PROTECTION IN OPTICAL MESH NETWORKS - A COST EFFECTIVE STRATEGY BASED ON TOPOLOGICAL CONSTRAINTS

D.SHEELA[1], C.CHELLAMUTHU[2]
[1]Department of Electronics and Communication Engineering,
Tagore Engineering College, Anna University, Chennai, India.
Sheela_rajesh@rediffmail.com
[2]Department of Electrical and Electronics Engineering,
R.M.K. Engineering College, Anna University, Chennai, India.
Malgudi60@hotmail.com

ABSTRACT

The physical topology of optical networks imposes significant effects on the wavelength requirements and the associated network cost. Some work on this topic has already appeared, but the impact of topologies on survivability, which is a prime issue in optical networks, is a nascent topic. This paper proposes a protection strategy in which the topological constraints are incorporated in a survivable network design, to achieve a cost effective solution. The performance metrics are recovery percentage against link failures and total network cost. Since the topological constraints imposed involve the forbidden nodes, the recovery performance is presented for node failures as well. To study the robustness to variations in traffic demand patterns, the proposed approach is evaluated with both uniform traffic and random traffic patterns, in the existing backbone networks of distinctly different topological characteristics. The proposed method is shown to yield promising results compared to the existing methods on optical network protection.

Keywords: *Topology, Network cost, Optical networks, Wavelength Division Multiplexing (WDM), Network protection, Recovery percentage.*

1.0 INTRODUCTION

The wavelength division multiplexing (WDM) technology is employed by the optical backbone networks, to handle the explosive growth and heterogeneity of the traffic demands on various WDM channels on a single fiber [1]. To meet the thousand-fold growth requirements, it is a challenge to build large-scale electronic routers and switches in a cost effective way with reduced power consumption. The future of optical networks lies in the significant reduction of lower capital expenditure (CAPEX) and operational expenditure (OPEX) [2]. Future optical networks should also have the ability to transport data in any type of format through the network and support dynamic demands [3].

Other than the cost issue, survivability is a critical concern in optical network design, since the failure of a network element can cause a huge amount of data loss. A network has to be resilient to survive network failures due to accidental or catastrophic events [4-5]. Network failures, such as fiber cuts and damaged components cause revenue loss and customer confidence; therefore, extensive studies of survivable networks have been performed [6-8]. The authors [9] have considered the physical layer impairments in the design aspects of survivable all-optical networks. SRLG (Shared Risk Link Group) disjoint protection, based on reliability constraints is proposed by [10].The authors [11] have proposed a hierarchical optical path network design, using dedicated waveband protection. A self diagnostic operation is demonstrated in [12] WDM networks to interconnect an array of sensors.

The major challenge in survivable optical networks is the design of resource allocation schemes, which assign network resources efficiently while ensuring better and faster recovery from failures. Although the network survivability problem in optical networks has been studied in detail, the physical topology factors of optical networks have not been taken into account to address this issue. The physical topology of the networks has significant effects on the resource requirements to honor the connection requests, since it directly determines the light path allocation, and the complexity of the network. Baroni and Bayvel [13] have proposed a heuristic algorithm for light path allocation in randomly connected networks, to evaluate the bounds on the number of wavelengths required to satisfy a uniform logical connectivity. The wavelength requirements in chordal ring and mesh-torus networks have been investigated [14]. The influence of topologies on wavelength requirements in optical networks has been investigated by Yuan and Xu [15]. They have considered two important characteristics of the networks, which are the average shortest path length and the 1-shell structure in small-world and scale-free networks. Better accuracy in the estimation of the wavelength usage is demonstrated by considering the node degree variance and the number of spanning trees in the network, [16]. In [17], a prediction formula relating the wavelength consumption to the network topologies is derived.

All these studies have analyzed how the topological metrics are related to the wavelength requirements in unprotected networks. It is still an open question as to how the topological factors can be applied for the benefit of network survivability. Consequently, it is essential to explore the impact of the topology parameters on network protection, to attain an effective network design. This paper proposes an approach, in which the topological factors and constraints are incorporated in the network survivability. It follows a two step approach in which as the first step, the critical links specific to a particular topology are identified, and assigned with additional capacity. Next, the most significant nodes in the network are designated as forbidden nodes, for calculating the protection paths. The prime objective of this approach is to minimize the consumption of the network resources, while providing adequate protection against network failures. Since both the links and nodes, which are vital from the topology perspective are considered in this method, not just the link failures, but also the node failures are considered in the network. For efficient usage of capacity, shared path protection is used in the ratio of 1:10. Three practical networks, which are distinctly different in terms of topological parameters, are taken for study. The performance evaluation is done in terms of the recovery percentage, the number of wavelengths, ports and fiber pairs used. The observations are made on the performance of the proposed method for the variations in traffic demands. This is done due to the fact that, for the optical networks to integrate well with the growing traffic demands, the major factors to be addressed are traffic characterization, resource dimensioning, and resource allocation [18].

2.0 CLASSIFICATION OF PROTECTION METHODS

Network survivability involves protection and restoration. Light paths are to be protected against failures by reserving the spare capacity during the connection setup. Restoration is the process of utilizing the spare capacity upon the occurrence of a failure. Survivability approaches are classified as link protection and path protection methods. In link-based protection, the traffic is rerouted around the end nodes of the failed link. In path-based protection, a protection path between the source and the destination nodes is pre-calculated. The protection schemes are further classified into dedicated [19], in which a dedicated protection path is used, and shared protection [20-22] where the protection paths share the bandwidth resources. Dedicated protection schemes have fast restoration times, but the resource requirement is high. Shared protection schemes handle resources more efficiently, at the expense of increased restoration time [23].

3.0 PROBLEM STATEMENT

The physical optical network is modeled as a graph $G = (N, L)$ where N is the set of nodes and L is the set of edges (links).Edges are assumed to be bidirectional, each representing a pair of optical fibers, i.e. one fiber per direction. The number of wavelengths per fiber in each direction is λ, and the nodes are assumed to have full wavelength conversion capabilities.The details of the network model is given in Table 1.

