International Journal of Future Generation Communication and Networking
Vol.10, No.8 (2017), pp.39-50
http://dx.doi.org/10.14257/ijfgcn.2017.10.8.04

Scalable, Optimal and Capacity Efficient Survivable Technique (SOCEST) for Optical Network

Amit Kumar Garg

Electronics & Communication Engg. Deptt.
Deenbandhu Chhotu Ram University of Science & Technology
Murthal-131039, Sonepat (HR.) INDIA
garg_amit03@yahoo.co.in

Abstract

It is seen that preplanned protection cycles (p-cycles) have emerged as a viable scheme for recovery from failure in mesh networks. Though, the benefits of p-cycles are well established, yet there has been no systematic analysis of how much bandwidth they consume in comparison with the classical shared link or with path protection schemes. It is observed that, even enumerating a huge number of cycles, not necessarily a guarantee for obtaining good quality solutions with the Integer Linear Programming (ILP) models. In the present work, a scalable, optimal and capacity efficient survivable technique (SOCEST) has been formulated and proposed which outperforms the existing ones in terms of capacity efficiency as well as in terms of traffic recovery speed. The proposed new framework is found to be efficient than existing schemes since it adds one or two links rather than constructing a new p-cycle. Moreover, it is faster w.r.t to provisioning since it does not require finding new cycles in the network and this makes it more beneficial for supporting dynamic traffic. Extensive experiments have been conducted for comparison. Simulation results show that the presented work outperforms the previous methods in terms of capacity efficiency as well as redundancy.

Keywords*: optical networks; protection; network survivability; WDM*

1. Introduction

WDM (Wavelength Division Multiplexing) networks have gained tremendous popularity due to their ability to tap the enormous amount of bandwidth in an optical fiber. Their growing popularity and bandwidth capacity have made survivability in these networks an important aspect.WDM mesh networks are promising as next-generation backbone networks as its intelligence, scalability and huge-bandwidth. Due to its high-speed characteristic, a single fiber cut may lead to huge data and revenue loss. WDM mesh networks are prone to failure [1-2]. Therefore, WDM mesh optical network survivability against a single failure is a very important issue in the design of WDM mesh networks.

A key driver for optical networking technology has been the sustainment of the internet growth. Researchers have contributed with many advances in optical wavelength division multiplexing (WDM) equipment and networking architectures to meet these Internet traffic needs, leading to an optical technology that currently offers immense bandwidth scalability. Given the immense scale of WDM networks and how much downtime can cost a business, service survivability issues are of paramount importance. The design of a mesh WDM network usually proceeds in two steps, firstly the establishment of the working (or routing) paths with the objective of minimizing the working capacity or the equipment cost. Secondly, protection paths are set in order to offer resilience against failures. It is well known that fiber cuts are the dominant failure pattern and that protection against single link failure is a reasonable assumption. In

