Protection and Minimal Interference in WDM Mesh Networks

Marco D. D. Bicudo[1], Igor M. Moraes[1], Rafael P. Laufer[1],
Daniel de O. Cunha[1], Pedro B. Velloso[1,2], and Otto Carlos M. B. Duarte[1]

[1]Grupo de Teleinformática e Automação (GTA)
Universidade Federal do Rio de Janeiro
Rio de Janeiro, RJ, Brazil

[2]Laboratoire d'Informatique de Paris 6 (LIP6)
Université Pierre et Marie Curie - Paris VI
Paris, France

***Abstract*— Due to the pre-computed spare capacity of conventional WDM protection mechanism, network resource is inefficiently used. Nevertheless, fault recovery mechanisms can not be neglected during network design, since a single fiber failure may causes a huge date loss. This work evaluates different protection mechanisms and their performance-specific characteristics. Then, it presents a novel mechanism, which reduce resource interference in connection establishment. The blocking probability and the connections availability are examined as performance metrics of the protection mechanisms. Our simulations employ conventional mechanisms as well as the proposed one in two network topologies, handling multiple-failure scenarios.**

I. Introduction

A conventional IP optical transport network model presents either ATM (Asynchronous Transfer Mode) or SONET (Synchronous Optical Network) layers. Such transport network tends to be rather static, and presents fixed-bandwidth connections (e.g., SONET OC-n), which are usually set up manually. This model is not well adapted to fulfill the existent Internet data traffic demands, such as bandwidth and low end-to-end latency, and its dynamic. The electronic packet processing, which inserts a delay in each network node, and the inefficient resource usage, which leads to less available resources, which occurs in less bandwidth to the connections, are the main reasons for this lack of performance. A network model more suited to transport dynamic data traffic, presented by [1] and [2] among others, is the multilayered IP/GMPLS(Generalized Multiprotocol Label Switching)-over-WDM. The GMPLS [3] is a set of protocols extensions that includes the MPLS platform and its features, such as traffic engineering and the connection oriented concept, provided by the LSP (Label Switched Path). Moreover, the GMPLS permits the network set up transparent lightpaths dynamically, introducing the Automatic Switched Optical Network (ASON) concept, as described by [4]. In an ASON network, implement protection mechanisms is a much easier job than it would be in an ATM or SONET network, since the lightpath establishment can use the GMPLS protocol set to set up the lightpath automatically.

Due to the frequent occurrence of fiber cuts and the traffic loss a failure can occur, network survivability becomes a critical concern in network design and operation. As networks migrate from ring based networks to mesh based networks, because its inefficient resource usage, researches on survivable WDM mesh network have received increasing attention like [5], [6], [7] and [8]. Most of the works suppose single-failure scenarios. Nevertheless, as the knowledge on the issue has matured, more realistic studies should be made (e.g., multi-failure scenarios).

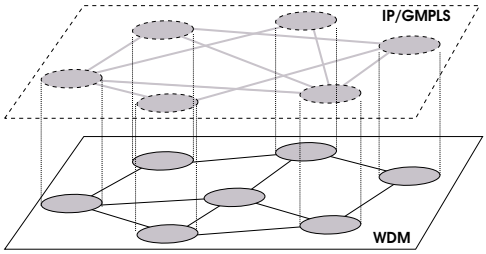
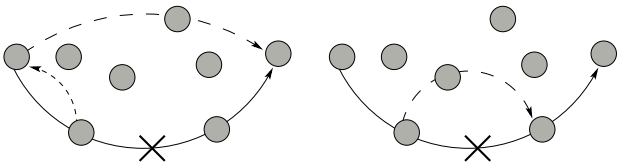


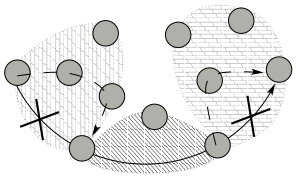
Fig. 1. Physical and Virtual Topology

Some researches use an approach from the IP/GMPLS layer, employing characteristics of this layer, like versatility, greater granularity and good configuration flexibility, to improve the protection mechanism performance. The BIRA and HIRA algorithm, proposed by Zheng et al. [9], and the Kodialam's algorithm proposed in [10], are some of those. Other researches, like [11], [12] and [13], have an approach from the WDM layer, achieving a smaller recovery time, because of the lower granularity and the lack of any extra signaling needed to execute the protection procedure.