Table 1 Network Model

N	Set of Nodes
i	Nodes, $i \in N$
L	Set of Links
j	Links, $j \in L$
C	Set of critical links $C \subset L$
c	Critical Links, $c \in C$
n	Connection request from a source to destination
T	Traffic Matrix with n demands
λ	Number of wavelengths in a fiber
$\delta\, jpn$	1 if path p of demand n uses link j 0 otherwise

In the traffic matrix T, a k^{th} connection request that is from the source node s to the destination node d is represented as $n_{s, d, k}$. Let $P_w^{s, d, k,}$ and $P_p^{s, d, k}$ denote the working path and the backup path of the k^{th} connection between s and d, respectively. The protection path is link disjoint with the working path. Shared path protection is used to improve the capacity efficiency in the ratio of 1:10. The recovery percentage in a survivable network is defined as

$$\text{Recovery percentage} = \frac{\#\text{Connections Recovered} * 100}{\#\text{Connections Lost}} \quad (1)$$

The total network cost is defined as the sum of all wavelength resources together with the node cost and link cost.

$$CNW = \sum_{j \in L} Wj + \sum_{j \in L} Cj + \sum_{i \in N} Ci \quad (2)$$

CNW – Total Network Cost
Cj -- Link cost
Ci – Node Cost

Therefore ,the problem can be formally stated as follows: route each new connection demand to provide the highest possible recovery percentage, subject to single link failures and single node failures with minimum network cost, for the given current network state and traffic demand pattern.

4.0 IDENTIFICATION OF CRITICAL LINKS

In irregular topologies, there are always some links with a high degree of usage compared to other links in the network. These links with a high frequency of usage are identified and denoted as critical links. The wavelength resources are rapidly exhausted on such links that lead to congestion in the network. The most congested or the almost congested links in the network are involved in the capacity exhaustion blocking [24].The existing routing algorithms do not significantly take this factor into account. The information on network topology and frequency of usage of each link should be considered for optical network design strategies. The concept of critical links is a static factor, specific to a given network topology. Previous work on the identification of most loaded links is based on the maximum flow calculation and the residual bandwidth availability. In the proposed approach, the critical links are identified offline to reduce the computational complexity.

The authors have described [25] a method where critical ducts are identified using Eqn (3) to provide protection for WDM networks. As an extension of this work, significant nodes are identified and made forbidden to calculate the protection paths to reduce the loss of traffic due to node failures. The frequency of usage of a link $Fj, j \in L$ relates its importance to the whole network. For a connection request n, the usage of a link j, $j \in L$ for k possible routes is calculated. This value is calculated for all possible source destination pairs, to obtain the frequency of usage of a link.

$$Fj = \sum_{n=1}^{M} \sum_{p=1}^{k} \delta\, jpn, \quad M = N(N-1)/2, \; j \in L \quad (3)$$

Fjmax is the link with the highest value of Fj. The links with Fj / Fjmax ≥0.8 influence the traffic congestion and eventually the network performance. These links are designated as critical links.

4.1 Multi fibers on Critical Links

If single-fiber connections are used, practical topologies need a good physical connectivity. This condition may not be feasible especially for larger networks with a higher number of nodes, since the installation of physical links is very expensive. An alternative approach is the use of multi fibers between the nodes, which is a better option in already defined topologies. In fully connected networks, the same wavelength can be used by all the transmitting nodes. In the arbitrarily connected networks, the reduced number of fibers leads to the need for a higher number of wavelengths. Adding multi fibers to all the links in the network is not an intelligent solution from the cost aspect. Restricting the addition of fibers to critical links will limit the number of additional wavelengths required for recovery.

Since the frequency of usage in critical links is high compared to the other links, additional care is to be taken on these links from both the protection and cost perspectives. In the single link scenario, backup light paths always take longer routes than primary light paths, which result in quicker network resource exhaustion. When additional fibers are added to the critical links, the availability of the spare capacity is increased substantially. This enables the selection of paths with smaller number of hops, thereby saving the network resources. The protection paths in a multi fiber design take shorter routes than the protection paths in a single-fiber category. Hence, the required network resources are lesser than those of the single fiber design for protection purposes. Moreover, since the additional fibers are provided only on specific links, the redundancy cost is also reduced. In view of network protection, the probability of finding link disjoint routes is increased, compared to the single fiber case, thus providing more flexibility in selecting the protection paths.
W is the number of fibers added to a link j, j ЄL

Then, $$W \begin{cases} = 1, & j \subset C \\ = 0 & j \cap C = \phi \end{cases} \quad (4)$$

4.2 Routing based on weights

The weight of the link j, ßj

$$\begin{cases} = 1, & j \cap C = \phi,\ j, C \in L \\ \dfrac{1}{F_j} & j \subset C, \end{cases} \quad (5)$$

Hence, the likelihood of selecting the paths with critical links increases even if they are not necessarily the shortest paths in terms of hop counts. Since these critical links are assigned with additional fibers in the initial phase itself, the potential for the availability of network resources to honor the traffic demand improves remarkably. The wavelengths are assigned according to the first fit scheme.

5.0 PROTECTION BASED ON TOPOLOGICAL CONSTRAINTS

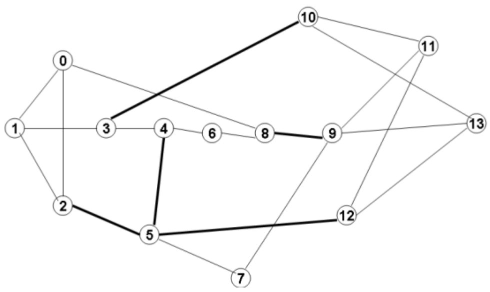
Since the critical links are very significant in terms of resource availability and network performance, eventually the nodes that adjoin these critical links are also very important. These nodes play a vital role in resource requirements and blocking probability. The critical links are listed according to their frequency of usage *Fj* with *Fjmax* being at the top of the list. The nodes which adjoin the top two links from the list are considered as the significant nodes in the network. For calculating the protection path, these nodes are designated as *forbidden*, so that they are not included in calculating the protection paths. These constraints define the nodes that should or should not be present in the route of a connection request.