ISSN: 2233-7857 IJFGCN

literature, there are two approaches namely ring and mesh to survivable network design. Ring restoration uses the protection of the fiber running in the opposite direction to the working flow for protection. Ring restoration schemes can be designed in multiple ways. They can be line switched or path switched unidirectional or bi-directional. The main quality of rings is that they can perform very fast switching of the order of 50ms.However they suffer from a main drawback of requiring at least 100% spare capacity. Protection paths are usually pre-connected and hence can provide fast restoration. Also they suffer from the limitation that the traffic can only be routed on the ring. Mesh restoration is more capacity efficient. Dynamic state dependent routing mechanisms are used that make each unit of spare capacity reusable. Also in a mesh network the traffic can be routed independent of the topology of the network using shortest path algorithms. However cost of this efficiency is increased delay. Restoration in a mesh network can take as much as two seconds to restore a span. Each of these mechanisms has its own tradeoffs. For WDM-networks, p-cycles can provide fast protection switching times and achieve high resource efficiency. The p -cycles based networks allow us to utilize the advantages of both rings as well as mesh networks. They are fast, efficient and allow the traffic flow to be routed independent of the protection topology. They have been proven to be most efficient pre-connected protection mechanisms. Several survivability strategies can be found in the literature, all based on a set of features that have an impact on the network operation. A survivable network can either use a protection or a restoration scheme. In a protection scheme, the redundant resources are pre-computed and reserved in advance. On the opposite, restoration schemes take action in real time, including resource allocation and path cross-connections, based on the failure and the state of the network at the time of failure. While restoration schemes are usually more bandwidth efficient because they do not allocate spare capacity in advance, protection schemes have faster restoration time and can always guarantee recovery from failure. Link protection (restoration) consists in protecting each link as one entity, regardless of the connection demands that go through it, while path protection (restoration) protects each demand individually by providing a surviving protection path between its end nodes. Although path protection (restoration) schemes lead to an efficient utilization of backup resources, they also lead to a longer failure detection and recovery than link protection (restoration). Moreover, survivability mechanisms can either use dedicated capacity, where spare capacity for each link or path is exclusively allocated or shared capacity, where spare capacity can be shared among several protection paths under the single failure assumption. The key advantage of pre-configured protection cycles or p-cycles lies in their switching speed and simplicity, similar to ring networks, as the protection paths around the surviving portions of the cycle are pre-connected at the outset and the only required switching actions take place at the end nodes of the failure. A p-cycle is a promising approach for survivable design in WDM networks because of its ability to achieve ring-link recovery speed while maintaining the capacity efficiency of a mesh-restorable network [3-4]. A p-cycle is a pre-configured cycle formed out of the spare capacity in the network, which occupies one unit of spare capacity on each on-cycle span. Like a self-healing ring, a p-cycle provides one restoration path for every on-cycle span; unlike a self-healing ring, a p-cycle also provides two restoration paths for every straddling span-a span whose two end nodes are on the cycle but itself is not on the cycle. Due to the highly combinatorial nature of p-cycle designs, nearly all studies are based on an explicit enumeration of cycles, resulting in difficulties for assessing the quality of the solutions provided by the resulting huge ILP models. The p-cycles are fully pre-connected cyclic protection structures with pre-planned spare capacity. When a link failure occurs, only the two end nodes of the failed link perform protection switching. Unlike rings, p-cycles protect against straddling link failures, enabling two protection paths, one on each half of the cycle, with only one unit of spare capacity. The p-cycles also provide protection against failures on links over the ring itself. Under a link protection scheme, the interrupted traffic is rerouted only around

the failed link. Thus, the total amount of working traffic on each link is considered for protection, regardless of the connections going through it. Link-protecting p-cycles were extended with the goal of providing end-to-end path protection, originating the Failure Independent Path-Protecting (FIPP) p-cycles [5-7]. Under FIPP p-cycles, the cyclic protection structures can be shared by a set of working paths for protection as long as the working paths or their protection paths are mutually disjoint in this set. Path protection consists in protecting each demand individually by providing a protection path, diversely routed from its working path. In case of a link failure, a notification signal is sent to the end nodes of each connection traversing the failed link in order for them to switch the traffic over from the working path to the protection path. Shared Backup Path Protection (SBPP) is a failure independent path protection scheme where the connections on the affected working paths are switched to predefined and diversely routed protection paths. Cross-connection operations to set up the protection paths are performed at the time of the failure. Unlike 1+1 protection, SBPP allows the spare capacity allocated to protection routes to be shared over failure-disjoint working paths. In a network with nodes and links there is a capacity (C_{ij}) associated with each link (ij). Also each link carries a traffic which is the working capacity (W_{ij}) of the link. This working capacity is always less than or equal to the capacity of the link. Spare Capacity (S_{ij}) of a link is the difference between the total and the working capacity of the link. The p-cycles are made out of this spare capacity. These p-cycles are used to protect the working capacity in case link fails. The p-cycles protect both on cycle and straddling links. The main reason to the efficiency of a p cycle is straddling link protection which is effectively obtained free of cost and the speed of restoration is inherited from their ring like structure.

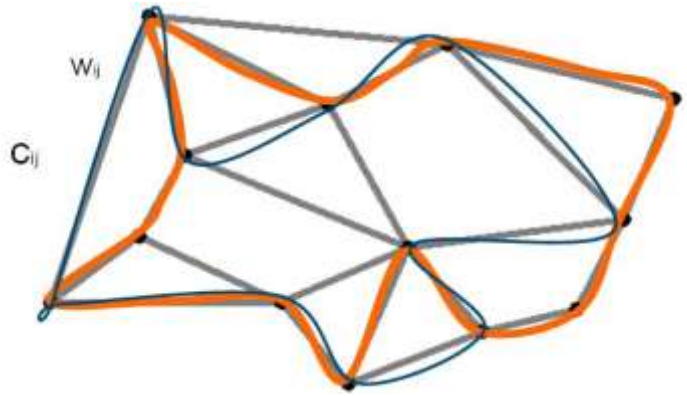

Figure 1. Formation of a p-cycle in a Network

The rest of this paper is organized as follows. Background and related work is reviewed in section II. Then, a proposed scheme named as a scalable, optimal and capacity efficient survivable technique (SOCEST) has been developed as well as described in section III. Section IV gives the simulation results. Finally, the paper has been concluded along with future directions in section V.

