; an adaptive routing mechanism selects the optimal path as well as the wavelength for the primary working path. The destination node also has the ability to select a backup path, either dedicated or shared, at the same time that it selects the primary path. This issue is discussed below. After selecting the path(s), the destination node starts backward reservation. Therefore, a

Reservation (RES) message will be sent back to the source node in the reverse direction along selected path(s). Therefore, a RES message will be sent back to the source node in the reverse in direction along selected working and backup path(s) in parallel.

- Upon receiving a RES, the intermediate nodes first examine whether the requested wavelength λ has been occupied. If it has not been occupied, the optical cross connect (OXC) will be tuned in order to setup the optical channel at wavelength λ and the RES message will be forwarded to the source node. Otherwise, if the wavelength has been occupied, the received RES message will be deleted, and, at the same time a NAK message will be forwarded to the source node and a Release (REL) message will be forwarded to the destination node to release the reserve resources. Note that we have explained the reservation process in the case of a working path or dedicated path. In the case of shared protection path reservation, allocating resources along the protection path is different since it does not involve the switch configuration; instead, the intermediate node updates the shareability database by adding information about the new connection. This information includes the ID of the new connection and the route along which the working path has been selected as well as the availability of that working path, all of which is added to the RES message of the shared protection path.
- Upon receiving RES, the source node confirms that the connection has been setup and begins transferring data. When the transmission ends, the source node sends a REL message to the destination node to disconnect the connection and release the resources.

A connection can be either unprotected or protected. In order to further reduce network costs without sacrificing service availability, we can protect a connection through either through dedicated-path-protected or shared-path protection based on the availability requirements of this connection and of all the connections in its sharing group. The destination node decides to assign a route(s) and wavelengths to the connections using a heuristic method. This method selects the working path and decides which type of protection should be provided in order to satisfy the required availability value, say SLA_v, of the connection while minimizing the resource usage. Algorithm 1 describes path(s) and wavelength(s) assignment. This algorithm run by the destination node of the connection to assigns the shortest path that satisfies the SLA_v if such path exists and has a free wavelength. Otherwise, it selects the shortest working and shared protection paths to the connection and computes the availability of this candidate combination. If the availability of one of the combinations satisfies the SLA_v and has free wavelengths, the algorithm assigns them to the connection. If no shared protection availability can satisfy the SLA_v the algorithm tries to select working and dedicated

Algorithm 1: Selecting the shortest reliable path(s) and its wavelength(s)

```
Let PP1 is the shortest path of the KMRPs;
Let PP2 is the second shortest path of the KMRPs;
Let PP3 is the third shortest path of the KMRPs;
Let SLA_v is the required availability of the connection.
ProtectionType = 0; // No path(s) have been selected for the connection
w =1;
While (w <= 3 and ProtectionType !=0 )
    If Avail(PPw) >= SLA_v and there is a free wavelength in PPw then
        ConnectionWorkingPath = PPw;
        ProtectionType = 1; // One of KMRPs satisfy the required availability (Unprotected)
    Endif
    w=w+1; // to check next working path candidate
loop;
If (ProtectionType == 0 ) then // nothing assigned yet
    w =1;
    While (w <= 3 and ProtectionType !=0 )
        s =1;
        While (s <= 3 and ProtectionType !=0 )
            If ( w != s and there is a free wavelength in PPw and there is a sharable or free wavelength in PPs) then
                Let Avail (PPw + PPs) is value of equation (4) by considering PPw as a working path and PPs as shared protection path;
                If Avail(PPw + PPs) >= SLA_v then
                    ConnectionWorkingPath = PPw;
                    ConnectionSharedProtectionPath = PPs
                    ProtectionType = 2; // satisfy the required availability (Shared Protection)
                EndIf
            EndIf
            s=s+1; // to check next protection path candidate
        loop;
        w=w+1; // to check next working path candidate
    loop;
If (ProtectionType == 0 ) then // nothing assigned yet
    w =1;
    While (w <= 3 and ProtectionType !=0 )
        d=1;
        While (d <= 3 and ProtectionType !=0 )
            If ( w != d and there is a free wavelength in PPw and there is a free wavelength in PPd) then
                Let Avail (PPw + PPd) is value of equation (3) by considering PPw as a working path and PPd as dedicated protection path;
                If Avail(PPw + PPd) >= SLA_v then
                    ConnectionWorkingPath = PPw;
                    ConnectionDedicatedProtectionPath = PPd;
                    ProtectionType = 3; // satisfy the required availability (dedicated Protection)
                EndIf
            EndIf
            d=d+1; // to check next protection path candidate
        loop;
    w=w+1; // to check next working path candidate
loop;
If (ProtectionType != 0 ) then
    Start the reservation process;
Else
    Block the connection ;
EndIf
```

