Optimization of Shared Path Protection for SONET/SDH Network

Deepak Dhadwal, Ashok Arora ,VR Singh

Abstract—High bandwidth applications and services requirements are provided by the SONET/SDH network. Because of this high bandwidth requirement fault tolerance and network recovery are important issues to optimize. SONET/SDH is time division multiplexing technologies popularly used in transport networks to provide bandwidth services. Dynamic services provisioning is one of the technique in which the algorithms are required that automatically compute the paths to which need to follow for routing purposes. This is needed to satisfy the service requests. In this paper, algorithms for multiplexing structures to provide the efficient bandwidth structures has been defined and implemented. Bandwidth is an important factor which is needed to optimize for efficient uses of SONET/SDH network. Two types of bandwidth protection is here one is Shared path protection and Dedicated Path protection. In this paper, Shared path protection studied, analyzed and implemented. An optimized shared protection algorithm is also discussed and implemented.

IndexTerms—SONET/SDH, Path protection algorithm, bandwidth protection algorithm.

1. INTRODUCTION

The emergence of SONET technology has provided a promising solution to the ever increasing demand for telecommunications bandwidth over recent years[1]. However, as a consequence of the high bandwidth demand, fault tolerance and network recovery have become important issues. Each channel transmitting at rates over 100 megabit per second, even one failure of fibre can result in severe data and revenue losses, with multiplexing of wavelength[2]. Service providers have been forced to seriously consider resilience mechanisms and schemes that could improve the performance of their networks and keep their customers satisfied.

The Service Level Agreement is a contract between the service provider or network operator and the customer that stipulates certain Quality of Service (QoS) guarantees[2]. The operator may bear financial penalties if the QoS doesn't meet the requirements. , One of the main concerns of the operator is to provide satisfiable connections to avoid penalty, along with minimizing resources and cost. There are several approaches that can be considered to ensure resilience in SONET[3][4][10]. These are based on two basic survivability paradigms:

1. Path/Link Restoration
2. Path/Link Protection

Recovery involves the rerouting of normal traffic by traversing the working path (WP) over a new path called the backup or protection path (PP). In general, restoration is a dynamic scheme whereby spare resources are used to find recovery paths at the time the failure occurs.

Restoration schemes therefore have the advantage of being more efficient than protection schemes since they utilize spare capacity only when required. Whereas, the schemes of dedicated protection reserve resources in advance to cater for possible scenarios of failure[2]. Dedicated protection schemes, shared-backup protection were introduced to improve resource utilization and allowing the sharing of backup resources between connections when the corresponding working resources are mutually diverse. These two methods could be applied to either the links that make up end-to-end connections or entire paths from sources to their respective destinations.

A major aspect of future optical networks will be the ability to provide fast provisioning along with recovery of efficient network. So, shared-path protection may be used due to its recovery speed, efficient resources and providing guarantees on itsrestoration ability. Therefore, for achieving this, there is a need for a union control plan and algorithms that should bear the responsibility for the management of Routing and Wavelength Assignment (RWA) protocols and the setup and tear down of connections. Different QoS requirements are also important, since different customers need different levels of fault tolerance and differ in their willingness to pay for a guaranteed service. Service providers will be benefited by providing such services with different levels of reliability by improvement of efficient resource utilization and allowance of service scalability.

In this paper, section II having literature review over the Shared path protection. Section III, shows the algorithm required for the shared path protection for SONET/SDH network. Section IV, shows theShared path protection algorithms for SONET/SDH network and Section V has its implementation. Section VI has the result description and finally section VII has the Conclusion of the article.

I. Related Work

In recent years, shared-backup path protection has received much attention and there have been many studies conducted and proposals made [3]. Shared-path protection is very beneficial since spare resources arc more efficiently reserved by sharing backup resources among many

connections. Some studies have also considered double or multiple link failure scenarios, mixed shared-path protection and others have considered more complicated routing algorithms and more involved cost analysis[4]. There have also been studies that consider partial path protection exclusively. In a survey of dynamic provisioning methods for shared-backup path protection in optical networks it was found that there exists a trade-off between the operational complexity and service blocking performance.