2. Background and Related Work

The interruption of service for even a short time may have disastrous consequences unless the channel failure is immediately recovered. For this reason, survivability against network failures is a particularly important issue. Network failures basically occur at either nodes or links of the network. Link failure is caused by cable cuts while node failure refers to the failure of components at the network nodes. The survivability of a network refers to a network's capability to provide continuous service and maintain

quality of service in the presence of such failures. Many researchers have investigated the issue of network survivability. Survivability should guarantee maximum restorability to provide quality of service (QoS) against failures. There exists both pre-planned protection and dynamic restoration mechanisms in survivability. Dynamic protection methods are not able to guarantee 100% protection, but offers faster restoration time [8].Pre-planned protections, however, provide 100% protection by reserving alternative paths in advance [8-9]; hence this mechanism is a more interesting development in survivable networks. Pre-configured protection cycle (p-cycle) has been developed to utilize the advantages of both ring and mesh protection mechanisms. It benefits from the fast restoration time of ring mechanisms and the capacity efficiency of mesh mechanism. A p-cycle protection makes it possible to achieve low spare capacity by determining an appropriate set of p-cycles [10-11]. However, determination of the optimal set of p-cycles for protection is an NP-hard problem. Existing approaches for solving the p-cycle problem are through the use of an Integer Linear Programming (ILP) model [12-13]. The ILP model achieves the optimal solution in terms of minimizing the spare capacity while maintaining 100% protection. However, the ILP model becomes intractable with large scale networks where the number of possible variables is very high. This gives the motivation to investigate heuristic approaches for p-cycle network design. Simple and efficient heuristic methods are greatly desirable. One of the most important issues in the network optimization problem is capacity utilization. It is generally evaluated by measuring the redundancy. Low redundancy is more efficient than high redundancy due to the fact that high redundancy requires large spare capacity to protect against failures. A p-cycle protection offers useful restoration paths depending on the relationship to the failed link. Searching suitable paths is an important issue in p-cycle protection since efficient paths can offer better capacity efficiency. A comprehensive comparison has been shown (table.1) between ring, mesh and p-cycle protection mechanisms.

Table 1. Comparison of Ring, Mesh and p-cycle Protection Mechanisms

Attribute(s)	Ring	Mesh	p-cycle
Restoration time	50 - 60msec	100msec - 2sec	50 - 60msec
Redundancy	100% - 200%	50 - 70 %	50 - 70 %
Network design	simple	complex	simple
Capacity efficiency	low	high	high
Cost	low	high	low

A p-cycle protection makes it possible to minimize the redundant capacity by determining an appropriate set of p-cycles. However, determining an efficient and sufficient set of p-cycles is difficult. Many researchers have investigated how to construct suitable candidate p-cycles for solving this optimization problem. Two versions of the optimization have been investigated the non-joint version and the joint version [6-7]. The objective of the joint version is to minimize the total capacity. It minimizes working capacity and spare capacity jointly by using p-cycles while maximizing the restorability. On the other hand, the non-joint version minimizes the working capacity and spare capacity separately. That is, after the distribution of working capacity in the non-joint version is known, a set of candidate p-cycles is computed to minimize spare capacity with maximum protection capability. According to the literature, the joint version of optimization may achieve better capacity utilization but has a higher complexity and requires a longer computation time. Besides link protection, p-cycles has been extended to protect segments and paths in [8-11]. Reference [9] proposed a Failure Independent Path-Protecting (FIPP) p-cycle which is a more capacity efficient protection strategy than link protecting p-cycle. Recently, the author of [14] introduced a new 1+N protection scheme

against single-link failures by combining network coding and p-cycles. Besides p-cycles, other pre-configured structures are also used for fast recovery, such as non-simple p-cycle, p-trails, p-trees and Cooperative Fast Protection (CFP) [12-14]. A cycle is a non-simple cycle if one or more node on the cycle is traversed by the cycle more than twice. The study in [13] reveals that the major capacity gain of non-simple p-cycles over simple p-cycles lies in small networks with lightly-loaded traffic. In [15], the authors extended traditional p-tree by adding links to form a more flexible protection pattern, such as cycles, trails or trees. It is a link-based protection scheme and provides higher protection capacity than link-protecting simple and non-simple p-cycles. However, the short recovery time cannot always be guaranteed due to the flexibility of the protection structure. The authors in [16] enhanced the protection capacity utilization by solving the backhaul problem, in which the same link is traversed twice in opposite directions by the protection path before reaching the destination after a link failure. However, it suffers from longer switch reconfiguration time due to the fact that all failure-aware nodes need to carry out protection switching after failure detection. Regardless of the protection schemes, the trade-off between the capacity efficiency and failure recovery speed always exists [17-21].