protection paths to satisfy the SLA_v of the connection before deciding to block the connection if none of the above choices is sufficient.

4. Performance Evaluation

To evaluate the performance, we carry out connection setup time analysis and a simulation study to show the performance of the presented protocol in terms of connections setup time and the connections blocking probability.

4.1. Connections setup time analysis

In this section we describe analytically the Connection Setup Time (CST), the time the framework takes to setup a lightpath. First, to give some notations and assumptions:

- Message processing time at each node is p.
- Time to configure, test and setup a switch is c.
- Time to configure, test and reserve as shared resource wavelength s.
- Average propagation delay on each fiber is D.
- Number of hops along the longer candidate path is h_c.
- Number of hops along a working path is h_w.
- Number of hops along a protection path is h_p.

CST of unprotected connections

Let T_{Prob} be the time to probing the candidate paths, let T_D^w be the time to setup a working path, and let CST_U be the connection setup time

$$T_{Prob} = h_c \times D + (h_c + 1) \times p .$$

$$T_D^w = T_{Prob} + h_w \times D + (h_w + 1) \times (p + c) .$$

$$CST_U = T_D^W .$$

CST of the shared protected connections:

As before, let T_{Prob} be the time to probe the candidate paths, T_S^w and T_S^P be the time to setup a working path and a protection path respectively, and let CST_S be the connection setup time.

$$T_{Prob} = h_c \times D + (h_c + 1) \times p .$$

$$T_S^w = T_{Prob} + h_w \times D + (h_w + 1) \times (p + c) .$$

$$T_S^P = T_{Prob} + h_p \times D + (h_p + 1) \times p .$$

$$CST_S = Max(T_S^W, T_S^P)$$

CST of the dedicated protected connections:

Let T_{Prob} be the time to probing the candidate paths, T_D^w and T_D^P be the time to setup a working path and a protection path respectively, and let CST_D be the connection setup time.

$$T_{Prob} = h_c \times D + (h_c + 1) \times p .$$

$$T_D^w = T_{Prob} + h_w \times D + (h_w + 1) \times (p + c) .$$

$$T_D^P = T_{Prob} + h_p \times D + (h_p + 1) \times (p + c) .$$

$$CST_D = Max(T_D^W, T_D^P) .$$

Note that the request probing and reservation in both schemes are done in parallel because the setup time is the maximum setup time of the working path and protection path. Moreover, unlike dedicated protection path, the shared protection path does not require switch configuration at each node along the path, but requires each node to update its local database.

4.2. Simulation study

The performance of the proposed protocol is also evaluated via extensive simulations of the mesh based 14-nodes NSFnet. As shown in Figure 2, all links in the network are assumed to have one fiber and each fiber has the same number of wavelength. Here we show the results for the case of a single fiber having 16 wavelengths and with no wavelength converters. We also assume the lightpaths to be bidirectional. Connection requests arrive as a Poisson process with mean arrival rate λ. The holding time μ of each connection is exponentially distributed. Thus the load is given by λ/μ. The destination of each request is uniformly distributed. The channel availability model and the corresponding MTTF and MTTR values in [6] are used to obtain availability. The availability requirements of the requests are uniformly distributed among five classes: 0.999, 0.9993, 0.9995, 0.9998 and 0.9999.