Since SONET carry huge volumes of traffic, maintaining high levels of service availability at an acceptable level of overhead is an important and critical requirement[2]. Recent studies regarding the evaluation of future optical networks have highlighted network reliability and placed emphasis on the performance of the routing and recovery algorithms used therein. Such networks are expected to provide fast, cheap and reliable services to satisfy the ever increasing demand by end users[6].

Network operators and service providers are in a fiercely competitive market, striving for more and more productivity. Therefore, high network performance and reliability are relied upon to reduce operation and maintenance costs and increase revenues[6][7]. Furthermore, the service providers are contractually obligated in terms of SLA requirements to meet certain levels of service. Investigating differentiated services that cater for different quality of service requirements is an interesting issue which is motivated by how much end users are willing to pay for the quality of service they require.

The above reasons provide the impetus and motivation to evaluate the performance of a shared-path protection algorithm called Reliability Aware Shared-path Protection (RASP) and, to determine whether there are any benefits over an algorithm that uses a more traditional approach, such as Conventional Shared-path Protection (CSP)[4]. The network performance parameters that are considered have been used in recent studies to evaluate important characteristics and to determine the credibility of such algorithms[8]. In general, a recovery algorithm would be considered advantageous if it results in the network having a higher degree of network integrity (the ability to provide the desired QoS) and a higher degree of survivability (the ability to recover from failures)[5]. With multimedia and real time applications forming a large percentage of today's traffic, specific QoS will be critical. Hence it is important that routing algorithms provide connections that satisfy their QoS needs, which include guaranteed reliability and tolerant to faults[6]. They are also expected to make fast and efficient use of available network resources. Studies based on the development of high performance algorithms have shown that such algorithms are an important requirement for future high performance networks. From points of view of the network and service providers, very high performance of network and its reliability will result in efficient network operation and maintenance.

In SONET, the failure of a network component leads to the failure of all connections traversing through that component [8]. The light path that carries traffic during normal operation is called the working path, in survivable networks. The traffic is rerouted over a new light path called the backup path, secondary path or protection path, when the working path fails[5]. The recovery scheme purpose is allowing the network to continue functioning in the event of a network failure. In these circumstances it would be advantageous for centralized or distributed control systems to make use of available resources to compute an alternate path (backup path) [3]. This backup path can then be used to reroute traffic affected by the failure. The backup paths may either be pre-computed or computed at the time the failure has occurred.

II. Shared Path Protection Algorithms analysis

The backup path may either be path based (i.e. from the source to destination node) or link based (i.e. from a node preceding the failure to a node succeeding the failure) So, paradigms of survivability can broadly be classified using four criteria: Execution, Computation, Rerouting and Resources.

a. Execution

Survivability scheme may be employed by a network that is executed and controlled either centrally or in a distributed manner. A central controller involved by the centralized scheme, where a source node generates requests which are to be received. The routing and wavelengthassignment have been done by the controller while updating and maintaining the network status. Frequent communicationrequired between the nodes and the central controller, to update them, which results in overhead and if the network size increases it will become problematic. No central controller is present in the distributed schemes. The operation of network is like a two level network with a network of data for physical transmission.

b. Computation

Backup or recovery paths may be computed prior or subsequent to the failure occurrence. Protection schemes use the pre-computed approach to calculate backup paths beforetheoccurrence of failure. Alternatively calculation of the backup path by the restoration schemes in real time, after the occurrence of failure. Protection schemes have the advantage of offering fast recovery due to the pre-computation of

backup paths. Restoration schemes have the advantage of efficient resource utilization since backup paths are computed only once a failure has occurred. For failure identification, time determining the recovery path and current status. These restoration schemes are slow and unattractive. Centralized schemes which involve pre-computed routes are conducive for practical implementation.

c. *Rerouting*

The backup paths may either be path based or link based. Link based approaches employ local detouring of disrupted traffic around the failed link. Path based rerouting methods provide end to end detouring by computing backup paths from the source node to the destination node.