The topology constraints are useful when we want to force a design action to route the connections using specific paths, without having to specify an entire path. In some topologies, the critical links may share a common node and in such cases, that node is not designated as forbidden, even if it is one among the nodes that adjoins the top two critical links. This is done due to the fact that if a node with critical links on either side is forbidden, it results in inconsistency in the calculation of the protection paths. Already the critical links which are influencing the network performance and resource requirements are assigned with additional fibers with lesser weights relative to other links. Hence, the possibility of selecting routes traversing through these critical links for working paths is increased more than in the normal scenario. Here, the shared path protection is followed and the protection paths are calculated on a link disjoint basis. When these topology constraints are imposed for selection, more number of non critical links is used for the selection of protection path. Hence, the unused capacity on non critical links is also effectively utilized, resulting in lesser number of wavelengths used to honor the given traffic demands.
The pseudo code for calculating the forbidden nodes is discussed as follows:

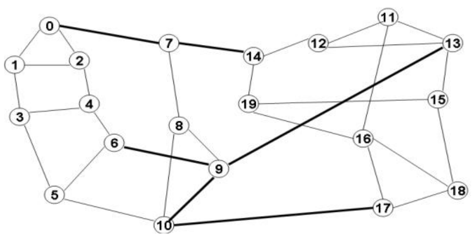
```
Set of Nodes    S = {s1, s2, .sn}
Set of Critical Links K = {c1, c2… cx},
Frequency of usage for x critical Links, [i] [j] = c1, c2… cx
Links [l ≠i, in 1to n] [m ≠ j, in 1 to n] =NULL;
Bubble sort (int Links[n] [n])
 {
    sort in ascending order;
    return links of [i] [j] with respect to last two greatest frequency of usage;
}
 for (i =1 to 4)
{
     nodes GU [ i ] = one of the nodes of last two links;
}
for (i =1 to n)
{
     for (j =1 to n)
    {
          if (Links [i] [j]  !=NULL &&  Links [i] [j]  !=
                         last two  greatest frequency of usage)
         {
           Nodes CL[b] = i;
           Nodes CL [b++] = j;
          }
      }
}
for (i =1 to 4)
{
     for (j=i+1 to 4)
     {
        if (nodes GU[ i ]= =nodes GU [ j ] )
        {
             set the flag;
        }
        break;
     }
        if (the flag is not set)
        {
            Nodes GUM[p] = i;
            p++;
        }
  Reset the flag;
}
for (i=1 to p)
{
    for (j=1 to b)
     {
       if (Nodes GUM[i] = =Nodes CL[j]
        {
            set the flag;
       }
      break;
   }
    if (the flag is not set)
    {
    print i as forbidden node;
    }
    Reset the flag;
}
```

In the algorithm, the x number of critical links is sorted, according to their value of the frequency of usage and the two links with higher values are returned. The nodes GU represent the nodes that connect the top two critical links of greatest usage, and the maximum value is four. It is possible that the top two links themselves share a common node, which therefore, should not be marked as forbidden. Hence, checking for the common nodes in the top two links is done. Then they are compared with the nodes that connect the other x-2 critical links .If they are not the same, then the nodes are marked as forbidden.

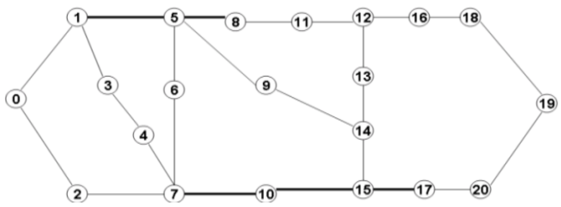
The NSFNET topology has been taken for the case study. The link with the maximum frequency of usage is the link that connects nodes 8 and 9.The link with the next higher value is the one that adjoins the nodes 2 and 5. Node 5 is a part of other critical links in the network. So, designating node 5 as forbidden will make the calculation of the protection paths very tedious. Thus in NSFNET, the nodes 8, 9 and 2 are noted as forbidden nodes for the protection paths. Note that, these nodes are not forbidden for calculating the working paths and are very much a part of them. Though the process of forbidding the critical nodes reduces the wavelength requirements, the number of forbidden nodes should be limited. As the number of forbidden nodes increases, the procedure of finding the protection path becomes hard and complicated, due to the reduced availability of candidate paths.



NSFNET



ARPANET



ARPA 2

Fig.1: Networks under Study

6.0 PERFORMANCE EVALUATION

The performance of the proposed approach has been evaluated on three well known networks- NSFNET, ARPANET and ARPA 2 as shown in Fig.1 using the OPNET tool. While the regular topologies have a simple routing procedure, the arbitrarily connected networks have the advantages of scalability and flexibility, needed for network evolution.

These networks are taken for study, for their distinctly varying topological parameters, such as connectivity and average node degree. The topological information of these networks is displayed in Table 2.

Table 2 Topology Information

Network	Nod es	Links	Average Node Degree	Connectivity %
ARPANET	20	32	3.2	17
ARPA 2	21	25	2.38	12
NSFNET	14	21	3	23

In the provisioning phase of the simulation, the network is populated with connections of indefinite holding time, meaning that once provisioned, the connections are not torn down or changed. Each fiber carries 40 wavelengths. All the nodes are equipped with full wavelength conversion capabilities. Each demand is assumed for a full wavelength and the problem of traffic grooming is not considered. For the comparison to be fair, the number of light path demands is set to be the same for all the three networks for a random traffic matrix. The connections honored remain active, and the new connection requests are accommodated by dimensioning the wavelength capacity. Single-link failure is considered in this paper; at any time, at most one link failure is allowed in the entire network. Instead of creating random link failures, definite failures are analyzed, the average value of the recovery percentage is taken for each link failure in the network. By doing so, the impact of every link failure on the network performance can be evaluated. Once the desired load is reached, a link failure is simulated and recovery is attempted. When all connections are either restored or lost, the network is reversed to its pre-failure state before the next link failure is evaluated. This procedure is repeated till all single link failures have been examined.

The protection strategies used should also consider the various aspects of the traffic flow. The proposed approach must be robust to variations in the traffic demand pattern. To study this aspect, different realization scenario of traffic may be characterized. By doing this, the over-dimensioning of the network resources may be minimized. Both the uniform traffic matrix and random traffic matrix are analyzed. Since the proposed scheme involves specific links and nodes which are very critical, two extreme cases of random traffic matrices are taken.1). No connection demands between the nodes that adjoin the critical links (Tmin). 2). Maximum connection demands of 15 between the nodes that adjoin the critical links (Tmax).

6. 1 Results and Discussion –Uniform Traffic

In this paper, a detailed analysis of the results on NSFNET is done as other networks follow a similar pattern. The results shown are for NSFNET unless stated otherwise. Fig. 2 shows the recovery percentage of single link failures for uniform traffic in NSFNET network. SPP-H denotes the shared path protection with the shortest path calculated with minimum hop count. SPP-LU is the shared path protection with the least used capacity as the cost metric. If λf is the free wavelengths in a link, the cost is $1/ \lambda f$. The proposed approach is noted as PBTC ((Protection based on Topological Constraints).A recovery path may be blocked due to the non availability of wavelengths on the route. One link failure is simulated at a time. All the links are considered for failures, the recovery percentage is calculated, and the average value is taken. The recovery percentage of the three schemes is equal to 100% when the number of light path demands between each source destination pair is one and two. But as the number of demands increases, the PBTC approach maintains a constant difference in the recovery percentage over the other two methods.