This article analyses the performance of conventional protection mechanisms in optical networks. Then, it presents a dynamic WDM protection approach that outperforms the conventional ones, and analyzes its impact on blocking probability and connection availability. The rest of the article is organized as follows. Section II introduces protection and restoration basic concepts and explains the advantages and disadvantages of protection in the WDM layer and in the IP/GMPLS layer. Section III presents conventional WDM protection mechanisms and the proposed mechanisms. Section IV describes how the simulation is done, it presents the simulation platform and network topologies used. Section V presents the results and elaborates the rationale used to conclude. Section VI is our conclusion.



(a) Path Protection (b) Link Protection



(c) Sub-path Protection

Fig. 2. Protection Mechanisms

II. Basic Concepts in Fault Management

Fault recovery mechanisms in optical mesh network are divided, basically, in two classes. Mechanisms that pre-compute and preplan the backup resources, named protection, and mechanisms that compute backup resources dynamically, named restoration. Generally, dynamic restoration mechanism uses network capacity more efficiently because it does not allocate spare capacity in advance. It establishes the backup path only if a failure affects its primary path. On the other hand, protection mechanism does allocate it in advance. This inefficient pre-allocating property penalizes the acceptance of future connections. Although protection mechanism penalizes the acceptance of future connections, its recovery time is tremendously smaller than restoration.

A protection mechanism can be classified in two aspects: the layer it is implemented; and if it protects the path, the sub-path or the link. In path protection, illustrated in Fig. 2(a), traffic is rerouted through a backup path once a link failure occurs on its primary path. The primary and backup path must be link disjoint, so that a link failure would not able to affect both paths. In sub-path protection, presented by Ou et al. [14] and Zang et al. [15], is an alternative mechanism to reduce recovery time. Compared to path protection, the sub-path protection, illustrated in Fig. 2(c), can achieve smaller recovery time, since the signaling does not need to traverse the entire path back to the source to initiate the protection procedure. On the other hand, sub-path protection sacrifices resource utilization. The link protection, illustrated in Fig. 2(b), is the fastest mechanism in terms of recovery time, but, because its tremendous detriment of resource utilization, is not considered a probable solution.

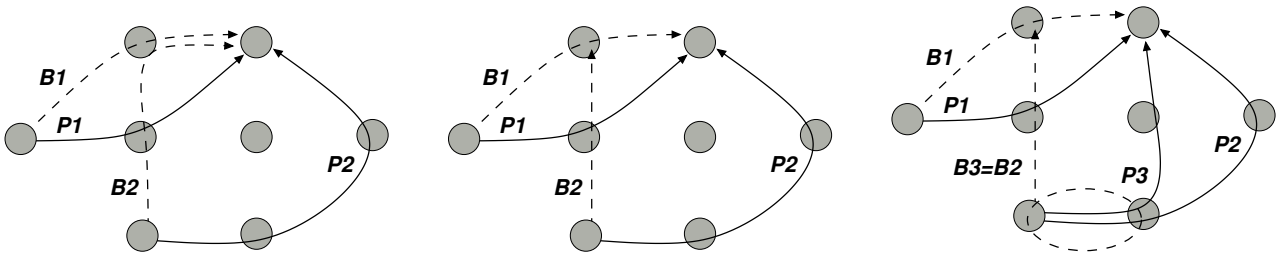
Survivability on IP/GMPLS-over-WDM networks can take place in the WDM layer or in the IP/MPLS layer. On the former, every lightpath is protected by a link disjoint backup lightpath. On the latter, every LSP is protected by a link disjoint backup LSP. The WDM protection is faster than MPLS protection; it does not depend on signaling to detect failure. Even if MPLS layer gets an integrated implementation, which would enable it to not depend on signaling to detect failures, as proposed by [9], its recovery time would not be lower than WDM protection recovery time. Since a single lightpath can transport a tremendously large number of LSPs, the MPLS layer would still get a heavier restoration overhead processing. The WDM protection drawback is the isolation between primary and backup lightpath. By isolation we mean that once the lightpath is assigned to be a backup, it will not be used unless for backup purposes. In MPLS protection, on the opposite, primary and backup LSPs can coexist in a lightpath. Since, in the MPLS protection, the WDM layer does not distinguish primary lightpath and backup lightpath, the co-existence of primary and backup LSPs leads to a more efficient resource utilization.