3. Proposed Scalable, Optimal and Capacity Efficient Survivable Technique (SOCEST) for Optical Network

Single link failure is easy to protect using p-cycles. However with the increasing size of networks today, simultaneous double failures are not uncommon. Designing p-cycle based networks to protect against such failures is gaining importance. In the present work, a scalable, optimal and capacity efficient survivable technique (SOCEST) has been proposed .This new framework is more efficient since it adds one or two links rather than constructing a new p-cycle. The proposed technique investigates the possibility of using a heuristic method in order to achieve the best performance in terms of computational complexity. Computation time and the capacity utilization are managed by the proposed scheme (SOCEST) to achieve the desired restorability. Consequently, it ensures better protection while minimizing the total spare capacity and reducing computation time.
The following is the detailed description and working of the analytical model of the proposed scheme (SOCEST) for WDM systems.

1) A network physical topology is considered as an undirected graph G (V, E), where V is a set of network nodes and E is a set of network spans.
2) The topology obtained after aggregation is composed of all border nodes, which are connected by virtual links. Each pair of border nodes within a domain is connected by a virtual link. A virtual link connecting a pair of border nodes corresponds to the set of primary lightpaths interconnecting these nodes in the physical topology. An integer is associated with each virtual link indicating the numbers of primary lightpaths existing between the two border nodes. Two virtual links have to be physically disjointed, which means that the light-paths connecting one pair of border nodes must be disjointed from all the lightpaths between any other pair of border nodes. For each link, an integer value indicating the working capacity of the link is associated.
3) The network configuration process of p-cycles in proposed scheme has been framed as follows. First, a given demand for connections is routed through the network, so that the links reserve (working) capacity for the demands. The spare capacity of the links is the remaining available capacity. Then the p-cycles are formed in the spare capacity of the network. The set of link p-cycles is chosen such that for every link the working connections are protected by p-cycles of corresponding capacity. The routing of the demands has to be adapted, if a protecting set of p-cycles cannot be found.

4) In the proposed scheme, working paths and protection cycles are provisioned jointly such that the minimum total cost is achieved.
5) Each unicast session is bidirectional with a unitary traffic rate (one wavelength) and the traffic in both directions has to be routed through the same paths and protected. Each span has enough wavelengths and each node is equipped with wavelength converters over all wavelengths such that wavelength continuity is not required in the network.
6) In order for the network to survive any single span failure and to minimize the spare capacity required for protecting a given working capacity distribution, the candidate cycles in the proposed scheme protect all spans in the network. That is, each span is either on an on-cycle span or a straddling span of some candidate cycle with high efficiency (efficiency means a priori efficiency).
7) A network is represented by a graph G = (V, E) where V is the set of nodes V = $\{v_1, v_2, v_3.....v_N\}$ and $|V|$ = N and E is the set of edges or link (L), E = $\{e_1, e_2, e_3.....e_N\}$ and $|E|$ = L.
8) A failure may be of a single link $e_l \in E$ or a single node $v_n \in V$ or a group of multiple links or multiple nodes or a combination of links and nodes. Sub-graph routing is a proactive fault tolerant technique that ensures 100% restoration for all failure scenarios, included in set 'F', for which the network is designed.
9) A sub-graph $G_k = (V_k, E_k)$ derived from a network G = (V, E) is created for each of the failure scenarios $f_k \in F$ by removing all the edges contained within the failure set.
10) Mathematically, $G_k = (V_k, E_k)$ where V_k = V and E_k = E - f_k. For a connection entering a sub-graph fault tolerant network, it must be successfully routed in all the sub-graphs. If it cannot be routed for any G_k, then the request is blocked, as it would not be protected against all failure cases. The original graph G = (V, E) is assumed to be as the base network.
11) The base network's constituent sub-graphs $G_k = (V_k, E_k)$ are conceptual graphs as they only maintain a state of the base network.
12) The proposed scheme avoids the computationally hard step of cycle enumeration at each step. It is based on the observation that a p-cycle may be seen as a combination of two node disjoint paths between a straddling span. A basic condition for this to happen is that both the end nodes have a degree of 3 at least.

The following is the pseudo code of the proposed SOCEST scheme for optical networks.