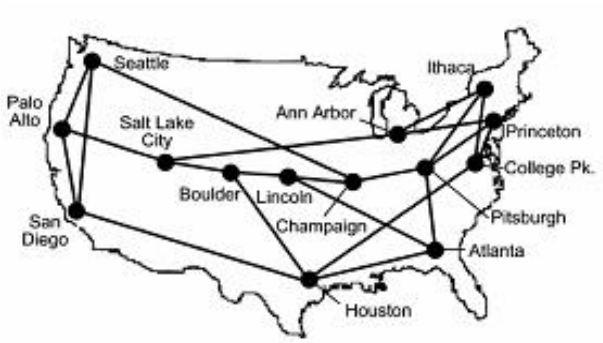

Figure 2: A 14-node NSFnet backbone topology.

We compare our proposed framework with our previous proposed protocol in [13] to show the enhancement done by the intelligent routing at the destination node of the connection. Figure 3 shows a comparison between the first version and our new proposed version of the availability aware framework in terms of the network blocking probability (BP). Network performance is better under our new provisioning framework than under the first version of the provisioning framework. This is due to efficient resource utilization done by the intelligent destination routing, which assigns the shortest reliable path(s) to provision the connections rather than assigning the most reliable path(s) as in [13]. Notice here, in [13] the authors show that the first version of the provisioning framework gives better performance than the existing protection schemes (i.e. the dedicated and the shared protection schemes). That is because the first and the new proposed frameworks either do not protect the connection, or protect it with shared or dedicated protection based on the required level of availability of that connection. Moreover, as can be seen from the figure, it is observed that when the load is very small, the blocking probabilities as well as their

difference are also very small. As the load increases, the blocking probabilities increase remarkably and the difference becomes significant. However, this is a result of the fact that blocking at higher loads is due to insufficient resources as well as the contention that exist in the distributed controlled networks.

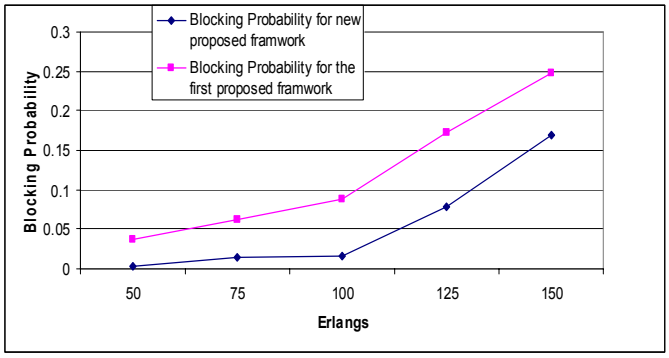

Figure 3: Blocking probability vs. load.

Table 1 shows the blocking probability for each class of service with the first and new proposed frameworks under light, moderate and heavy loads. Network performance is better under our new provisioning framework than under the first version of the provisioning framework with all class of services. However, both frameworks provide relatively small blocking probability. That is because of their parallel mechanism that probes many paths as a candidate working and protection paths and sets them up in parallel instead of probing one path as working path and anther one as backup path.