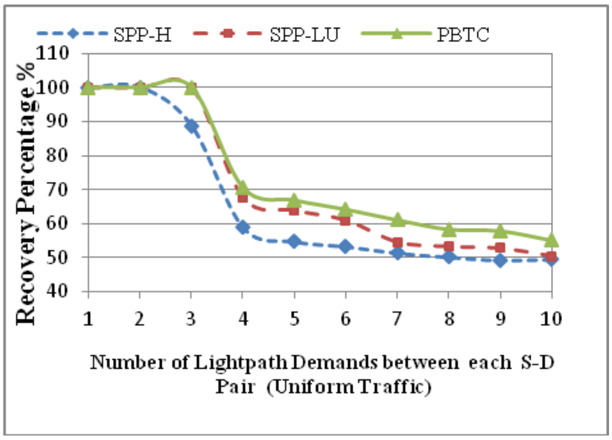


Fig. 2: Recovery Percentage

The total number of wavelengths used by the three methods in the NSFNET network is shown in Fig.3. The difference in the performance of the three methods is observed, once the number of light path demands between the source destination pair reaches the value of four. For this reason, further analysis focuses on the results starting from four. The higher value of wavelengths is due to the fact that the connections once honored remain active and not torn apart. The additional fibers added to the critical links in the initial phase result in increased possibility of the availability of shortest paths to honor a light path demand between a source destination pair. So the demands are accommodated using a smaller number of wavelengths as evident from Fig.3. Though the network cost involves node and link equipments like optical cross connects, transponders, amplifiers and regenerators, the number of wavelengths used is of prime concern, since the cost of most optical network components is affected by this value.

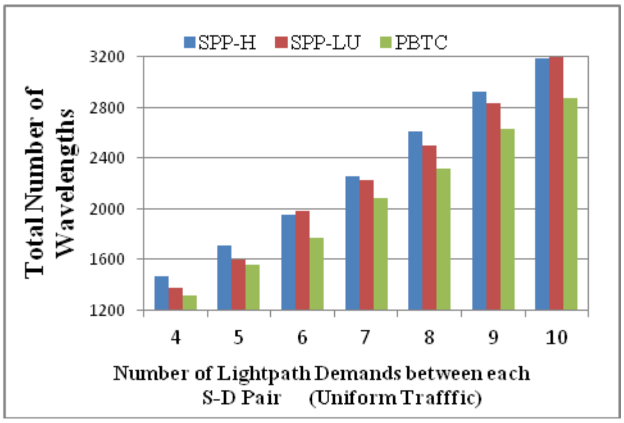


Fig. 3: Total Number of Wavelengths used

Fig.4.shows the percentage savings in the number of ports normalized to the number of ports used in 1+ 1protection.

$$\% \text{ Savings in Ports} = \frac{\#\text{ Ports }(1+1) - \#\text{Ports (SPP-H/LU//PBTC)}}{\#\text{ Ports }(1+1)} \quad (6)$$

The port savings in the PBTC is uniformly higher than in the SPP-H and SPP-LU methods. The reduction in the port count leads to a substantial total network cost reduction, since the port count usually dominates the node cost.

The number of fiber pairs used to honor the given uniform traffic matrix is given in Fig.5. The network is dimensioned, according to the increase in the demands, by adding more capacity to the network. There is a substantial reduction in the number of fibers used in the PBTC than in the other two methods. Smaller number of fibers used means, lesser number of terminal multiplexers, regenerators, optical amplifiers and so on. This factor also contributes to the reduction in the total network cost. The link wise usage of fiber pairs is displayed in Table 3 for uniform traffic, with number of demands between the source destination pair equal to nine.

Table 3 Link wise usage of Fiber Pairs Uniform Traffic-Number of demands =9

Links	SPP-H	SPP-LU	PBTC
0 <-> 1	3	3	3
0 <-> 2	3	3	2
0 <-> 8	3	5	5
1 <-> 2	3	3	2
1 <-> 3	5	7	7
10 <-> 11	5	5	5
10 <-> 13	2	2	2
11 <-> 12	3	3	3
11 <-> 9	5	7	6
13 <-> 12	3	2	2
2 <-> 5	7	9	6
3 <-> 10	7	7	6
3 <-> 4	5	6	7
4 <-> 5	5	7	4
4 <-> 6	5	5	5
5 <-> 12	7	7	5
5 <-> 7	5	5	5
6 <-> 8	5	3	2
8 <-> 9	9	7	4
9 <-> 13	3	3	2
9 <-> 7	3	3	3
Total	96	102	86