Input: Network topology, Graph G = (V, E), failure set F = {f_1, f_2, f_3.....f_k} and a set of requests R.
O_{ss}: Overlap segment source
O_{sd}: Overlap segment destination
O_{ws}: Wavelength of overlap segment
Output: Set of candidate p-cycles to route a request R_k, unprotected working capacity (W)
Check network condition
S ← number of spans in the network
Create sub-graphs $G_k = (V_k, E_k)$ where $V_k = V$ and $E_k = E - f_k \; \forall \; f_k \in F$
Attempt routing the connection on each sub-graph Gk.
if the connection is accepted in all sub-graphs then the connection is accepted in the base network
else the connection is dropped from the network

while sum of W is not zero do
calculate for each candidate cycle, R (Redundancy)= $\frac{\sum_{i \in S} p_i}{\sum_{i \in S} w_i}$, where w_i indicates the number of units of working capacity on span i and p_i is the corresponding number of spare capacity units on span i. Remove the working capacity of the selected p-cycle from W
end while
for i = 1 to |S| do
search two shortest disjoint path between two end nodes of span i
determine a p-cycle using the two paths found
end for
for w ← 1 to W do
if w≠ O_{ws} and $P^{w}_{os,od} \neq \emptyset$ then
compare links of overlap segment and $P^{w}_{os,od}$osod
if Links are the same then
relocate overlap segment to $P^{w}_{os,od}$
else relocate overlap segment on $P^{w}_{os,od}$
end if
end if
end for

Since the number of cycles increases exponentially with network sizes, all the cycles are not enumerated in a given network formulation. Instead, the flow variables form the cycles in the proposed scheme. The source and destination nodes of the session connect to only one span used by each path, but each intermediate node is connected by two adjacent spans. The working and backup paths of any session are link-disjoint to survive any single-link failure. The cycle constraints make sure that each node on the cycle is passed twice by on-cycle spans. The proposed scheme (SOCEST) is found to be more efficient than existing schemes since it add one or two links, rather than constructing a new p-cycle. The proposed scheme (SOCEST) proved to be efficient and provided promising results. Also another key point here is that protection against multiple failures is provided without adding extra capacity to the network using the same cost and thus more protection is obtained.

Moreover, it provides fast provision since it does not require finding new cycles in the network and this also makes it more suitable for dynamic traffic.

4. Performance Evaluation

The node-pair is interconnected by a bi-directional fiber link. Each network node is assumed to have the wavelength conversion capacity. All simulations were run on a DELL Quadri Dual Core Xeon processor with 4GB of RAM. Matlab is used to solve the ILP formulations. The traffic demand is uniformly distributed among all source–destination pairs. Each demand requests one unit of capacity. The working capacities on the network links are obtained by routing each demand over the shortest path. Also in the simulation, it is assumed that request arrival follows a poisson process with an average arrival rate λ and the request holding time follows an exponential distribution with an

average holding time μ. Thus, the offered traffic load for the network is given by λ/μ. The results for network traffic simulations have been obtained using the software Network Simulator [22] and for analytic results, data processing and plotting are carried out using standard commercial software. Computational complexity is an important factor when evaluating any survivable scheme. It is defined as the time it takes for an algorithm to find a solution. If an algorithm can achieve a near optimal solution with acceptable computational complexity, it will likely be a desirable solution to the problem. It is assumed that the original lightpath establishment is on the route with the minimum number of hops between source-destination nodes, i.e., the route with the shortest hop length. The processing delay for handling each restoration request on each node is assumed to be equal to 6 microseconds. Link transmission rate is 2.5Gb/s. Each node maintains global network state information for routing and this information is periodically updated. The network topology (l1nodes and 23links) used for the simulation is shown in Figure 2.

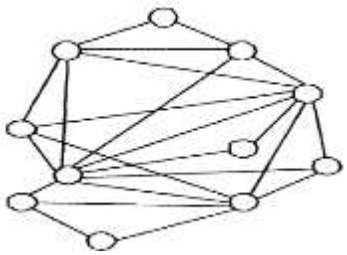

Figure 2. Simulated Network Topology (l1nodes and 23links)

A performance criterion for each metric is computed according to the traffic load. For each traffic load value, 5×10^5 requests were generated. This number of requests is enough to measure blocking probability, resource utilization and average computation time with a 95% confidence interval. The physical parameters used for the simulated network are shown in table.2.

