approach is the following: when a XC receives a connection request, it first selects and establishes the service path, then sends a restoration path request to the path server along with the service path information. The server selects an efficient restoration path based on the service priority and other network usage. If the path server is unable to select a restoration path due to insufficient capacity, it has the option to re-optimize the restoration paths of some or all previously established connections and then download new information to the source nodes. During a failure event, no communication exchange is required between XC and the restoration path server, and the restorations start simultaneously at different source nodes. This avoids the latency of centralized restoration.

Another alternative to speed up the restoration path selection is to allow initial selection of a simple restoration path, such as min-hop, by the source node. Then, on a regular cycle (e.g., once a day), the centralized server recomputes the restoration paths of some or all connections and then downloads these new restoration paths at a convenient time. Because there could be only few connections with sub-optimal paths between restoration path re-optimization events, such an approach can achieve virtually the same performance as optimal path selection, but without the real-time penalty of computing paths on a per-connection basis. In both alternatives, a node makes a restoration path request after a control plane reboot.

The advantages of the hybrid approach are summarized here: (1) The network achieves both the speed of distributed restoration and the use of optimized restoration paths; (2) This capability can be added to cross-connect platforms with no or minimal change to existing signaling mechanisms; (3) The path server allows carriers to customize restoration to their own specifications, while avoiding modifications to distributed vendor XC solutions. Carriers can reflect restoration requirements that are not easily captured in vendor distributed path selection methods, such as a particular Shared Risk Group (SRG) topology (e.g., shared fiber span or WDM structures), or service criteria (e.g., priority of connections).

3. Centralized Path Selection Algorithm

In this section, we describe our capacity planning heuristic called ***pushdown*** that optimizes restoration paths to minimize the total restoration capacity. Suppose that capacity is purchased in units of OC-48, the XC employs STS-1 switching granularity, and the network supports two types of connection services: class 1 and class 2. Class 1 services have more stringent restoration time requirements than class 2 services. The inputs to the pushdown algorithm include the network topology, service connections in STS-1 units and service type, as well as service paths for all connections. The output is an SRG-disjoint restoration path for each service connection. Since the time to establish a restoration path depends on the number of path hops [3], the pushdown algorithm selects minimum hop SRG-disjoint restoration paths for class 1 connections. For class 2 connections, the pushdown algorithm selects an SRG-disjoint path, while attempting to minimize the total number of OC-48s.

The pushdown algorithm is based on a greedy online algorithm described in [2]. It operates in two phases. In the first phase, we consider one service connection at a time and apply a locally optimal algorithm. In the second phase, we try to do a global optimization. We maintain an array $failneed_k[e]$ for each link k, where $failneed_k[e]$ denotes the needed restoration capacity on link k when SRG e fails. In order to provide 100% restoration for any single SRG failure, link k must place at least $M_k = \max_e failneed_k[e]$ STS-1s. For example, if $M_k = 49$ STS-1 units, then two OC-48s of capacity must be provisioned on link k. However, it is possible that only one SRG failure requires two OC-48s and all the remaining SRG failures require only one OC-48 of capacity. Thus, we try to select alternative restoration paths for some of the service paths with a goal of bringing M_k down to one OC-48. Reducing one OC-48 on link k and fixing the required OC-48s on all other links accomplishes this. As a result, a few service paths can no longer be restored on link k. Then we try to select alternative restoration paths for these service connections without increasing the required capacity on all links. If we succeed, we pushed down one OC-48. If we fail, we restore the original restoration paths and repeat this process with the next link. We iterate until no OC-48 can be pushed down.

4. Performance Evaluation

For our simulation study, we used a 95-node, 164-link network representative of an intercity backbone network. The demand sets are based on the private line demand distribution of a large intercity backbone. We assume requests for bandwidth occur in units of STS-1, STS-3, or STS-12 and that 25% of connections are class 1 while 75% connections are class 2. We compare our pushdown algorithm with a solution that consists of disjoint shortest restoration paths solution and other published heuristics. For every demand set, we calculate the total number of OC-48s required for each restoration scheme. Figure 1 shows the restoration overbuilds for different demand sets. The top curve is the overbuild requirement for the SRG-disjoint minimum hop restoration path. The middle curve is the overbuild requirement using the algorithm provided in paper [2]. As shown, the pushdown algorithm reduces the restoration overbuild up to 50% compared with the shortest path algorithm, and 15% compared with the greedy algorithm in [2].