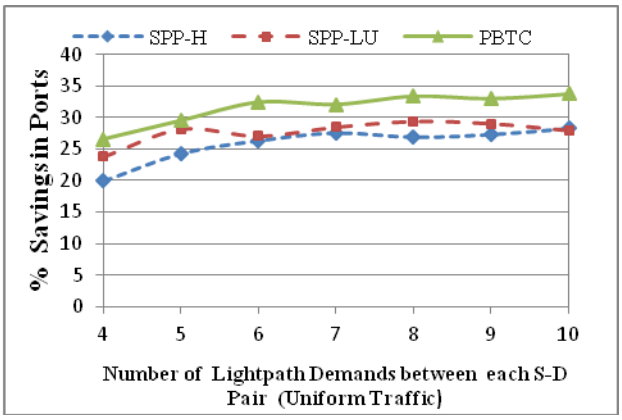


Fig. 4: Percentage Savings in Ports

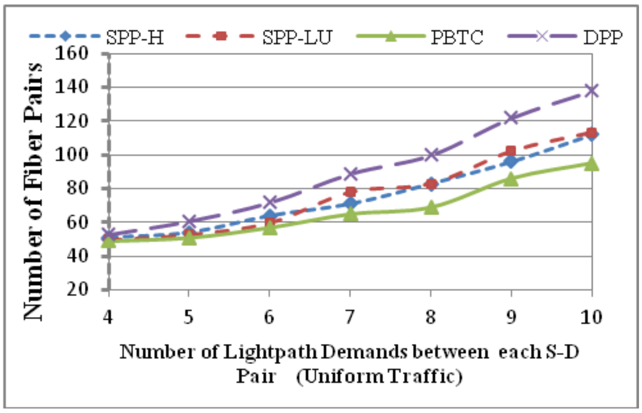


Fig. 5: Number of Fiber Pairs Used

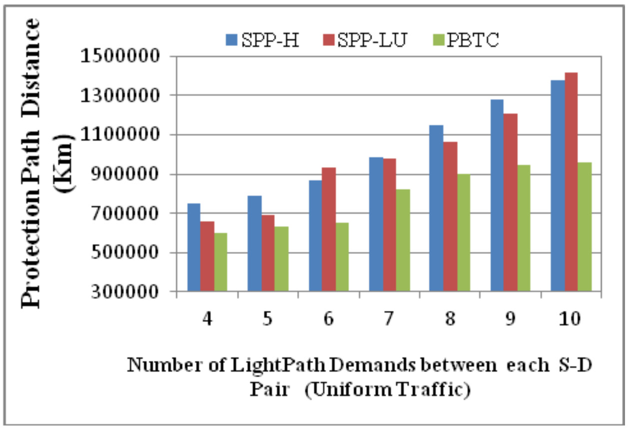


Fig. 6: Protection Path Distance

The total distance traversed by the protection paths in Km for uniform traffic is given in Fig. 6. It is evident from the result that the distance passed by the protection paths is lesser in the PBTC than in the other schemes. In the PBTC, due to the additional fibers assigned to the critical links, the availability of the protection paths is increased. Therefore, the distance covered is lesser in the PBTC, resulting in a reduction of both cost and delay.

Table 4 Number of Hops –Protection Path

Demands (b/w SD Pair)	SPP-H	SPP-LU	PBTC
4	688	600	536
5	735	625	585
6	788	812	602
7	897	862	717
8	1056	944	760
9	1167	1,080	875
10	1242	1,262	930

Since the basic mechanism followed in all the three methods is shared path protection, the number of hops used in the protection path is smaller than in the working path. The weight based routing increases the possibility of the inclusion of critical links in the selection of paths. The fibers added to the critical links increase the availability of the shortest paths; therefore, the destination can be reached with lesser number of hops as shown in Table 4. Due to the topology constraints imposed in the proposed strategy, the protection paths are calculated without considering the forbidden nodes. Therefore, the usage probability of the non critical links for the protection paths is greater than that of the normal scenario. This can be further explained with the spare capacity distribution for random traffic in Table 5, as the number of protected path hops is directly related to the spare capacity. The links with a forbidden node on one side have the minimum spare capacity compared to the other two methods, while for some insignificant links ,say for the link that connects nodes1 and 3, the spare capacity in the PBTC is higher than that in the other two methods. The number of hops increased otherwise, due to the usage of non critical links is offset by the drastic reduction of the usage of links that contain the forbidden nodes. This eventually leads to a smaller number of hops which implies a higher wavelength reuse.

Table 5 Spare Capacity Distribution for Random Traffic Matrix (Tmin)

Links	SPP-H	SPP-LU	PBTC
0 <-> 1	40	40	43
0 <-> 2	46	40	21
0 <-> 8	43	60	40
1 <-> 2	35	17	0
1 <-> 3	56	73	84
3 10 <-> 11	47	59	59
10 <-> 13	30	40	26
11 <-> 12	38	37	37
11 <-> 9	42	56	37
13 <-> 12	40	34	37
2 <-> 5	40	40	23
3 <-> 10	57	56	52
3 <-> 4	49	67	60
4 <-> 5	42	22	43
4 <-> 6	48	32	56
5 <-> 12	40	42	49
5 <-> 7	40	40	42
6 <-> 8	54	43	23
8 <-> 9	77	58	0
9 <-> 13	40	40	13
9 <-> 7	42	40	14
Total	946	936	759

6. 2 Results and Discussion –Random Traffic

As stated before, random traffic matrices are taken for study with two extreme cases, Tmax and Tmin. For the sake of uniformity the total number of demands in both the cases is set to be 700. Figs. (7-11) show the recovery percentage, number of wavelengths used and other performance metrics for random traffic.

Fig.7: Recovery Percentage

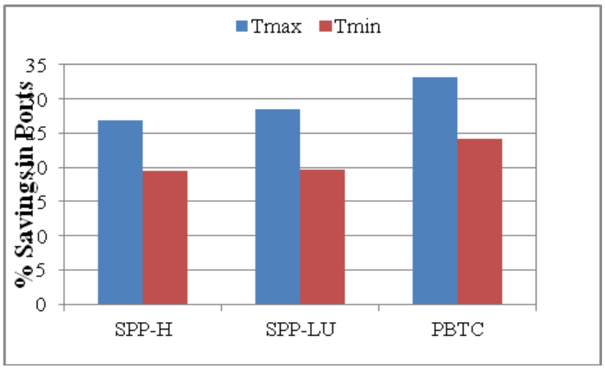


Fig. 8: Percentage Savings in Ports

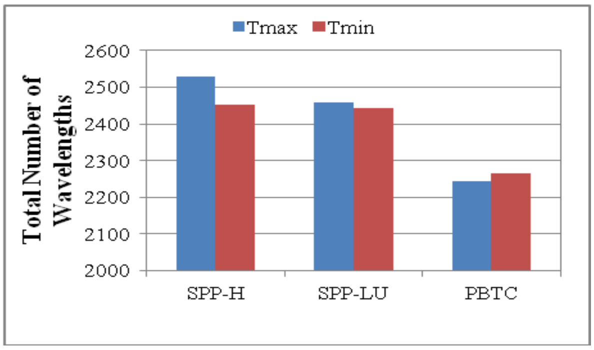


Fig. 9: Total number of Wavelengths used

Fig.10: Number of Fiber Pairs Used

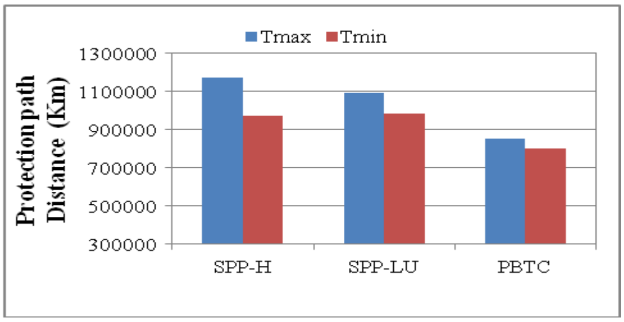


Fig.11: Protection Path Distance

Table 6 Number of Hops –Protection Path

	SPP-H	SPP-LU	PBTC
Tmax	1023	1,044	737
Tmin	946	936	759

The results show that the proposed approach, PBTC, outperforms the other schemes in all aspects of interest. In the PBTC, the difference in the required number of wavelengths and fiber pairs for Tmax and Tmin is negligible. The number of hops used is minimum as evident from Table 6. While the absolute number of ports in Tmin is less than that of Tmax, the percentage savings of ports normalized to 1+1 protection is high in Tmax. As the demands between the source destinations pairs that adjoin a single critical link are high in Tmax, the link failures in Tmax result in lesser recovery percentage than in Tmin.