Table 2. Physical Parameters used for the Simulated Network

S.No.	Attribute	Numerical Value
1.	Signal peak power	2 mW
2.	Bit duration	100 ps (10 Gbps)
3.	Pulse shape	NRZ
4.	Adjacent port crosstalk	−25 dB
5.	Non adj. port crosstalk	−50dB
6.	Fiber loss	0.2 dB/km
7.	Linear dispersion	15 ps/nm/km
8.	Noise factor	2
9.	Receiver electrical bandwidth	7 GHz
10.	Minimum Q factor	6
11.	Span length	80 Km

In the proposed work, the comparison is based on the redundancy of the network. Redundancy is a measure of architectural efficiency for survivable networks and is measured by the ratio of spare to working cost. In other words, the more redundant is the design, the more protection cost it requires. As shown in Figure3, the redundancy is reduced for all design methods as the network average nodal degree increases. The proposed scheme achieves the lowest redundancy and conventional protection schemes have the highest redundancy. When the nodal degree is relatively small, the difference in the redundancy between proposed scheme and conventional protection schemes is significant. When the nodal degree increases, the difference becomes smaller. That is, the proposed scheme is superior to conventional protection schemes, especially when the network nodal degree is relatively small.

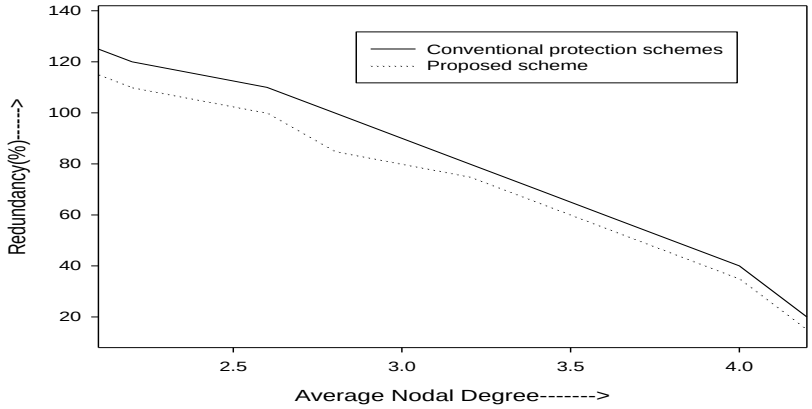

Figure 3. Redundancy Vs. Average Nodal Degree

Capacity redundancy is defined as the ratio of spare capacity usage over working capacity usage. As shown in Figure4, the redundancy is decreased when more candidate p-cycles are selected. For conventional protection schemes, the redundancy is high when less candidate p-cycles are selected. However, proposed scheme is better than conventional protection schemes. The main reason is that conventional protection schemes consider the topological relationship between a p-cycle and a network, but without any other aspects like traffic demand pattern and traffic flow characteristics of the network, where as the proposed scheme considers not only topology information, but also how the traffic demand routing on the p-cycles. It is seen that the proposed scheme shows less capacity redundancy (more capacity efficient) than conventional protection schemes. The differences of capacity redundancy between proposed scheme and conventional protection schemes range from 7% to 10%. The result suggests that proposed scheme is an efficient protection approach for both link and node protection against a single failure. The larger the p-cycle is, the more likely it is to enable working paths share the protection path against a single node failure. As the resulting solution requires less distinct p-cycles thus it is more capacity efficient and also outperforms conventional protection schemes in terms of management.

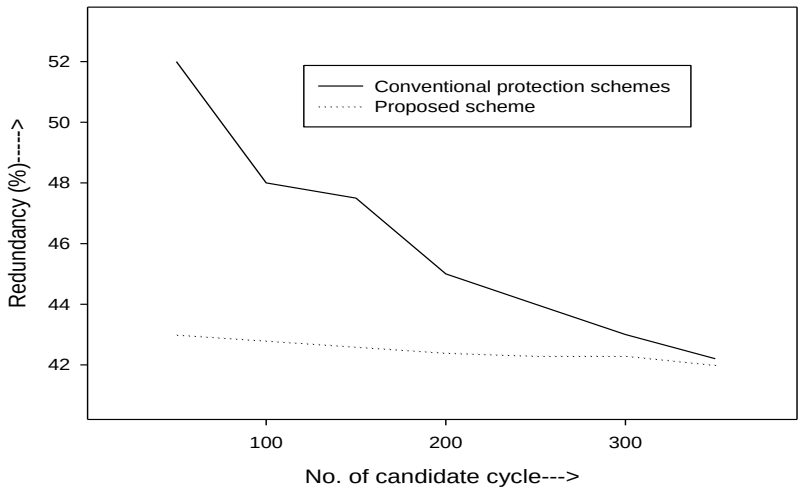

Figure 4. Redundancy Vs. No. of Candidate Cycles

Figure 5 plots the blocking probability against various traffic load (arrival rate per node in erlangs) for the proposed scheme (SOCEST) and conventional protection schemes. As the arrival rate increases, the blocking probability increases but in less proportion as compared to conventional protection schemes because of the scarcity of network resources at higher arrival rates.

