A new shared protection scheme in optical network

P. P. Sahu

Department of Electronics, Tezpur University, Tezpur 784 028, India

In this paper, we have proposed a restricted shared protection (RSP) scheme that provides restriction on the sharing of some of the backup light paths to increase the reliability of the protection in optical network. From the reliability theory, we have proved that the reliability in RSP network is more than that of existing shared protection (SP) network. As failure rate increases, the reliability of RSP decreases with slower rate than that of SP. For the study of RSP, we have considered routing based on minimum time delay and assign the wavelength using parallel reservation method. It is also observed that the blocking probability in RSP network is more than that of shared protection. To reduce the blocking probability we have used alternate path routing for both the protection schemes. It is seen that the blocking probability reduction using alternate path routing in case of RSP is more than that of SP.

Keywords: Optical network, restricted shared protection, RWA, shared protection.

MULTIWAVELENGTH optical networks using routing and wavelength assignment (RWA) is one of the most promising candidates for the backbone of high speed wide area network (WAN), due to their information transparency and wavelength reuse characteristics. The RWA is used to select the best route (path) and a wavelength for the connection of a source-destination (s–d) pair so that any connection sharing a common link does not have the same wavelength. There are two types of RWA – static and dynamic. The static RWA is used for fixed path traffic pattern whereas dynamic RWA is used in response of changing traffic pattern.

The dynamic RWA plays an important role for highly variable traffic of IP over WDM network, which has become essential to fulfill the demand of bandwidth for tremendous increase of Internet users. Here, after getting a connection request, the establishment of lightpath of a s–d pair is carried out by dynamic RWA approach. If the connection request is not served within a time interval (termed as holding time), it is rejected. It is termed as blocked connection. So the performance of dynamic RWA is expressed in terms of blocking probability. Blocking probability is a probability that a connection is blocked due to unavailability of wavelengths.

The network monitor shows that failures occur in the optical backbone. The survivability against the failure is required for such high capacity network, since failures may result in significant degradation of network performance. It is made through protection mechanism.

Background

This section presents relevant background information on dynamic routing, wavelength assignment, and protection mechanism. This paper considers a dynamic network in which the traffic is not fixed and non-uniformly distributed over the s–d pairs. Each connection request specifies the s–d pair and bandwidth requirement. The previous studies indicate that the path is selected based on current link state information and wavelength is chosen by using distributed wavelength reservation protocol. The wavelength for the connection is assigned for the entire session. In this paper, we have used the dynamic RWA in which minimum time delay path is found for a s–d pair based on link state information and wavelength is selected based on wavelength status information at each node.

To make IP over WDM optical network efficient and reliable, protection is required against failures. The failures are of two types – link and node failure. The previous studies show that two types of protection can be made against these failures – dedicated protection (1:1 protection) and shared protection (1:M protection). In dedicated protection, a dedicated backup path is established for each s–d pair. In shared protection, a wavelength is shared among multiple backup paths for a large number of s–d pairs, provided they are not active simultaneously. The latter scheme reduces blocking probability as well as number of wavelengths for protection.

For nationwide high bandwidth coverage, we have taken NSFNET T1 backbone, which is shown in Figure 1. It consists of 14 nodes and 21 links. It is evident from the figure that each link consists of two unidirectional fibres in reverse manner. Earlier, NSFNET is upgraded using wavelength routing switches to support WDM. Further, it is upgraded using dynamic wavelength routing node. Dynamic wavelength routing node is one that is capable of switching a signal, adding and dropping its signal dy-
namically. Such a node can be implemented by a set of optical cross connect (OCC) and add/drop multiplexer (ADM) and wavelength division multiplexer (WDM). In this paper, we examine dynamically wavelength routed NSFNET under proposed shared protection (RSP) and compare the same with existing shared protection.

Dynamic routing and assignment

When paths are established dynamically, wavelength assignment decisions must be taken on the basis of link state information, which is updated periodically through the link state routing protocol. To formulate the problem, physical topology of the network has been modelled as a unidirectional graph $G(V, E)$, where $V$ is the set of nodes and $E$ is the set of links between nodes in network. As mentioned earlier, we consider each link consisting of two unidirectional fibres (two fibres can carry same wavelengths in reverse direction). It is assumed that each fibre link can carry the same number of wavelengths. We first introduce the following notation:

- $i, j$ denote the end points of physical link that might occur in the route of a connection.
- $l$ is used as an index for link number where $l = 1, 2, 3... L; L =$ total number of links.
- $w$ is used as an index for the wavelength number, where $w = 1, 2, 3... W; W =$ total number of wavelength carried by each fibre link.
- Connection request $c(s, d, t_{id})$ is specified by source $(s)$ and destination $(d)$ and holding time $(t_{id})$ of connection.