6. 3 Node Failure Analysis

Since the proposed approach comprehensively considers both the links and nodes, the analysis on node failures is also carried out. Each node in the network is failed; the number of connections lost and the connections recovered, are evaluated.

Table 7 Average Lost and Recovered Connections for Node Failures

	SPP-H		SPP-LU		PBTC	
	Avg Conn Lost	Avg Conn Recov	Avg Con n Lost	Avg Conn Recov	Avg Conn Lost	Avg Con n Reco v
Tma x	151.9	5.57	147. 9	9.57	141	16.4 2
Tmi n	148.7	8.92	145. 9	11.71	136.2	21.4 2

The average value is shown in Table 7. The PBTC approach has shown considerable improvement both in terms of lost connections and the number of connections recovered. Table 8 gives a focused view of the number of connections lost and recovered, when the nodes 8, 9 and 2 fail in the NSFNET network. In the PBTC, as these three nodes are forbidden, the protection paths do not include these nodes, and hence, the recovery process does not depend on these nodes. Therefore, the failure of these specific nodes has the least effect on network protection.

Table 8 Lost and Recovered Connections for Node Failures (Forbidden Nodes -8, 9, 2)

	SPP-H		SPP-LU		PBTC		SPP-H		SPP-LU		PBTC	
	Tmax		Tmax		Tmax		Tmin		Tmin		Tmin	
Node Failed	Conn Lost	Conn Recov	Conn Lost	Conn Recov	Conn Lost	Conn Recov	Conn Lost	Conn Recov	Conn Lost	Conn Recov	Conn Lost	Conn Recov
2	154	0	163	0	143	20	120	0	114	15	103	26
8	205	0	179	10	151	38	186	8	174	0	122	52
9	222	0	197	14	150	61	211	8	208	14	148	74

Table 9 Random Traffic Matrix (Tmax)

	0	1	10	11	12	13	2	3	4	5	6	7	8	9
0	-	4	10	6	8	0	2	6	12	2	9	10	13	1
1	4	-	3	9	6	9	1	0	10	3	2	13	12	13
10	10	3	-	5	8	14	12	**15**	8	1	8	1	10	0
11	6	9	5	-	2	1	10	13	10	7	10	11	10	3
12	8	6	8	2	-	2	3	5	2	**15**	8	4	5	5

13	0	9	14	1	2	-	3	0	14	2	13	15	11	14
2	2	1	12	10	3	3	-	8	11	**15**	13	13	9	12
3	6	0	**15**	13	5	0	8	-	10	4	3	5	0	13
4	12	10	8	10	2	14	11	10	-	**15**	2	1	13	4
5	2	3	1	7	**15**	2	**15**	4	**15**	-	15	6	9	10
6	9	2	8	10	8	13	13	3	2	15	-	12	10	10
7	10	13	1	11	4	15	13	5	1	6	12	-	10	8
8	13	12	10	10	5	11	9	0	13	9	10	10	-	**15**
9	1	13	0	3	5	14	12	13	4	10	10	8	**15**	-

Table 10 Random Traffic Matrix (Tmin)

	0	1		11	12	13	2	3	4	5	6	7	8	9
0	-	12	9	0	13	14	15	12	10	10	14	0	12	14
1	12	-	8	9	3	7	13	13	4	7	13	0	7	7
10	9	8	-	6	9	10	9	**0**	8	2	6	10	9	12
11	0	9	6	-	10	11	4	6	10	5	11	10	10	5
12	13	3	9	10	-	12	5	10	6	**0**	2	7	9	6
13	14	7	10	11	12	-	2	4	14	8	9	13	8	12
2	15	13	9	4	5	2	-	3	1	**0**	14	12	9	0
3	12	13	**0**	6	10	4	3	-	13	2	7	8	14	11
4	10	4	8	10	6	14	1	13	-	**0**	8	9	0	12
5	10	7	2	5	**0**	8	**0**	2	**0**	-	3	3	9	12
6	14	13	6	11	2	9	14	7	8	3	-	8	9	0
7	0	0	10	10	7	13	12	8	9	3	8	-	9	8
8	12	7	9	10	9	8	9	14	0	9	9	9	-	**0**
9	14	7	12	5	6	12	0	11	12	12	0	8	**0**	-