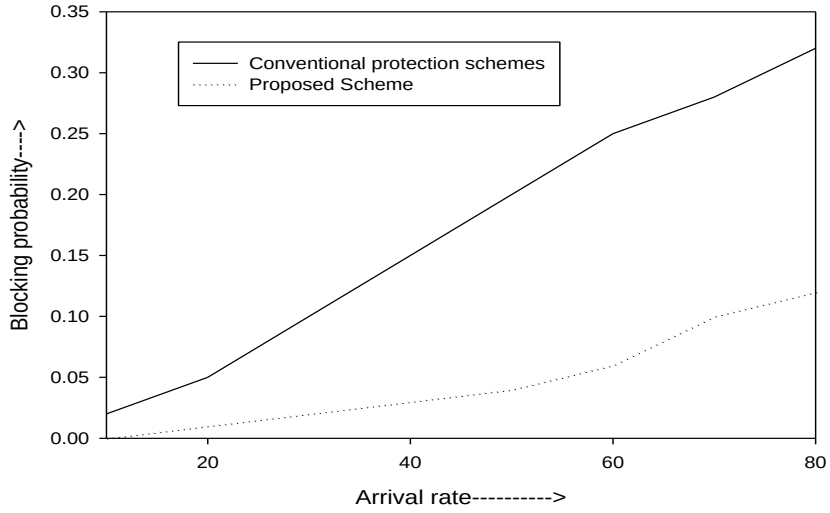

Figure 5. Blocking Probability vs. Arrival Rate

To assess the speed of the proposed scheme, performance metric average computation time has been considered for setting up a multicast request. The average computation time in the proposed (SOCEST) scheme is very low compared with that of the existing protection scheme (as shown in fig 6). This is due to the availability of reasonable number of optimum-cycles for providing resiliency in the network.

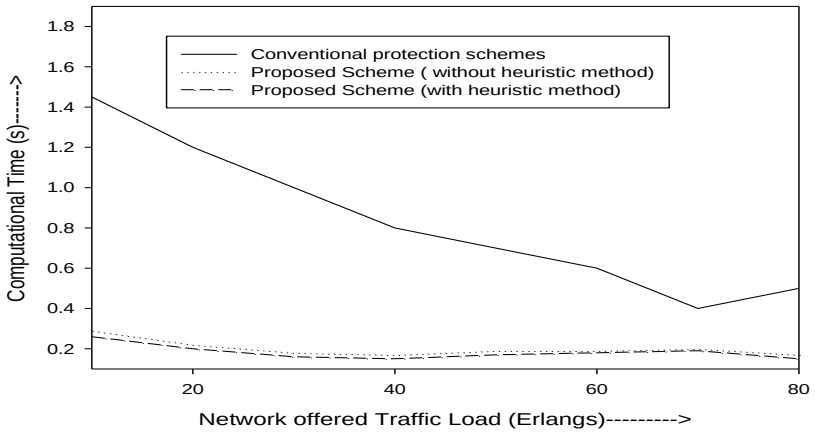

Figure 6. Performance Comparison of Average Computation Time

5. Conclusion and Future Scope

In the proposed work, a scalable, optimal and capacity efficient survivable technique (SOCEST) has been proposed with a motive on balancing towards optimality of solution and computational complexity. The objective of the proposed scheme is to perform a fair and accurate comparison based on optimal or near optimal design solutions. The simulation results indicate that the proposed (SOCEST) scheme outperforms the traditional protection schemes in terms of blocking probability, computation time and redundancy. More redundant designs are less capacity efficient and consequently, less costly. Although p-cycle designs are more redundant than classical protection schemes, yet the proposed scheme is an attractive choice from the operational point of view. This scheme also achieves near optimal solutions within acceptable computational complexity. Numerical results show that an improvement in capacity redundancy from 15 to 20 % over the previous methods has been observed by using the proposed scheme. Future efforts will look at developing more detailed optimization models to derive lower bounds on achievable performance.