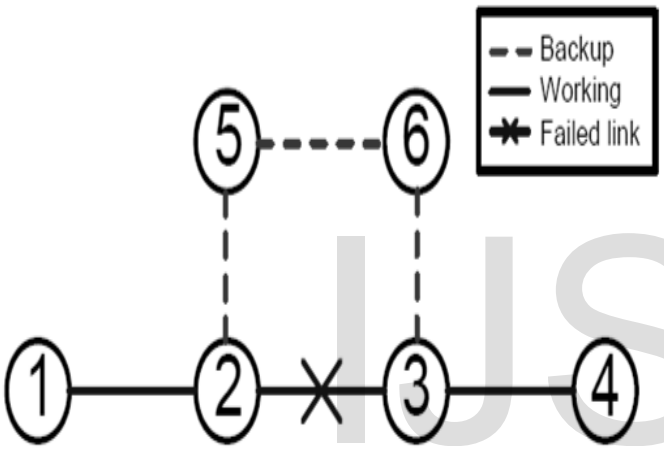

Fig. 1: Link based

Sub-path protection involves dividing the WP into a number of segments and protecting each segment separately. Compared with path protection, sub-path protection can achieve high scalability and fast recovery for a modest sacrifice and resource efficiency.

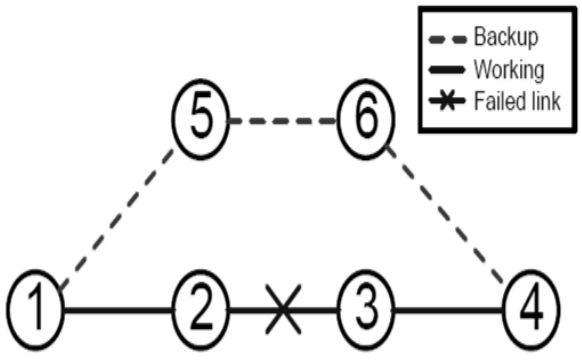

Fig. 2: Path based

d. *Resources*

Survivability schemes also differ with respect to how backup capacity or resources arc utilized. Dedicated techniques specify that each primary path should have its own dedicated backup path. In protection schemes, dedicated protection is classified into 1+1 and 1:1 schemes. In 1+1 protection, data is transferred to both the primary and secondary paths simultaneously, whereas in the 1:1 case, data is sent over the primary path only and the secondary path may be used for other low priory traffic. When the failure does occur, traffic is switched over to the backup path. 1:1 protection makes more efficient use of capacity but it is slower too. Dedicated schemes therefore use twice the bandwidth required for transmitting data to protect connections against single link failures. In the shared case, primary paths may share the same backup resources as long as the primary paths are disjoint of node and link. Backup multiplexing is done by shared approaches. To improve utilization of link, resources are shared among backup paths and these are categorized as shared-backup path protection schemes, in M:N protection. Segment shared protection may also be the form of shared protection , where protection segments may be shared between different working paths.

An example of shared-backup path protection is shown inFigure 2. In the fig. 2link disjoint working paths (l-5-6-3 and I-7-84) share common protection links (l-2 and 2-3). The disjoint constraint for the working paths is to ensure that if one of the working paths should fail, then that connection would be able to use the protection path to recover. If the working paths shared a common working path link and if that common link failed, then recovery of only one of the working paths would be possible. If the number of working paths that share protection bandwidth increases then the problem could be worse.