Table 1: Blocking Probability for each class of service

Erlangs	Version	Class 1	Class 2	Class 3	Class 4	Class 5
50	First version	0.05156	0.03916	0.01994	0.03145	0.04925
	New version	0.00408	0.00502	0.00438	0.00250	0.00302
100	First version	0.09750	0.08534	0.07733	0.08437	0.09950
	New version	0.01736	0.01406	0.01702	0.01498	0.01407
150	First version	0.25676	0.24849	0.22811	0.24563	0.25729
	New version	0.16080	0.16566	0.15564	0.18522	0.17688

5. Conclusions

In this paper, we present an improvement for our novel distributed availability-aware routing and wavelength assignment framework for mesh-based wavelength-division multiplexed (WDM) optical networks with intelligent destination routing. Our proposed framework probes the k most reliable paths in parallel. The probing technique used in this framework is the first probing technique that probes each path as both a candidate working path and a candidate shared protection path at the same time. Moreover, we propose to use connection availability as a metric for providing differentiated protection services in WDM mesh networks. Based on the availability information collected, our provisioning strategy selects an appropriate level of protection to each connection. The effectiveness of our provisioning approaches is demonstrated through simulation results. We have shown that the presented framework reduces the blocking probability for all service classes.

6. References

[1] J. Doucette, M. Clouqueur, and W. D. Grover, "On the availability and capacity requirements of shared backup path-protected mesh networks," SPIE Optical Networks Mag., vol. 4, no. 6, pp. 29–44, Nov. 2003.

[2] H.T. Mouftah and P.-H. Ho, "Optical Networks- Architecture and Survivability", Kluwer Academic Publishers, 2003, ISBN 1-4020-7196-5.

[3] S. (Ramu) Ramamurthy, L. Sahasrabuddhe, and B. Mukherjee, ``Survivable optical WDM networks," *IEEE/OSA Journal of Lightwave Technology*, vol. 21, no. 4, pp. 870-883, April 2003.

[4] H. Naser and H.T. Mouftah, "Availability Analysis and Simulation of Shared Mesh Restoration Networks", Proceedings Ninth IEEE International Symposium on Computers and Communications (ISCC2004), Alexandria, Egypt, June 2004, pp. 779-785.

[5] D. Arci, G. Maier, A. Pattavina, D. Petecchi, M. Tornatore,"Availability models for protection techniques in WDM networks," in Proceedings, DRCN 2003, Oct. 2003.

[6] Jing Zhang, Keyao Zhu, Hui Zang, Matloff, N.S., and Mukherjee, B.,"Availability-Aware Provisioning Strategies for Differentiated Protection Services in Wavelength-Convertible WDM Mesh Networks," IEEE transaction on Networking, vol. 15, no. 5, pp. 1177-1190, Oct. 2007.

[7] Q. Guo, Pin-Han Ho, A. Haque, and H. T. Mouftah, "Availability-Constrained Shared Backup Path Protection (SBPP) for GMPLS-Based Spare Capacity Reconfiguration", *in Proceedings IEEE International Conference on Communications (ICC),* 2007

[8] Pin-Han Ho, J. Tapolcai, H. T. Mouftah and C. –H. Yeh, "Linear Formulation for Path Shared Protection", accepted by IEEE International Conference on Communications (ICC), France, June 2004.

[9] K. S. Trivedi, Probability and Statistics with Reliability, Queuing, and Computer Science Applications. Englewood Cliffs, NJ: Prentice-Hall, 1982.

[10] S. Ramamurthy and B. Mukherjee, "Fixed-alternate routing and wavelength conversion in wavelengthrouted optical networks," Proc. of IEEE Globecom '98, Vol. 4, Nov. 1998 , Australia, pp. 2295- 2302.

[11] H. Harai, M. Murata, and H. Miyahara, "Performance of alternate routing methods in all-optical switching networks," Proc. of IEEE Infocom '97, Vol. 2, Apr., 1997, Kobe, Japan, pp. 516-524.

[12] S. Subramaniam and R. A. Barry, "Wavelength assignment in fixed routing WDM networks," Proc. of ICC '97, Vol. 1, Jun. 1997, Montreal, Canada, pp. 406-410.

[13] Emad M. Alsukhni, and H. T. Mouftah, "A Novel Distributed Availability-Aware Provisioning Framework for Differentiated Protection Services in Optical Mesh Networks," , under review in CCECE 2008, available upon request.