References

[1] D. Stamatelakis and W. D. Grover, “Theoretical underpinnings for the efficiency of restorable networks using pre-configured cycles p-cycles,” IEEE Transactions Communications, vol. 48, **(2000)**, pp. 1262-1265.
[2] S. Ramamurthy, L. Sahasrabuddhe, and B. Mukherjee, “Survivable WDM mesh network,” Journal of Lightwave Technology, vol. 21, no. 4, **(2003)**, pp. 870-883.
[3] D. Xu, Y. Xiong, C. Qiao, and G. Li, "Trap avoidance and protection schemes in networks with shared risk link groups", IEEE Journal of Lightwave Technology, vol. 21, no. 11, **(2003)**, pp. 2683-2693.
[4] G. X. Shen and W. D. Grover, “Extending the p-cycle concept to path segment protection for span and node failure recovery”, IEEE Journal on Selected Areas in Communications, vol. 21, no. 8, **(2003)**, pp. 1306-1319.
[5] Z. Zhang, W. D. Zhong and B. Mukherjee, "A Heuristic Method for Design of Survivable WDM Networks With p-Cycles", IEEE Communication Letters, vol.8, no. 7, **(2004)**, pp. 467-469.
[6] H. Wang, H.T. Mouftah, "P-cycles in multi-failure network survivability", Transparent Optical Networks, 2005, Proceedings of 2005 7th International Conference , vol.1, **(2005)**, pp. 381-384.
[7] W. D. Grover, A. Kodian, "Failure-independent path protection with p-cycles: efficient, fast and simple protection for transparent optical networks", Transparent Optical Networks, vol.1, **(2005)**, pp. 363-369.
[8] G. Shen and W. D. Grover, “Design and performance of protected working capacity envelopes based on p-cycles for dynamic provisioning of survivable services”, Journal of Optical Networking, vol. 4, no. 7, **(2005)**, pp. 361-390.

[9] A. Kodian and W. D. Grover, "Failure-Independent Path-Protecting p-Cycles: Efficient and Simple Fully Preconnected Optical-Path Protection," IEEE Journal of Lightwave Technology, vol. 23, **(2005)**, pp.3241-3259.
[10] L. Ruan, F. Tang and C. Liu, "Dynamic establishment of restorable connections using p-cycle protection in WDM networks", Journal of Optical Switching and Networking, vol. 3, no. 3-4, **(2006)**, pp. 191-201.
[11] D. Lastine, A.K. Somani, "Supplementing Non-Simple p-Cycles with Preconfigured Lines", Communications, IEEE International Conference, **(2008)**, pp. 5443-5447.
[12] A. Eshoul and H. Mouftah, "Survivability approaches using p-cycles in WDM mesh networks under static traffic," IEEE/ACM Transactions on Networking, vol. 17, no. 2, **(2009)**, pp. 671–683.
[13] B. Wu, K. L. Yeung and P.-H. Ho, "ILP formulations for non-simple p-cycle and p-trail design in WDM mesh networks", Computer Networks, vol. 54, no. 5, **(2010)**, pp. 716-725.
[14] A. E. Kamal, "1+N Network Protection for Mesh Networks: Network Coding-Based Protection using p-Cycles", IEEE/ACM Transactions on Networking, vol. 18, no. 1, **(2010)**, pp. 67-80.
[15] R. Asthana, Y. Singh, and W. Grover, "p-Cycles: An overview," Communications Surveys Tutorials, IEEE, vol. 12, no. 1, **(2010)**, pp. 97–111.
[16] H. Li, B. Jaumard and X. Fu, "A new approach for the provision of non-simple node-protecting p-cycles", Advanced Research on Electronic Commerce, Web Application and Communication, **(2011)**, pp. 303–308.
[17] D. Onguetou and W. Grover, "p-Cycle protection at the glass fiber level," Computer Communications, vol. 34, **(2011)**, pp. 1399 – 1409.
[18] A. Saleh and J. Simmons, "All-optical networking - evolution, benefits, challenges, and future vision", Proceedings of the IEEE, vol. 100, no. 5, **(2012)**, pp. 1105 –1117.
[19] M. Eiger, H. Luss, and D. Shallcross, "Network restoration under dual failures using path-protecting preconfigured cycles", Telecommunication Systems, vol. 49, **(2012)**, pp. 271–286.
[20] H. Alazemi, S. Sebbah, and M. Nurujjaman, "Fast and efficient network protection method using path pre-cross-connected trails", Journal of Optical Communications and Networking, vol. 5, no. 12, **(2013)**, pp. 1343-1352.
[21] J. Lopez Vizcaino *et al*., "Protection in optical transport networks with fixed and flexible grid: cost and Energy efficiency evaluation", Optical Switching and Networking, vol.11, **(2014)**, pp.55-71.
[22] The Network Simulator: NS2, http://www.isi.edu/ ns-nam /ns/.