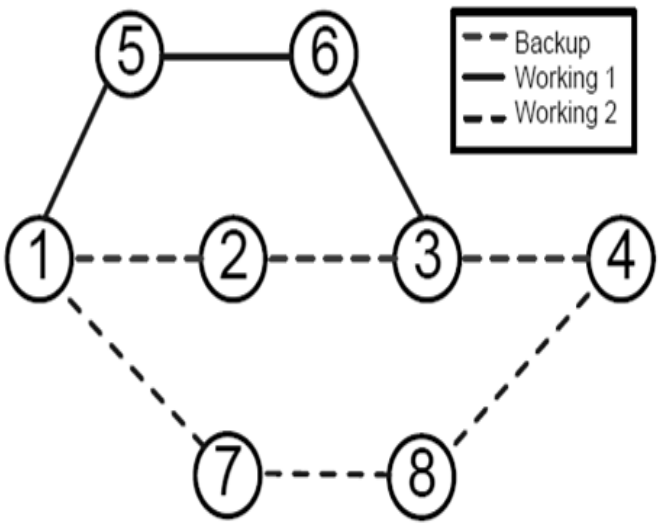

Fig. 3: Example of shared path protection

Survivability of network in general, enhances the ability of the network to support a committed QoS continuously in the presence of various failure scenarios. QoS service is a combination of several qualities, as:

- The time percentage of the operational state of the service (Availability).
- Attacks' data integrity, resistance, authentication and confidentiality (Security).
- Time taken to give response to requests to services, including recovery time, connection setup time and service mean down time (Response Time).
- Rate at which services can process requests (Throughput).

Reliability parameters mainly include availability and restoration time. Service disruption time and the quantity of data lost due to disruption are also metrics used to capture the routing dynamics in telecommunication networks. Telecom carriers and network service providers offer contracts or SLAs to their customers providing details of the QoS that their customers may expect and the penalties that may result from the SLA(Service Level Agreement) being violated. SLAs typically specify the minimum availability of service and the maximum downtime that is acceptable. The more stringent the requirements of reliability, the more costly will be the service.

III. Shared Protection Proposed Algorithm

a. Network Model:

D(N,L,W), the topology of network, where N is a node sets, L is a bi-directional link sets and W is a set of wavelengths per link. Each link is allocated a capacity of eight wavelength channels. Here, it is assumed that all nodes have wavelength conversion capability. It is also assumed that only one connection request arrives at any time point. A_N, availability matrix, has the availability values of all the links in the network. The network state is compromises of two other such matrices λ_w and λ_p which respectively store the number of working and protection wavelengths being utilized on each link at any time point. λ_p includes information about connections that are sharing protection wavelengths on a particular type of link. The traffic is dynamic and connection requests arrive without knowledge of subsequent arrivals. A connection request is described by r(s, d, a_r), where source node is 's', destination node is 'd' and availability requirement of the request is 'A_{req}'.

b. Traffic Model:

Telecommunication traffic is defined as the average number of connections in progress. A widely accepted approach to dynamic traffic modeling has been adopted in which the arrival of connection requests is a Poisson Process with a constant arrival rate ß. The arrival rate is the rate at which connection arrival requests are received by the network per unit time. Using a constant arrival rate assumes that the network is in a statistical equilibrium i.e. sudden changes in arrival rate can be ignored. This model is popular since it realistically describes the arrival of connection requests, which arc independent of each other. The connection holding time refers to the time duration of a connection from its establishment to its termination. Holding times are random and a negative exponential distribution, with a mean of l/μ, is used as time for holding. Erlangs is the measurement for traffic which is a dimensionless unit. In general, Erlang traffic ($T_{Erlangs}$) is defined by the equation

$$T_{Erlangs} = \beta(1/\mu)$$

where ß refers to the connection arrival rate and 1/μ, the mean holding time. In this study, the time measurements have been normalized by assuming 1/μ = 1 so that the network
traffic load can be considered, in units of Erlang as being equivalent to β.Destination and source nodes are randomly chosen which allows for more than one connection to be established between any pair of nodes. The implementation of waiting queue is not done and if the connection is not

established by the algorithm, then it is immediately rejected or blocked.

c. Connection Availability Analysis:

Here, reliability is measured using availability since availability denotes thetime percentage that a connection will be in its normal operating state at anyrandom point in time. Here, availability is defined and calculated for an end to end connection that is established as either a working path or a combination of working and backup paths. Connection requests that meet their fault tolerance requirements (A_{req}) are called dependable connections. Furthermore, availability is an important decision criterion, used in network planning and dimensioning studies as it is often indicated in SLAsbetween service providers and customers. It is assumed that only one link fails at a time and that the MTBF(Mean Time Between Failure) and the MTTR(Mean Time To Repair) are independent, memoryless processes. Due to the greater effect that link failures have on network performance, other network components' availability such as amplifiers and nodes has been neglected and assumed being 1.