To evaluate restoration process efficiency, we compared our proposed approach with a fully distributed approach (using min-hop paths) with the same network and demand matrix models. We used the pushdown algorithm to plan the capacities and evaluated the restoration success ratio by simulation of the distributed restoration process. Both approaches restore nearly 100% of class 1 connections in the first attempt since we always give higher priority to class 1connections in our simulator. Figure 2 shows the results for class 2 connections. Our approach restores nearly 100% of class 2 connections in the first attempt. In contrast, the distributed approach can only restore 60% of class 2 connections at first attempt under high demand load.

5. Conclusion

We proposed a hybrid distributed/centralized approach for optical network restoration that combines the merits of centralized and distributed solutions. It avoids the scalability issues of centralized solutions by using a distributed control plane for service path computation and service/restoration path provisioning. The hybrid approach improves the first restoration attempt success rate by 40% compared with the distributed approach. We also presented a restoration path computation algorithm. Simulation results show that our algorithm saves up to 50% of restoration capacity compared with the shortest path algorithm and 15% compared with a previously published greedy algorithm.

6. Reference

[1] R. Doverspike, et al., "Fast restoration in a mesh network of optical cross-connects," OFC 99.
[2] G. Li, et al., "Efficient distributed path selection for shared restoration connections," IEEE INFOCOM 2002.
[3] E. Bouillet, et al., "Enhanced Algorithm Cost Model to Control Tradeoff in Provisioning Shared Mesh Restored Lightpaths," OFC 2002.

FQ6 **12:00 PM**

A Novel Bidirectional Wavelength Division Multiplexed Passive Optical Network with 1:1 Protection

T. J. Chan, Y. C. Ku, C. K. Chan, L. K. Chen, F. Tong, *Chinese University of Hong Kong, Shatin, Hong Kong Special Administrative Region of China, Email: tjchan1@ie.cuhk.edu.hk.*

We propose a novel network architecture for WDM-PON which offers 1:1 protection capability. In case of any fiber cut between remote node and ONUs, the affected ONU can re-route the wavelength channels via the adjacent ONU.

1. Introduction

There has been a tremendous growth in optical access networks due to the availability of low cost optical components in recent years. Passive optical networks (PONs) [1] does not require electric power supply at the remote node (RN), which greatly eases the network maintenance, thus it is considered to be one of the most promising approach to allow further penetration of fiber towards the subscriber side. However, in conventional PONs, both upstream and downstream bandwidths have to be time-shared among all optical network units (ONUs). Therefore, new schemes on WDM-PONs [2] [3] have been proposed to further enhance the total system capacity. Little work has been done to offer protection capability in both conventional PONs and WDM-PONs except fiber-cut detection methods. Whenever a fiber link from the RN to the ONU is broken, the affected ONU will become unreachable from the optical line terminal (OLT), leading to enormous loss in data and business. In this paper, we propose a novel network architecture for WDM-PON which offers 1:1 protection capability in both downstream and upstream fiber connections. The traffic for both directions can be re-routed via the adjacent ONU if any fiber cut between the RN and an ONU occurs.

2. Network Design

Fig. 1 shows our proposed network architecture. The RN comprises an array-waveguide grating (AWG) and N 1x2 3-dB couplers to route the

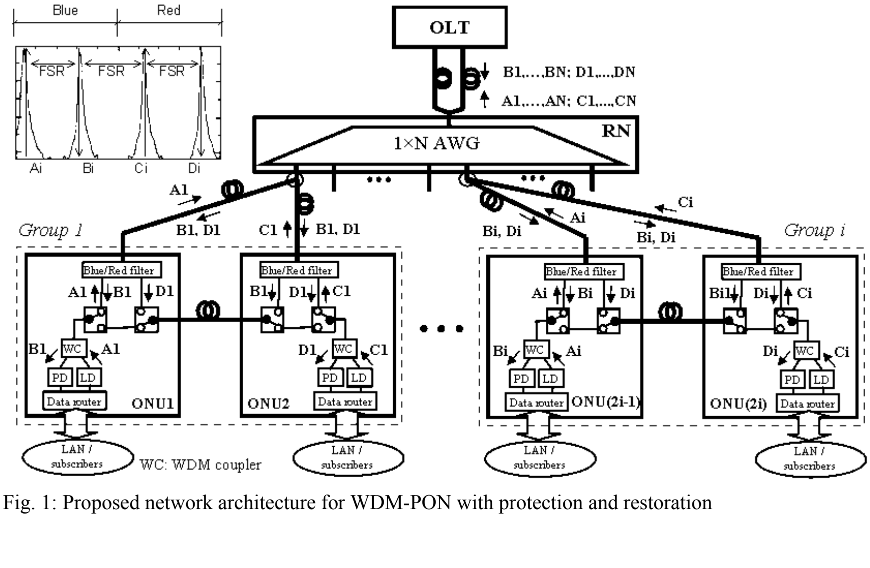

Fig. 1: Proposed network architecture for WDM-PON with protection and restoration