The following inputs are supplied to the problem.

- An $N \times N$ distance matrix, where $N =$ total number of nodes in the network and $d_{ij} =$ (i, j)th element distance matrix = distance between $i$ and $j$ node. Note that $d_{ii} = d_{jj}$ if and only if there exists a physical fibre link between $i$ and $j$ node and $d_{ij} = \infty$, if there is no fibre link.

- An $N \times N$ traffic matrix where the (i, j)th element, $\alpha_{ij}$ is the traffic flow rate from $i$ to $j$ node.

The time delay ($T_r$) experienced by a traffic is a combination of propagation time delay ($T_p$) and queuing time delay ($T_q$). The propagation time delay can be computed as:

$$T_p = \sum_{i \neq j} \sum_{x, y = 1}^{W} \frac{\alpha_{i,j} P_{i,j,w}^{x,y} d_{x,y}}{L_v}$$

where $P_{i,j,w}^{x,y} =$ lightpath–wavelength–link indicator

- $= 1$, if there is a light path from node $i$ to node $j$ and it uses wavelength $w$ on a physical link from node $x$ to node $y$.
- $= 0$, otherwise.

$L_v =$ Velocity of light.

The queue delay can be computed as follows

$$T_q = \sum_{i \neq j} \frac{\alpha_{i,j}}{C_m - \alpha_{i,j}}$$

where $C_m =$ maximum capacity per light path.

$$\alpha_{i,j} = \sum_{r, d} \alpha_{i,j}^{r,d} \forall i, j.$$  

The above equation shows that the traffic offered in the light path is the sum of the traffic on to the light paths due to all node pairs.

The objective function is given below.

Minimize: $T_{r, q}$

Traffic flow constraints

The traffic flow constraints pertain to the traffic routed over the lightpaths in the network.

$$\alpha_{i,j} \leq C_m \quad \forall (i, j)$$

$$\alpha_{i,j}^{r,d} \leq P_{i,j} t^{r,d}$$

where $P_{i,j} =$ lightpath indicator.

- $= 1$, if there is a light path from node $i$ to node $j$.
- $= 0$, otherwise.

$t^{r,d} =$ Average traffic rate flow from source node, $s$ to destination node, $d$.

$$\sum_j \alpha_{i,j}^{r,d} - \sum_j \alpha_{j,i}^{r,d} = t^{r,d}, \quad \text{if } s = i$$

$$= -t^{r,d}, \quad \text{if } d = i$$

$$= 0, \quad \text{if } s \neq i \quad \text{and} \quad d \neq i.$$
Equation (4) defines the network congestion, i.e., the component of traffic offered onto a lightpath due to a node pair can be at the most the amount of traffic flows between the node pair. Equation (5) shows that the traffic can flow only through the existing lightpath. Equation (6) expresses the conservation of traffic flow at the end nodes of a lightpath.

**Wavelength constraints**

The wavelength constraints pertain to the assignment of wavelengths to the lightpaths.

\[
P_{i,j} = \sum_{w=0}^{W-1} P_{i,j,w} \quad \forall (i, j),
\]

\[
P_{i,j,w} \leq P_{i,j,w} \quad \forall (i, j), \quad (x, y), w,
\]

\[
\sum_{i,j} P_{i,j,w} \leq 1 \quad \forall (x, y), w,
\]

Equation (7) shows that the wavelength used by a lightpath is unique. Equation (8) expresses the wavelength continuity constraint. Equation (9) shows that two lightpaths cannot use the same wavelength on a link. Equation (10) expresses the conservation of wavelengths at the end nodes of physical links on a lightpath.