The following notation has been used:

ij: i and j are the link connecting nodes which is represented by two unidirectional fibres.

a_{ij}: the availability of ij.

c_{ij}: the ij cost, determined by ij availability and and the ij wavelength assignment.

a_{path}: arbitrary path availability, consists of series of connected links.

a_{LDP}: the availability of a Link disjoint pair or working and protection paths.

a_{wp}: the availability of a link disjoint working path.

a_{pp}: the availability of a link disjoint protection path.

a_{PLDP}: the availability of a partial Link disjoint pair of working and protection paths.

S_1 : a set of links common to both the working and protection paths of a partial link disjoint path pair.

S_2: a set comprising the links of all link disjoint path segments of a partial link disjoint path pair.

LDP_k: the kth Link disjoint segment of a partial link disjoint path pair.

wp_k: the working path of the L- link disjoint path segment.

pp_k: the protection path of the k link disjoint path segment.

ξ: the link disjoint parameter defined between 0 and 1.

θ: the spare capacity usage factor.

d. Availability of a link Disjoint Path Pair:

An example of a link disjoint path is given in Figure 4. The example consists of a working path l-2-3-4 and a backup path l-5-6-4. CSP makes use of a pair of link disjoint paths when provisioning a connection.

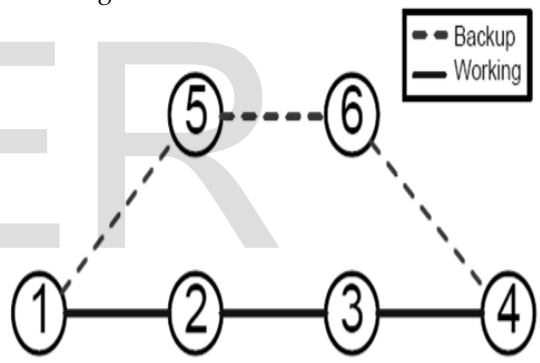

Fig. 4: Link disjoint working and backup path pair

RASP may also establish a pair of link disjoint paths, but if one is not available then it has the advantage of provisioning a partial link disjoint path as well. An example of a partial link disjoint path is given in Figure 5.

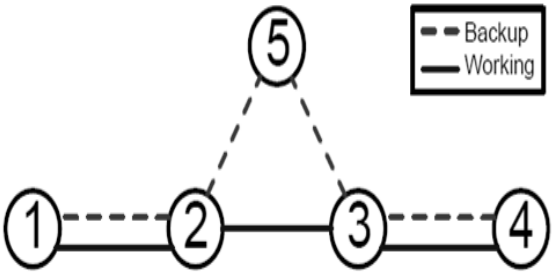

Fig. 5: Partial link disjoint working and backup path pair

As defined, the availability of wait arbitrary pathconsisting of a number of interconnected links from source to destination is given by the equation:

$$a_{path} = \prod_{ij \, \varepsilon \, path} a_{ij} \quad (2)$$

Following from Eq. 2 and with respect to Figure 4, the availability of the working and protection paths, a_{wp} and a_{pp} are respectively described by the equations:

$$a_{wp} = a_{12} \, a_{23} \, a_{34}$$

and

$$a_{pp} = a_{15} \, a_{56} \, a_{64}$$

The calculation for the availability of a link disjoint path pair is given by the equation:

$$a_{LDP} = 1-(1-a_{wp})(1 - \theta \, a_{pp})$$

$$= a_{wp} + a_{pp} - a_{wp} \, a_{pp}$$

In the following explanation, this connection will be referred to as R, comprising working path A and protection path P. In Eq.5, the spare capacity usage factor, θ, is introduced. Since RASP and CSP are both shared-backup protection schemes, the backup resources maybe shared with other connections on condition their working paths do not traverse common links.