III. WDM Protection

Due to the legacy SONET networks usage in telecommunication, resilience studies has been made in WDM mesh networks to achieve the SONET's performance, in order to replace it. Despite MPLS protection being more efficient than WDM protection, the WDM protection is the only capable of offering the 50 ms recovery time necessary for the SONET substitution. WDM-shared protection is an alternative for the WDM protection mechanism that improves the resource usage efficiency. WDM-shared allows two or more backup paths to share wavelength channels, as long as their primary path comply with the *Shared Risk Link Group*(SRLG) constraint. According to the SRLG constraint, backup paths whose primary path can fail simultaneously can not share resources. In other words, connections that want to share backups must not have primary links in common, even if the wavelength channel is different. The WDM and WDM-shared protection are illustrated in Fig. 3(a) and Fig. 3(b), respectively. Here, we can see the different behavior of both mechanisms. It is evident that WDM-shared protection can efficiently reassign resources previously allocated to backup lightpath $B1$ to backup lightpath $B2$. Meanwhile, WDM protection uses the network resources inefficiently, reallocating resources to $B2$ unnecessarily, as depicted in Fig. 3(a). Obviously, this behavior leads to a higher blocking probability since future connections have less network resources available.

A. Proposed WDM-shared-non-SRLG Protection

Despite the better WDM-shared resource efficiency than WDM protection, there are improvements to the path establishment procedure that could improve the WDM protection performance. Our proposed mechanism, called WDM-shared-non-SRLG protection, accomplishes the objective and, therefore, reduces perceptibly blocking probability. This reduction is obtained increasing the backup path *share-ability*. We propose the constraint for sharing a backup resource base itself upon the percentage of primary path shared links. The algorithm determines whether the establishing backup path



(a) WDM Protection (b) WDM-shared Protection (c) WDM-shared-non-SRLG Protection

Fig. 3. WDM Protection Mechanisms

can share resources based on the *SRLG-percentage* constraint. The SRLG-percentage denotes the maximum percentage of primary links shared. Taking the Fig. 3(c) example, the SRLG-percentage of primary path $P2$ to $P3$ is 25%, since one of the four primary links is shared with $P3$, while the SRLG percentage of primary path $P3$ to $P2$ is 33%, since one of the three primary links is shared with $P2$. Note that the maximum value of the SRLG-percentage should be considered because it is a unidirectional property. If only one of the values is considered, the result can mislead to an unfair behavior.

Fig. 3 illustrates how WDM-shared-non-SRLG differs from WDM-shared. The behavior of the non-SRLG mechanism is illustrated in Fig. 3(c). Obviously, the primary paths $P2$ and $P3$ could not share backup $B2$ if employed a WDM-shared protection. For matters of share ability, the novel mechanism lets connection 2 share backup path $B2$ with connection 3 and, therefore, improves acceptance of future connections. Note that, there is a trade of between blocking probability and availability. The non-SRLG mechanism, gain in blocking probability, but at the cost of sacrificing availability.

The mechanism consists, basically, of three procedures executed successively: the link weight scaling; the shortest path computation; and the wavelength channel reservation. These three procedures are executed twice. The first time the procedures compute the primary path. The second time they compute the backup path. The first procedure is an algorithm that assigns weights to the network graph edges. The weights assigned to the edges depend on network state and on specific link parameters, such as usage percentage. If link does not have available resources or has failed, the weight scales to infinite. Otherwise, the weight scales based on the percentage of usage, as depicted in Eq. 1. In Eq. 1 α is unit, but one could vary it to study network share-ability response. The second procedure consists of a shortest path algorithm to compute the path in the weighted graph, such as Dijkstra's. The third procedure traverses the entire path determining which wavelength channel should be used in each link. After the first execution round, and the primary path establishment success, the second round is executed to establish the backup path. The three procedures execute like the first round, only with two adjustments. The first procedure must scale the edges used by primary path to infinite, as a prioritized rule. Doing so, the shortest path algorithm is forced to not consider the primary links as candidates for backup path. If backup sharing is used, the third procedure should assure if it is possible to share a wavelength channel already reserved to other backup path, in addition to its regular routines. The SRLG-percentage parameter of the establishing connection with the connections already using the wavelength channel decides whether or not the channel will be shared.

$$weight = weight \times \alpha(\%\ wlen\ usage) \tag{1}$$

When failure occurs the recovery operations verify the availability of the backup path for each connection using the failed link. If the backup is available, the primary path is switched to its backup path. Note that, if backup sharing is used, the backup availability test must verify the other connections associated with this backup path to confirm the inactivity of the latter.