After finding a route from the routing table, which is updated periodically, a wavelength reservation mechanism is required to assign a wavelength for the route. Previous studies show that there are two types of wavelength reservation mechanism—paralleled reservation and hop by hop basis reservation. It is reported that the set time for parallel reservation is less than that of hop by hop reservation. So we have used parallel reservation. In this case, after selection of the route, the source attempts to reserve the wavelength by sending a reservation request to each node of the route. The nodes of the route send positive and negative acknowledgement of reservation back to the source. After receiving the positive acknowledgement, the light path is established for the entire session of a connection request. Each node in the network has traffic and network information, which are updated on the basis of link state information periodically. Once connection is established, the back up path is formed using protection trees as given in Table 1. The algorithm procedure is given below:

1. Initialize with network configuration, \( G(V, E, W) \).
2. If a connection request \( c(s, d, t_0) \) comes, compute \( k \) number routes \( R_i \) on the basis of link state information in descending order of time delay \( T_d \) (where \( i = 1, 2, 3...k \) correspond to 1st, 2nd, \( k \)th shortest traffic delay path) using eqs (3) to (6).
3. For \( i = 1 \) to \( k \),
   - Try to assign the wavelength to the connection in ith shortest path within holding time \( t_h \) using the constraints from (7) to (10). If it is assigned, go to step-4. Otherwise, it is treated as a blocked connection.
4. Set up backup path for the assigned connection using protection trees as given in Table 1.

**Computational complexity**

The time complexity of the algorithm is \( O(EW + n^3) \), where \( n = K \) and \( K \) = number of distinct paths, \( N \) = total number of nodes in the network. The complexities of step-1 and step-2 are \( O(EW) \) and \( O(1) \) respectively. The complexities of step-3 and 4 are \( O(n^3) \) and \( O(W^5) \) respectively.

**Protection mechanism**

In this section, we discuss existing shared protection and proposed restricted shared schemes. In this direction, Gowda and Sivalingam have used converter-multiplexing technique for shared protection for reduction of wavelengths used for protection. To decrease the cost of network, we have avoided the use of wavelength converter. The protection trees are obtained using 4th shortest route because for alternate routing with \( k > 3 \), there is no improvement of blocking probability performance (which are discussed in simulation results section). Table 1 shows protection trees for different source nodes.

**Existing shared protection**

Figure 2a shows the existing shared protection for source node (2) to other destination nodes using wavelength-1. In this figure, we assign the wavelength-1 for source (2) to other destination. It is evident that 2-1-8-9-12-14, 2-1-8-9-12-11, 2-1-8-9-10, and 2-1-8-9-13 are sharing same the wavelength-1. The path 2-4-5-7, 4-5-7, 2-4-5 and 4-5, also share the same wavelength-1. Similarly, for other source nodes to their destinations, shared pro-
Proposed shared protection

Considering more reliability against simultaneous failures, we have proposed to restrict sharing of the sub branching paths of the tree. Figure 2b shows the restricted sharing protection tree with source node-2 using four wavelengths. It is seen in the figure that 2-1-8-9-12-14, 2-1-8-9-10 and 2-1-8-9-13 routes are not sharing the same wavelength and so are assigned by wavelength-1, wavelength-2, wavelength-3 and wavelength-4, respectively. Like Figure 2a, the same wavelength-1 is shared by 2-4-5-7, 4-5-7, 2-4-5 and 4-5 routes. So, shared protection requires single wavelength, as shown in Figure 2a whereas in case of restricted shared protection, four wavelengths are required for backup paths of node-2 as a source and other nodes as destination, as shown in Figure 2b. Similarly, we have made restricted shared protection trees for other sources and their destinations and evaluated number of wavelengths used for the same, as shown in Table 1.
Table 1. Protection trees for different source nodes ($N_R = $ number of wavelengths of RSP)