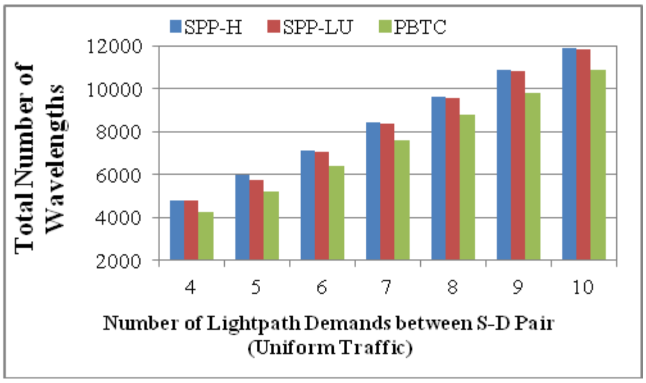


Fig.12: Total number of Wavelengths used for Uniform Traffic Matrix-ARPA 2

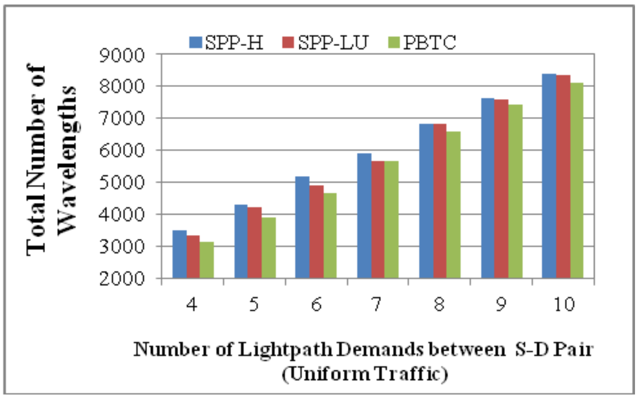


Fig.13: Total number of Wavelengths used for Uniform Traffic Matrix-ARPANET

Figs.12 and 13 show the wavelength requirements for uniform traffic in ARPA 2 and ARPANET respectively. The two extreme cases of traffic matrices, Tmax and Tmin are given in Tables 9 and 10 with the number of demands between the nodes that adjoin the critical links emphasized. Table 11 displays the wavelength requirements for a random traffic pattern. The behavior of the two networks is similar to that of NSFNET, but with a higher number of wavelengths used due to poor connectivity.

Table 11.Total Number of Wavelengths used –Random Traffic Matrices

	ARPA 2			ARPANET		
	SPP-H	SPP-LU	PBTC	SPP-H	SPP-LU	PBTC
Tmax	3773	3700	3382	3059	2942	2772
Tmin	4000	3915	3593	3281	2969	2878

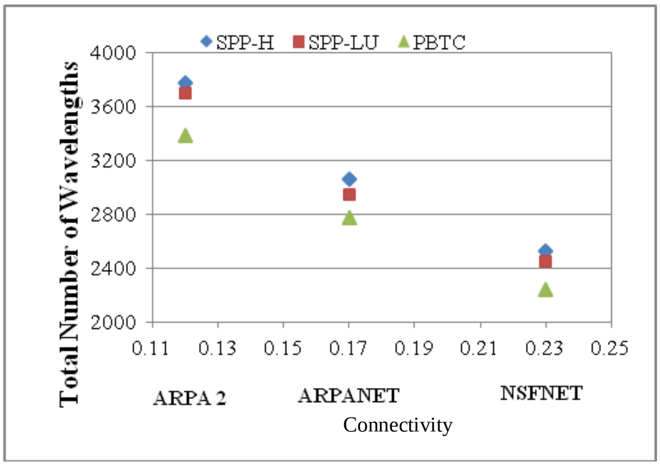


Fig.14: Comparison of Wavelength Requirements (Tmax)

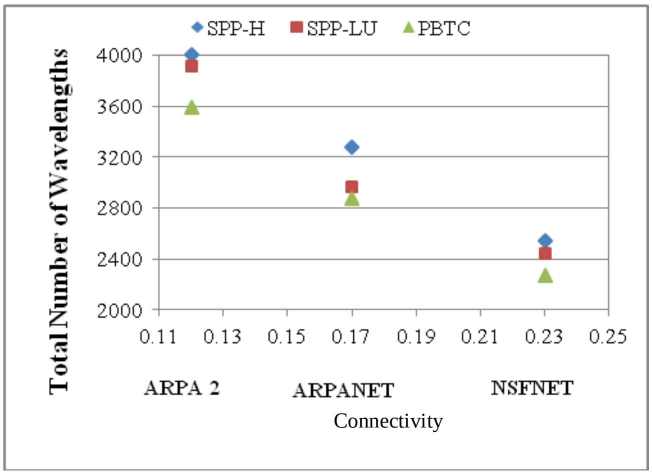


Fig.15: Comparison of Wavelength Requirements (Tmin)

A comprehensive picture of the wavelength requirements as a function of connectivity for all the networks is shown in Figs. (14-15). For the same number of light path demands, ARPA 2 which has the least connectivity of 0.12, consumes more number of wavelengths followed by ARPANET and NSFNET. The difference in the number of wavelengths used for Tmax and Tmin is distinct in ARPA 2 and ARPANET, but is very narrow in NSFNET due to its better connectivity of 0.23.

7.0 CONCLUSION

A novel approach was proposed and investigated in which topological constraints of optical networks were considered for survivability in optical networks. Both the network survivability and cost aspects were addressed in this method. The links with a higher frequency of usage in a network topology were identified, and termed as critical links. Additional fibers were added to those links in the network. These links were assigned weights with the inverse of their frequency of usage. Based on the critical links, forbidden nodes were identified for the calculation of the protection paths. The performance of the proposed method was demonstrated in three backbone networks, with distinctly different topological characteristics. To study the robustness of the approach, it was tested with both uniform traffic and random traffic patterns. In the random traffic study, two extreme cases were taken, in which zero and maximum light path demands between the node and destination pair that adjoin the critical links were considered. The recovery percentage and the network cost were taken as the performance metrics. Single link failures were considered and the recovery percentage of the PBTC was compared with the shared path protection with the hop count metric (SPP-H) and shared path protection with the least used metric (SPP-LU). The results showed an improvement in the performance of the PBTC compared to the other methods. The cost wise improvement of the PBTC was shown in terms of the number of wavelengths used, to satisfy the given number of demands, number of fiber pairs, and percentage savings in ports. The advantages of using multi fibers in critical links were demonstrated by the significant reduction in the resource requirements. The PBTC approach results in a smaller distance traversed by the protection paths than the other methods, presenting a reduction in the cost and delay incurred.

Since this approach comprehensively considered both the links and nodes by designating some of them as critical links and forbidden nodes, the performance had to be evaluated for node failures also. The PBTC yielded lesser number of connections lost and higher number of connections recovered. The effect of failures occurring at the forbidden nodes was also analyzed. The results showed that the wavelength requirement strongly depended on the physical connectivity. The proposed approach outperformed the other methods, in terms of protection issues and cost reduction, irrespective of the topologies and variations in the traffic demand pattern. Since the critical links and forbidden nodes were calculated offline, the computational complexity was also considerably reduced.

REFERENCES

[1] Menglin Liu, Massimo Tornatore, and Biswanath Mukherjee, "New Strategies for Connection Protection in Mixed-Line-Rate Optical WDM Networks", *Journal of Optical. Communication and Networking*, Vol. 3, No. 9, 2011 pp.641-650.

[2] Siamak Azodolmolky et al.," Experimental Demonstration of an Impairment Aware Network Planning and Operation Tool for Transparent/Translucent Optical Networks", *Journal o f Light wave Technology*, Vol. 29, No. 4, February 15, 2011, pp 439-448.