IV. Simulation

The simulation compares the performance of different protection mechanisms. It is executed on two network topologies with different number of nodes, but with same node connectivity. The first network, illustrated in Fig. 4, consist of 6 nodes interconnected by 9 links. The other network is the NSFNet, illustrated in Fig. 5, with 16 nodes and 23 links. Both networks were simulated with four wavelength channels per link. Traffic arrival follows a Poisson distribution with 2 hours of mean. The connection holding time is exponentially distributed, and its mean is varied to get the different network loads. The source and destination pair is randomly chosen among all nodes in the network. The event of a link failure is exponentially distributed with 50 days per 1,000 km of mean, and the fiber failure restoration is exponentially distributed with 12 hours of mean, as presented in [13]. Each simulation round takes as much time as necessary to complete a mean of 100,000,000 connections per node. The simulation is repeated several times until achieve a 95 percent of confidence level. Confidence intervals are shown in the graphics.

The simulations compare the performance of both networks analyzing the blocking probability and availability metrics.

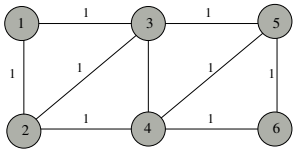


Fig. 4. Network 1

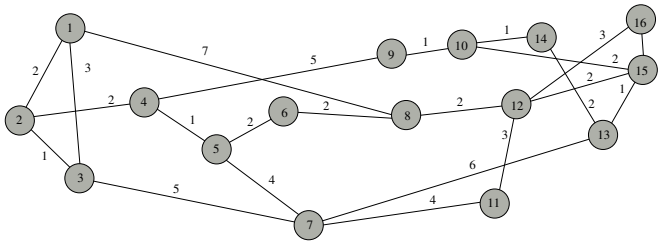


Fig. 5. Network 2

The simulator platform was programmed in C++, utilizing the Standard Template Library (STL).

V. Results

The graphics in Fig. 6 and 7 show the blocking probability and availability behavior for network 1, respectively. The graphics in Fig. 8 and 9 show the blocking probability and availability behavior for network 2, respectively. The figures show the performance of the two networks when applied no protection, WDM (dedicated), WDM-shared, WDM-shared-non-SRLG-25% and WDM-shared-non-SRLG-50% protection mechanisms. The metrics response was equivalent for both simulated networks. As predicted, the blocking probability with no protection mechanisms is lower than with other protections, its availability is the worst though. On the contrary, the (dedicated) WDM protection presents the highest blocking probability, due to its inefficient resource usage. Note that, for all protections, network 2 presents lower blocking probability than network 1. This behavior does not surprise, even though the node connectivity and load per node is the same for both networks. This network 2 performance obtained is expected, mostly, because its considerably larger node number, which enables the resource assignment statistical multiplexing. In our case, the resource statistical multiplexing means that a large network enables the protection avoiding a location with deficient capabilities, such as an unexpected connection burst or equipment failure.