<table>
<thead>
<tr>
<th>Source node</th>
<th>$N_R$</th>
<th>Protection tree</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>4</td>
<td>2-4-5-7</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3-8-9-12-5-7</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3-6</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>2-3-6</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2-1-8-9-12-5-7</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3-6</td>
</tr>
<tr>
<td>3</td>
<td>4</td>
<td>2-3-6</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2-1-8-9-12-5-7</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3-6</td>
</tr>
<tr>
<td>4</td>
<td>5</td>
<td>4-2-1-8-9-12-5-7</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3-6</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>5-4-2-1-8-9-12-5-7</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3-6</td>
</tr>
<tr>
<td>6</td>
<td>5</td>
<td>6-3-2-1-8-9-12-5-7</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3-6</td>
</tr>
<tr>
<td>7</td>
<td>5</td>
<td>7-5-4-2-1-8-9-12-5-7</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3-6</td>
</tr>
<tr>
<td>8</td>
<td>4</td>
<td>8-9-12-13-14-11</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3-6</td>
</tr>
<tr>
<td>9</td>
<td>2</td>
<td>9-12-13-14-11-10</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3-6</td>
</tr>
<tr>
<td>10</td>
<td>5</td>
<td>10-9-12-13-14-11-10</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3-6</td>
</tr>
<tr>
<td>11</td>
<td>5</td>
<td>11-12-9-13-14-11-10</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3-6</td>
</tr>
<tr>
<td>12</td>
<td>4</td>
<td>12-9-10-13-14-11-10</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3-6</td>
</tr>
<tr>
<td>13</td>
<td>5</td>
<td>13-9-10-14-11-11</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3-6</td>
</tr>
<tr>
<td>14</td>
<td>5</td>
<td>14-12-9-13-10-8-1-2-4-5-7</td>
</tr>
</tbody>
</table>

Reliability of protection

In the protected network, there are two types of paths for a source-destination pair—primary routing path and backup path. For the calculation of reliability, we assume that each primary routing path has a failure rate of $f_p$ and similarly each backup wavelength has a failure rate of $f_b$. Figure 3a shows the reliability model of shared protection for 2-9 pair using single wavelength. The figure contains two paths—primary path and backup path. So the reliability as a function of failure rate at a time, $t$ for (2-9) s-d pair is given below

$$R_{2,9}^{SP} = e^{-f_p t} + \frac{f_p}{f_p-f_b}[e^{-f_b t} - e^{-f_p t}].$$

(11)

Similarly, for other branches, $R_{2,9}^{SP} = R_{2,6}^{SP} = R_{9,13}^{SP} = R_{12,11}^{SP} = R_{9,10}^{SP} = R_{2,9}^{SP}$.

So reliability at time $t$ for protection tree of node-2 is given by

$$R_2^{SP} = [R_{2,9}^{SP}]^6.$$ (12)

Figure 3b shows the reliability model for restricted shared protection of (2-9) s-d pair using four wavelengths. The figure shows four protection wavelengths for different wavelength. So the reliability for restricted shared protection of (2-9) s-d pair can be given as

$$R_{2,9}^{RSP} = e^{-f_p t} + \frac{f_p}{f_p-f_{RSP}}[e^{-f_b t} - e^{-f_p t}].$$ (13)

where $f_{RSP}$ = failure rate for restricted shared multiple wavelength = $N_f$, $N = $ number of wavelength paths. In case of (2-9) s-d pair, $N = 4$.

Similarly, for other branches,

$$R_{2,7}^{RSP} = R_{2,6}^{RSP} = R_{9,13}^{RSP} = R_{12,11}^{RSP} = R_{9,10}^{RSP} = R_{2,9}^{RSP}.$$ (14)

The reliability for source node-2 and all other nodes as destination for RSP is given as

$$R_2^{RSP} = R_{2,9}^{RSP} R_{2,6}^{RSP} R_{9,13}^{RSP} R_{12,11}^{RSP} R_{9,10}^{RSP} R_{9,13}^{RSP} = R_{2,9}^{RSP} [R_{2,9}^{SP}]^5.$$ (15)

The overall reliability of all s-d pairs of the SP network for NSFNET is given by

$$R^{SP} = \prod_{i=1}^{N} R_i^{SP},$$ (16)

where $R_i^{SP} =$ reliability for shared protection tree of source node-$i$ and $i = 1, 2, \ldots, N.$
The overall reliability of all s-d pairs of the RSP network for NSFNET is given by

$$R_{RSP}^{N} = \prod_{i=1}^{N} R_{RSP}^{i},$$

(17)

where $R_{RSP}^{i}$ is reliability for restricted shared protection tree of source node $i$ and $i = 1, 2, \ldots N$.