[3] S. Azodolmolky et al., "A dynamic impairment aware networking solution for transparent mesh optical networks," IEEE *Communication Magazine*, Vol. 47, No. 5, May 2009, pp. 38–47.

[4] T. H. Wu, *Fiber Network Service Survivability*. Norwood, MA: Artech House, 1992.

[5] T. E. Stern and K. Bala, *Multi wavelength Optical Networks: A Layered Approach*. Reading, MA: Addison Wesley Longman Inc., 1999.

[6] J.-P. Vasseur, M. Pickavet, and P. Demeester, *Network Recovery: Protection and Restoration of Optical, Sonet-SDH, IP and MPLS*. San Mateo, CA: Morgan Kaufmann, 2004.

[7] D. Zhou and S. Subramaniam, "Survivability in optical networks," *IEEE Network Magazine*, Vol. 14, No. 6, Nov-Dec. 2000, pp.16-23.

[8] S. Ramamurthy and B. Mukherjee, "Survivable WDM mesh networks, part I-protection," *Proceedings of* IEEE *Conference on Computer Communications (INFOCOM)*, 1999,pp. 744–751.

[9] Amir Askarian,et al., **"**Cross-Layer Approach to Survivable DWDM Network Design" *Journal of Optical Communication and Networking*, Vol. 2, No. 6, June 2010, pp.319-331.

[10] Lei Guo, and Lemin Li, "A Novel Survivable Routing Algorithm With Partial Shared-Risk Link Groups (SRLG)-Disjoint Protection Based on Differentiated Reliability Constraints in WDM Optical Mesh Networks" *Journal Of Light wave Technology*, Vol. 25, No. 6, June 2007, pp.1410-1415.

[11] Yoshiyuki Yamada, Hiroshi Hasegawa, and Ken-Ichi Sato, "Hierarchical Optical Path Network Design Algorithm Considering Waveband Protection" *Journal of Light wave Technology*, Vol. 27, No. 24, December 15, 2009 pp.5736-5748.

[12] Paul Urquhart, Hervé Palezi, and Pascale Jardin, "Optical Fiber Bus Protection Network to Multiplex Sensors: Self-Diagnostic Operation "*Journal Of Light wave Technology*, Vol. 29, No. 10, May 15, 2011,pp.1427 -1436.

[13] Baroni and Bayvel," Wavelength Requirements in Arbitrarily Connected Wavelength-Routed Optical Networks", *Journal of Light wave technology*, Vol. 15, No. 2, 1997, pp. 242-251.

[14] Freire et al., "Influence of chord length on the blocking performance of wavelength routed chordal ring networks", Towards *on Optical Internet: New Visions in Optical Network Design and Modeling*, Kluwer,2002, pp. 79–88.

[15] Yuan and Xu, "The Influence of Physical Network Topologies on Wavelength requirements in Optical Networks", *Journal of Light wave Technology*, Vol. 28, No. 9, 2010, pp.1338-1343.

[16] Fenger, E. Limal, U, Gliese, and C. J. Mahon,"Statistical study of the correlation between topology and wavelength usage in optical networks with and without conversion", Vol. 1815 - *Lecture Notes in Computer Science*, Springer, 2002, pp.168–175.

[17] Châtelain, Bélanger, Christine Tremblay, François Gagnon, and David V. Plant," Topological Wavelength usage Estimation in Transparent Wide Area Networks", *Journal of Optical Communication and Networking*, Vol. 1, No. 1, 2009, pp. 196-203.

[18] Lumetta, S.S., Zhang, X.J., Kim, S,"Robust Dimensioning and Routing for Dynamic WDM Networks", *Proceedings of Wireless and Optical Communications Conference,* Shanghai, 2010, pp.1-5.

[19] C. Ou, K. Zhu, J. Zhang, H. Zhu, B. Mukherjee, H. Zang, and L. Sahasrabuddhe, "Traffic grooming for survivable WDM networks: dedicated protection ",*Journal of Optical Networking,* Vol. 3, No. 1, Jan. 2004,pp. 50–74.

[20] C. Ou, K. Zhu, H. Zang, L. H. Sahasrabuddhe, and B. Mukherjee, "Traffic grooming for survivable WDM networks-shared protection," IEEE Journal of Selected Areas on Communication, Vol. 21, No. 9, Nov. 2003, pp. 1367–1383.

[21] W. Yao and B. Ramamurthy, "Survivable traffic grooming with path protection at the connection level in WDM mesh networks," *Journal of Light wave Technology,* Vol. 23, Oct. 2005, pp. 2846–2853.

[22] K. Ratnam, M. Gurusamy, and L. Zhou, "Differentiated QoS routing of restorable sub-lambda connections in IP-over-WDM networks using a multi-layer protection approach," *Proceedings of the 2nd Int. Conf. on Broadband Networks,* vol. 1,Oct. 2005, pp. 127–136.

[23] Abdelhamid E. Eshoul and Hussein T. Mouftah,*"* Survivability Approaches Using p-Cycles in WDM Mesh Networks Under Static Traffic", *IEEE/ACM Transactions on Networking*, Vol. 17, No. 2, April 2009,pp.671-683.

[24] P. Rajalakshmi, , and Ashok Jhunjhunwala, "Re-Routing at Critical Nodes to Enhance Performance of Wavelength Reassignment in All-Optical WDM Networks Without Wavelength Conversion", *Journal of Light wave Technology*, Vol. 26, No. 17, September 1, 2008 ,pp. 3021- 3029.

[25] D.Sheela and C. Chellamuthu, "A Cost Effective Approach for WDM Network Protection under Critical Duct Constraints", *WSEAS Transactions On Communications,* Vol.11, No.3, March 2012, pp.103-112.

BIOGRAPHY

D. Sheela is working as a faculty in the department of electronics and communication engineering, Tagore Engineering College and currently pursuing Ph.D. in Anna University, Chennai. Her areas of interest are optical communication and networks, wireless communication and computer networks.

C. Chellamuthu received his PhD degree in Power Electronics from IIT Chennai, India. After working as an associate lecturer in GCT Coimbatore, India, he joined the Anna University Chennai, India. He is the former head of the department of electrical and electronics engineering, Anna University, India. He is currently working as a Professor at R.M.K Engineering College, Chennai, India. He has published several works in several International and National journals, pioneered several new research directions and made a number of landmark contributions in his field. His areas of interest are Power electronics, PMBDLC designs, Wind energy, Microprocessor based system design, Networking, and Image processing.