Channel no	Wavelength value	Channel no	Wavelength value	Channel no	Wavelength value	Channel no	Wavelength value
A1	1532.29	**B1**	1539.37	**C1**	1546.52	**D1**	1553.73
A2	1533.07	**B2**	1540.16	**C2**	1547.33	**D2**	1554.54
A3	1533.86	**B3**	1540.95	**C3**	1548.11	**D3**	1555.34
A4	1534.64	**B4**	1541.75	**C4**	1548.91	**D4**	1556.15
A5	1535.43	**B5**	1542.54	**C5**	1549.72	**D5**	1556.96

Table 1

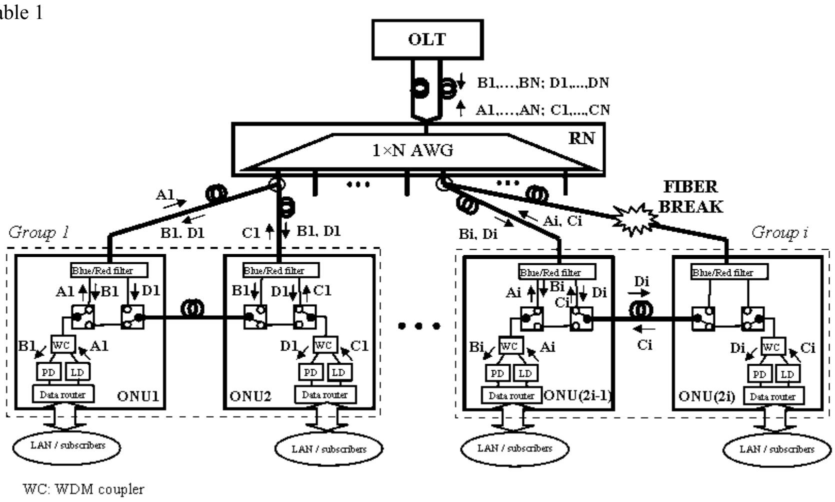

Fig. 2: Network restoration when the fiber link between RN and ONU(2i) is broken

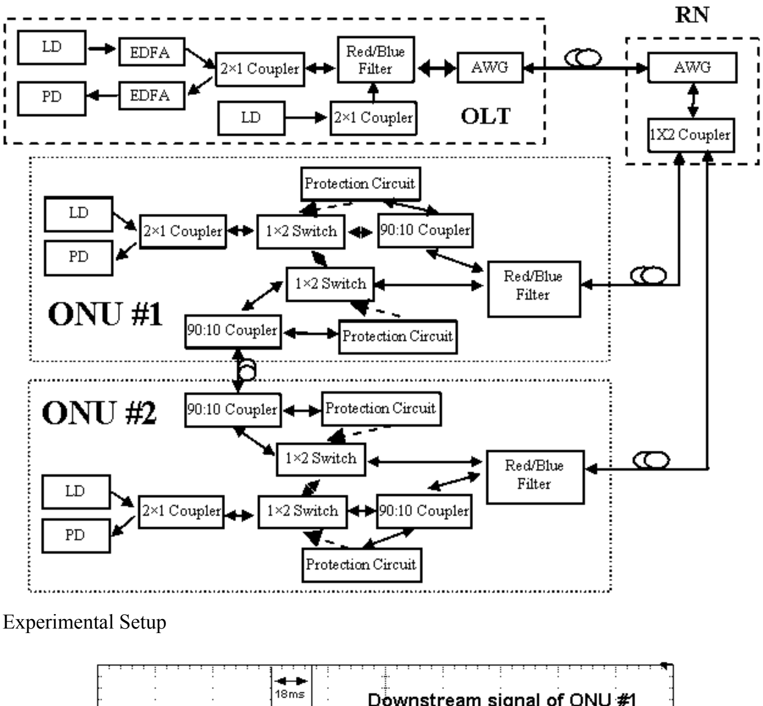

Fig. 3: Experimental Setup

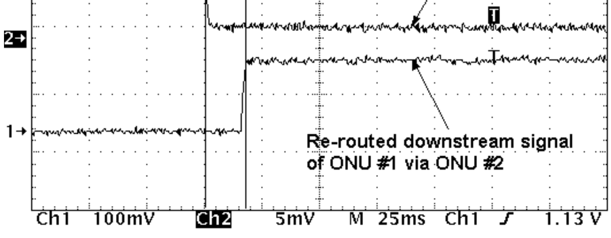

Fig. 4: Switching time measurement

wavelength channels to the ONUs. Every two adjacent ONUs are assigned to a group. Each ONU in a group is separately connected to the same output port of the AWG via the fiber coupler. In each group of ONUs, a single piece of fiber is used to connect the two ONUs to provide an alternative path. Whenever there is a possible fiber cut between an ONU and the RN, it can still route its upstream and downstream traffic to/from the OLT via its adjacent ONU in the same group. Thus an ONU can protect its adjacent ONU from being isolated due to fiber cut, although each of them can still serve their respective connected subscribers in both normal and protection modes. A mutual 1:1 protection is therefore achieved.

Under normal operation (see Fig. 1), the downstream wavelengths, ***Bi*** and ***Di***, are carried on the fiber link connecting to **ONU(2i-1)** and the same composite signal is also delivered to **ONU(2i)**. At the front-end of **ONU(2i-1)**, its destined downstream wavelength, ***Bi***, will be filtered out by the Red/Blue filter and so is ***Di*** in **ONU(2i)** . The use of the WDM coupler is to separate the upstream and the downstream wavelengths within the ONU. For upstream wavelengths, ***Ai*** from **ONU(2i-1)** and ***Ci*** from **ONU(2i)** will pass through their own Red/Blue filters and their respective fiber links. They are then combined before being fed into the same output port of the AWG. Under normal operation, there will be no traffic running on the fiber link connecting two ONUs in the same group.