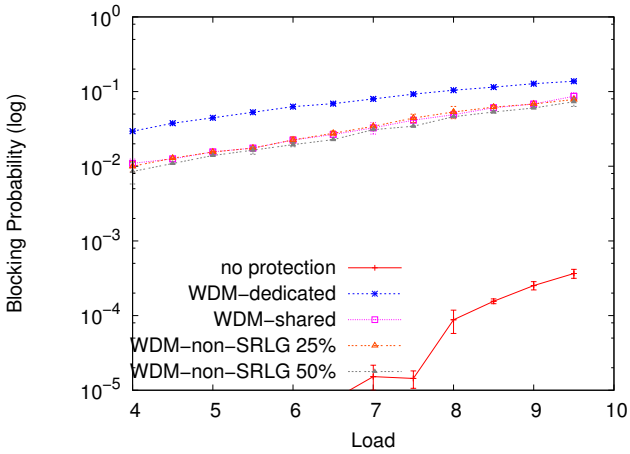


Fig. 6. Network 1: Blocking Probability

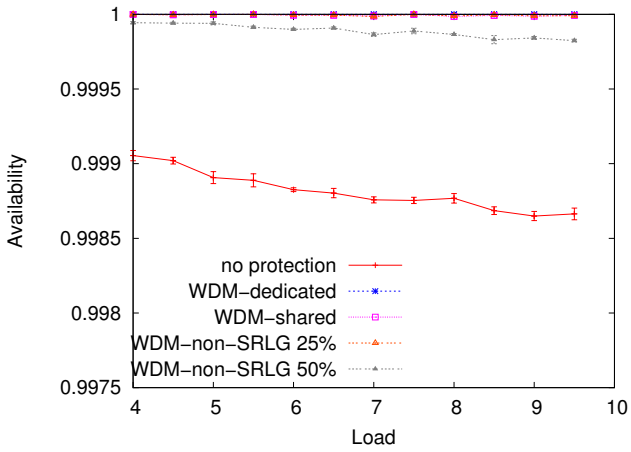


Fig. 7. Network 1: Availability

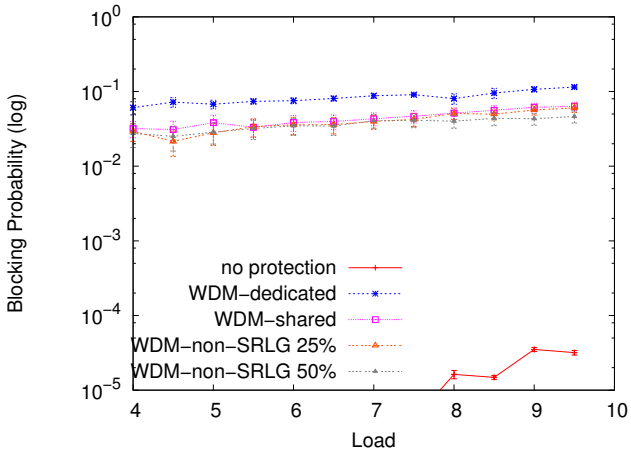


Fig. 8. Network 2: Blocking Probability

The Fig. 8 shows that the protection non-SRLG with 50% outperforms all other mechanisms in blocking probability. Its drawback, illustrated in Fig. 9, is its availability detriment. Due to the backup contention, increasing the SRLG-percentage leads to blocking probability increase, but, on the other hand, decreases the availability, which is not desired. This availability detriment denotes the protection mechanism inefficiency to offer survivability upon failure.

Theoretically, the availability should be only affected by the failure rate. But simulations show that increasing network load reduces the availability. This behavior is due to the higher number of affected connections upon a failure event. This is an occurrence not expected to occur frequently when the network is not heavily loaded. In the opposite situation, where few link

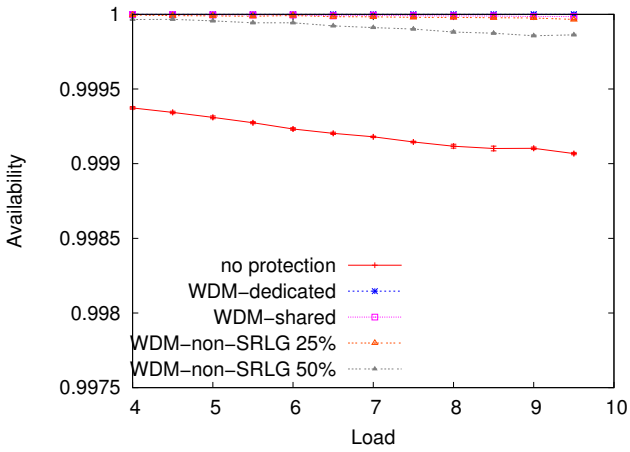


Fig. 9. Network 2: Availability

failures affect connections due to the light loaded network, the availability is less sacrificed. It is worth mentioning that, in network 2 simulations, the protection mechanisms responses distinguishes reasonably from each other just when the network load is considerably higher than applied in network 1. This is so because of the statistical multiplexing property, as explained earlier, which leads to larger networks behave more efficiently during heavy load.

VI. Conclusion

The IP/GMPLS-over-WDM network model is pointed out to be the most appropriated for the future usage of the IP transporting optical networks. The GMPLS brings features, and protocols like OSPF-TE and CR-LDP, enabling easier the management and operation of these networks. This set of protocols, allied to the actual necessities, offers theoretical and operational background for protection and restoration research area in optical IP mesh WDM networks.