We have calculated overall reliability using the eqs. (11)–(12) and (16) for SP NSFNET whereas for RSP NSFNET, we have determined reliability using eqs. (13)–(14) and (17). For $f_e = 5 \times 10^{-3} \text{h}^{-1}$ and $f_p = 1 \times 10^{-3} \text{h}^{-1}$ (which are generally considered for other electronic systems), reliability of shared and restricted shared protection for the time duration of 24 h are $R_{SP} = 0.4673$ and $R_{RSP} = 0.9059$ respectively. So reliability of RSP is almost double of that of SP for these values of failure rates. Figure 4 shows the plot of reliability versus failure rate ($f_e$) varying from $6 \times 10^{-3} \text{h}^{-1}$ to $0.2 \text{h}^{-1}$ for RSP and SP NSFNET with $f_e = 5 \times 10^{-3} \text{h}^{-1}$ and time duration of 24 h. It is seen from the figure that as failure rate ($f_e$) increases, the reliability of both RSP and SP decreases and the rate of decrease of reliability for lower $f_e$ is greater than that for higher $f_e$. The figure also shows that as failure rate increases, the reliability of RSP decreases with slower rate than that of SP.

**Simulation results**

In this section we evaluate the performance of the proposed scheme by a computer simulation. As discussed earlier, our proposed scheme is based on dynamic RWA under shared and restricted shared protection. Simulation is performed for NSFNET T1 backbone as shown in Figure 1. Here, the blocking probability is used as a performance metric. Actually, blocking probability is defined as the number of blocked connection divided by the total number of connections present in the network. We have simulated the proposed scheme based on fixed path routing and alternate path routing with the connection requests (varying from $10^4$ to $10^5$) from all possible s-d pairs (i.e. 182 s-d pairs).

Figure 5 shows simulation result of blocking probability versus number of wavelength ($W$) per fibre link for unprotected, shared protected and restricted shared protected NSFNET using fixed path routing ($k = 1$). It is seen in the figure that blocking probability variation with $W$ for unprotected network is lower than that of shared and restricted shared protected network. This is due to the assignment of extra wavelengths for backup paths for the protection of the networks. It is also seen from the figure that in case of restricted shared protection, the blocking probability is more than that of shared protection. This is because more wavelengths are used due to restriction in sharing of wavelengths in RSP. In case of unprotected network, no blocking occur at $W \geq 20$, whereas in the case of shared protection it is at $W \geq 24$. But it is observed (not shown in Figure 5) that for restricted shared protection, no blocking occurs at $W \geq 30$. So the blocking probability in restricted shared protection is higher than that of shared protection.

To reduce the blocking probability, we have simulated the proposed scheme based on alternate path routing. Figure 6a compares blocking probability variation with $W$ between fixed path routing and alternate path routing. For alternate path routing, we have considered $k = 3$ (i.e.
alternate path is selected from second and third shortest time delay path from the routing table). It is also observed (not shown in Figure 6a) that for K > 3, there is no improvement in reduction of blocking probability. As k increases beyond 3, some paths might contain more hops and thereby the wavelength in more links in comparison to previous alternate path link. So it does not improve blocking probability performance. Other drawbacks of increasing k is the increase of setup time, which is discussed later on. Figure 6a shows that the blocking probability increases with W for both fixed and alternate path routing. Using alternate path routing, the reduction of blocking probability in RSP network is more than that in SP network.

The average setup time is the total set up time required for establishment of all the connection present in the network divided by the total number of successful connections. Figure 6b shows the variation of connection setup time with W for fixed path routing and alternate path routing with k = 3 and k = 4. It is seen from the figure that as W increases, average set up time decreases. It is also seen that average set up time for alternate path routing is more than that of fixed path routing. Again, as the number of alternate path (k) increases, the setup time also increases. This is because the extra processing time is required to find alternate paths.

We also compare the blocking probability of shared and restricted shared protected NSFNET using alternate path routing with unprotected NSFNET using fixed path routing Figure 6c. It is evident that blocking probability variation with W for SP using alternate path routing is very close to that of unprotected fixed path routing. But
for RSP, blocking probability is more than that for SP. Although the blocking probability is higher in RSP, it provides more reliability in protection of the network.

Conclusion

In this paper, we have studied dynamic RWA-based minimum time delay path. For survivability of the network, we have proposed restricted shared protection against failures and we have compared the same with conventional shared protection. Here, it is found that the reliability in RSP network is more than that of SP network but the blocking probability of the network is more in RSP. For the reduction of blocking probability we have considered alternate path routing. It is observed that although the blocking probability of SP is less than that of RSP, the reduction of blocking probability with alternate path routing in later case is more than that of the former case.


Received 3 April 2006; revised accepted 6 September 2006