For each ONU, two distinct wavelengths are assigned for upstream and downstream signals. Moreover, as two adjacent ONUs in the same group are actually connecting to the same output port of AWG at the RN, we make use of the spectral periodicity property of AWG to support the set of working and re-routed wavelengths. The upstream wavelengths (***Ai***, ***Ci***) and downstream wavelengths (***Bi***, ***Di***) in the ONU group ***i***, i.e. **ONU(2i-1)** & **ONU(2i)**, are spaced by one free-spectral-range (FSR) of the AWG, thus one AWG port can support the transmission and routing of all four wavelength channels (see the inset of Fig. 1) simultaneously. Table 1 shows the example of the wavelength assignment for a WDM-PON with 10 ONUs.

In case of fiber cut at the fiber link connecting to **ONU(2i)**, for example, the optical switches inside both ONUs in the same group would be reconfigured as illustrated in Fig. 2. Both upstream and downstream wavelengths of the isolated **ONU(2i)** will be routed to the **ONU(2i-1)** via the single fiber connecting between them. Conversely, **ONU(2i)** protects **ONU(2i-1)** in a similar way. With this protection mechanism, a fast restoration of the broken connection can be achieved, with minimal affect on the existing traffic.

Assuming the transmitted powers from the LDs in the ONUs are 0 dBm, the receiver sensitivities of the photodiodes at the OLT are -24dBm (at 2.5Gb/s), the insertion losses of optical switches, AWG, Red/Blue filters and WSC are 1dB, 5dB, 1dB and 1dB, respectively; the optical power margin will be 10dB in the re-routing path of upstream traffic, and so is that in downstream traffic. Therefore, a transmission distance of more than 40km can be achieved.