In this article, we address the problem of providing protection capability to dynamically arriving lightpath connections in mesh WDM networks. We study several conventional protection mechanisms, and compare their performance with the proposed mechanism. The proposed mechanism graphics show a trade of between blocking probability and availability. The mechanism allows the network operator chose to prioritize either the availability or the blocking probability in the client's SLA contract. To find the mean term between protecting connection and traffic engineering optimization, the network operator should adjusts the SRLG-percentage. Another interesting result is the reduction of blocking probability induced by the network share ability increase. The availability is affected by the network load, because a link failure affects more connections when the network is heavily loaded network.

Acknowledgment

This work has been supported by CNPq, CAPES, FAPERJ, FINEP, RNP and FUNTTEL.

References

[1] J.-P. Vasseur, M. Pickavet, and P. Demeester, *Network Recorver: Protection and Restoration of Optical, SONET-SDH, IP, and MPLS*, 1st ed. Morgan Kaufmann Publ., 2004.

[2] S. Maesschalk, D. Colle, A. Groebbens, C. Develder, I. Lievens, P. Lagasse, M. Pickavet, P. Demeester, F. Saluta, and M. Quagliotti, "Intelligent Optical Networking for Multilayer Survivability," *IEEE Communications Magazine*, pp. 42–9, Jan. 2002.

[3] E. Mannie, "Generalized Multi-Protocol Label Switching (GMPLS) Architecture," *Internet RFC 3945*, Oct. 2004, pROPOSED STANDARD.

[4] D. Colle, S. Maesschalck, C. Develder, P. Heuven, A. Groebbens, J. Cheyns, I. Lievens, M. Pickavet, P. Lagasse, and P. Demeester, "Data-Centric Optical Networks and Their Survivability," *IEEE JSAC*, vol. 20, no. 1, pp. 100–09, Jan. 2002.

[5] G. Ellinas, A. G. Hailemariam, and T. E. Stern, "Protection Cycles in Mesh WDM Networks," *IEEE JSAC*, vol. 18, no. 10, pp. 1924–37, Oct. 2004.

[6] G. Mohan and C. S. R. Murthy, "Lightpath Restoration in WDM Optical Networks," *IEEE Network*, pp. 24–32, 2000.

[7] O. Gerstel and S. Ramaswani, "Optical Layer Survivability - An Implementation Perspective," *IEEE JSAC*, vol. 18, no. 10, pp. 1885–99, Oct. 2000.

[8] L. Sahasrabuddhe, S. Ramamurthy, and B. Mukherjee, "Fault Management in IP-over-WDM Networks: WDM Protection vs. IP Restoration," *IEEE JSAC*, vol. 20, no. 1, pp. 21–33, Jan. 2002.

[9] Q. Zheng and G. Mohan, "Protection Approaches for Dynamic Traffic in IP/MPLS-over-WDM Networks," *IEEE Communications Magazine*, pp. S24–9, May 2003.

[10] M. Kodialam and T. Lakshman, "Integrated Dynamic IP and Wavelength Routing in IP over WDM Networks," in *Proc. IEEE INFOCOM*, 2001.

[11] J. Wang, L. Sahasrabuddhe, and B. Mukherjee, "Path vs. Sub-Path vs. Link Restoration for Fault Management in IP-over-WDM Networks," *IEEE Communications Magazine*, vol. 40, pp. 2–9, Nov. 2003.

[12] S. Ramamurthy and B. Mukherjee, "Survivable WDM Mesh Networks: Part I, Protection," in *ACM Sigcomm*, 1999.

[13] J. Zhang and B. Mukherjee, "A Review of Fault Management in WDM Mesh Networks: Basic Concepts and Research Challenges," *IEEE Network*, pp. 41–8, Apr. 2004.

[14] C. Ou, H. Zhang, and Bmukherjee, "Sub-Path Protection for Scalability and Fast Recovery in Optical WDM Mesh Network," in *Proc. OFC*, Mar. 2002.

[15] J. Zhang, "Service Provision to Provide Per-Connetion-Based Availability Guarantee in WDM Mesh Network," in *Proc. OFC*, Mar. 2003.