3. Experimental Results

Fig. 3 shows the experimental setup to demonstrate the principles of the bi-directional transmission and protection operations of the proposed WDM-PON network. The 1550nm DFB laser diodes (LD) used were 2.5Gb/s, directly modulated, while each of the arrayed-waveguide gratings (AWGs) had 16 channels with 100-GHz channel spacing and had an FSR of 12.8nm. Each Red/Blue filter had a bandwidth of about 18nm in each passband. On the OLT side, EDFAs were inserted in front of the AWG in order to compensate the components' insertion losses and to achieve the required transmitted power. Using this setup, we measured the switching time in case of fiber cut between ONU #1 and the RN. The optical power of the downstream signals from RN and from ONU #2 were monitored and the result was shown in Fig. 4. The upper waveform showed the downstream signal from RN to ONU #1 while the lower was the re-routed downstream signal via

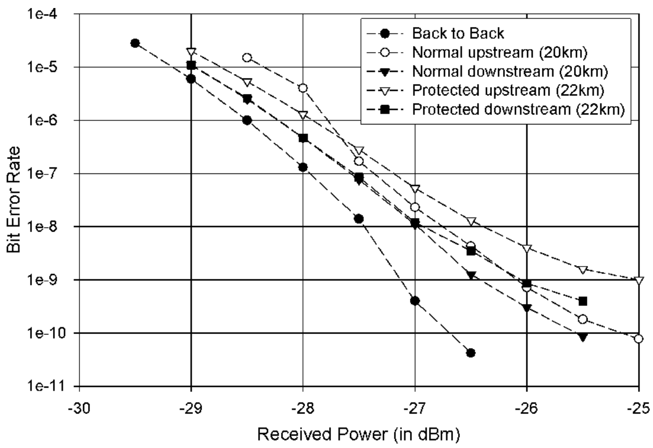

Fig. 5: BER measurements of 2.5Gb/s upstream and downstream traffic in normal and protected modes

ONU #2. The switching time was measured to be about 18ms and this corresponded to the network traffic restoration time.

We have also measured the bit-error-rate (BER) performance using 2.5Gb/s 2^{23} -1 PRBS data for both the upstream and the downstream traffic; and the measurement results were depicted in Fig. 5. In normal operation, both the upstream and the downstream wavelengths travelled through a transmission distance of 20km between the OLT and the ONU. Then, the fiber link between the RN and ONU1 was intentionally disconnected to simulate the fiber cut scenario. With our automatic protection mechanism, the fiber cut was detected and both the upstream and downstream wavelengths serving ONU1 were automatically switched to the fiber link (2km) between the two ONUs. Both wavelengths were then routed back to the OLT via the fiber link between ONU2 and the RN. Thus, the re-routed wavelengths travelled though a distance of 22km between the OLT and the ONU1. In all cases, the measured receiver sensitivities at 2.5-Gb/s varied from -25dBm to -26.5dBm. The additional 2-dB power penalty with respect to the back-to-back measurement was induced by fiber dispersion.

4. Conclusion

We have proposed a novel bidirectional protection scheme for WDM-PONs. By incorporating simple optical switches and optical filters into the ONUs; and by connecting two ONUs in the same group by a single piece of fiber, bi-directional signal re-routing can be achieved. Thus the isolated ONU can still communicate with the OLT in case of fiber cut. The automatic protection switching mechanism and the transmission aspect of the 2.5Gb/s signals were experimentally characterized.

5. References

[1] D. W. Faulkner, et al, IEEE J. Lightwave. Technol., vol. 7, pp. 1741-51, 1989.
[2] N. J. Frigo, et al, IEEE Photon. Technol. Lett., vol. 6, no. 11, pp. 1365-67, 1994.
[3] P. P. Iannone, et. al, IEEE Photon. Technol. Lett., vol. 10, no. 9, pp. 1328-30, 1998.

FQ7 **12:15 PM**

Shared Sub-Path Protection with Overlapped Protection Areas in WDM Networks

J. Li, H. Park, *Information and Communications University, Daejeon, Republic of Korea;* H. Lee, *Electronics and Telecommunications Research Institute, Daejeon, Republic of Korea, Email: jqli@icu.ac.kr.*

A partitioning configuration that divides a given network into overlapped protection areas for shared sub-path protection is investigated. The performances of capacity requirement and restoration time are improved without any significant degradation of other performances.

I. Introduction

A sub-path is defined as a subset of the links along a path. To find protection paths for the sub-paths of a working path is called sub-path protection. How to divide a working path into several sub-paths is an important problem in the sub-path protection scheme. One idea is to divide each working path into several protection domains [1]. The other idea is to partition a larger network into several smaller areas [2]. However, partitioning configuration in [2] is not practicable for most actual networks. Moreover, sub-path protection requires more resources [2]. This is critical for network dimensioning.

We propose a new partitioning configuration that divides a given network into overlapped protection areas where a wavelength on the link that belongs to the overlap can be shared for protection sub-paths whose corresponding working sub-paths belong to adjacent separated working areas. It not only guarantees practicability but also provides higher resource utilization and decreased restoration time without any significant degradation of other performances.

II. Partitioning Configuration

We examine two ways of partitioning a working path in detail and then describe our new partitioning configuration. We only consider link failures in this paper. For convenience, we name the method that divides a working path into several protection domains as Path Dividing (PD); we name the method that partitions a larger network into several smaller areas as Network Partitioning (NP). The main difference between PD and NP stems from the sharing method of the protection sub-paths. In PD, two protection sub-paths can share some wavelength-links as long as their corresponding working sub-paths are link-disjoint. In NP, two protection sub-paths that only belong to the same area can share some wavelength-links if their corresponding working sub-paths are link-disjoint. The NP in [2] divides a larger network into several separated areas. We called this partitioning configuration Separated Network Partitioning (SNP). However, two protection sub-paths whose corresponding two working sub-paths belong to adjacent areas can share some wavelength-links without checking the disjoint requirement because their working sub-paths belong to different areas. This motivates us to consider new partitioning configuration in order to improve the resource utilization.

The other disadvantage of SNP is that it has a requirement that the node degree of the Area Border Router (ABR) must be larger than 3. The node degree refer to the number of other nodes in the network to which a node is connected, which is also equal to the number of links connected to the node. As an ABR, it must guarantee that a working path that traverses it can be divided into two working sub-paths and each working sub-path and its corresponding protection sub-path belong to the same area. This means that it must have at least 4 links connected to it and that at least two links belong to one area, and other two links belong to the other area. If the degree of a node is 2, it is not possible as an ABR. For a mesh network, it must have some nodes whose degree is larger than 2. Otherwise, it is a ring. If a larger network does not have suitable nodes whose degree is more than 3 as ABRs, we cannot divide the larger network into smaller separated areas according to SNP [2]. Most actual networks belong to this category. In order to partition this type of larger networks, we need to choose some nodes whose degree is 3 as ABRs. If we divide a given network into overlapped areas, the partitioning problem can be solved. However, the wavelength assignment of sub-paths for overlapped areas is more complex than for the separated areas. To deal with the wavelength assignment issue for a wavelength on the link that belong to the overlap, we must consider the wavelength assignment for adjacent areas that overlap each other. This is not benefit for ILP calculation. In order to maintain the calculation complex of ILP not to be increased significantly, we propose a new partitioning configuration.

Our partitioning configuration is described as follows. We divide a given network into several areas, but areas for working and protection sub-paths are different. Areas for the working sub-paths are called working areas. Working areas are separated. Areas for protection sub-paths are called protection areas. One protection area corresponds one working area. It can be bigger than the corresponding working area. Protection areas can be overlapped. The objective of overlapping of protection areas is to increase the sharing for the protection sub-paths that belong to the adjacent protection areas. Our partitioning configuration is called Network Partitioning with Overlapped Protection Areas (NPOPA). The difference between NPOPA and SNP is that a working area and its corresponding protection area are different. The difference between NPOPA and PD is that in NPOPA a working area and its corresponding protection area can have many pairs of working and protection sub-paths, but in PD one protection domain only has one pair of working and protection sub-paths.

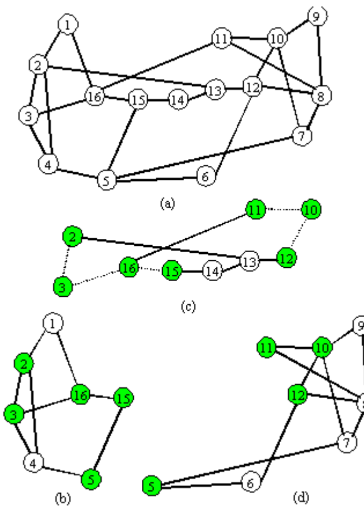

Fig. 1 (a) 16-node and 25-link NSFNET backbone. (b), (c), and (d) are three areas of (a). Working areas include only solid links. Protection areas include solid and dashed links. Node 5, 2, 3, 15, 16, 10, 11, and 12 are ABRs. The wavelengths on dashed links are permitted to be assigned only for protection sub-paths whose corresponding working sub-paths are in this working area.

We give an example to illustrate the practicability of our NPOPA. The 16-node and 25-link NSFNET backbone is shown in Fig. 1. It can be