The spare capacity usage factor is therefore used to denote the probability that connection R can use the resources of P to recover from the failure of A. This probability is determined by the probability that the other connections sharing backup resources with R, will not fail before the failure of R occurs. The value of θ is inversely proportional to the number of connections sharing the backup resources with R. In the multiple failure cases, the greater the number of connections sharing backup resources, the higher the probability that the resources will be utilized by one of them. Here, the study considers single link failures; only one connection may fail at any time resulting in θ having a value of l.

e. Availability of a Partial Link Disjoint Path Pair:

Figure 5 gives an example of a partial link disjoint path pair. The example shows that the connection comprises three sub-paths, i.e. 1-2. 3-4 and 2-5-3. Sub-paths 1-2 and 3-4 include fibres that share protection and working links. The remaining sub-path 2-5-3.which is link disjoint consists of a working path 2-3, and protection path 2-5-3. Therefore consistent with their definitions, in this example s_1 consists of links l-2 and 3-4, and s_2 consists of links 2-3,2-5 and 5-3. Furthermore, k=1, since there is only one sub-path which is link disjoint.

The calculation for the availability of a partial link disjoint path is given by developed in the following equations:

$$a_{LDP} = a_{S1} \, a_{S2} \quad (3)$$

$$a_{s1} = \prod_{ij \, \varepsilon \, S_1} a_{ij} \quad (4)$$

$$= a_{12} \, a_{34}$$

$$a_{S2} = \prod_{LDP_k \, \varepsilon \, S_2} a_{LDPk} \quad (5)$$

$$a_{LDPk} = 1-(1-\prod_{ij \, \varepsilon w_{pk}} a_{ij})(1-\prod_{ij \, \varepsilon pp_k} a_{ij})$$

$$= a_{23} + a_{25} \, a_{53} - a_{23} \, a_{25} \, a_{53}$$

f. Routing and Cost Analysis:

A routing algorithm is used to establish an appropriate path from a source to a destination. There are two main objectives of network routing. One is to maximize network throughput by providing as many connections as possible. The other is to minimize the cost of these paths, by providing least cost paths.

Both CSP and RASP employ the concept of shared-backup path protection where, in order to protect WPS from single link failures and make efficient use of resources, the protection wavelengths may be shared by different PPs only if their respective WPs are link disjoint. Lightpaths are established and taken down dynamically using the traffic model. Dijkstra's least cost routing algorithm is used to search the network to discover possible working and protection paths to satisfy requests. Dijkstra's algorithm uses information provided by the arrival request, r, such as the source node, s, and destination node, d, as well as additional information about the current network state provided by λ_w and λ_P. In order to find a least cost path. A_N is required to

compute the cost of each link. When a connection request arrives, both CSP and RASP respond by searching for a suitable working path. The cost of each link is first computed using Eq. 10:

$$c_i \begin{cases} +\infty & \text{,if } SW_{ij} = 0 \\ -\ln a_{ij} & \text{,otherwise} \end{cases} \quad (10)$$

As mentioned, each link is assumed to have a capacity of eight wavelength channels. SW_{ij} represents the number of free wavelengths present on link ij and is equal to zero when all eight wavelengths are being utilized. A link cost of infinity excludes a particular link from the search for a route. Eq. 10 results in a link having a high cost when its availability is low and vice versa. When Dijkstra's algorithm is unable to find a suitable working path.due to the lack of resources, the connection is blocked.

Satisfying a connection request may also involve finding a suitable backup path. RASP, being a reliability aware algorithm, is able to establish a working path without protection if the availability of the working path is greater or equal to the availability requirement of the connection. CSP does not consider reliability requirements and compensates by routing every connection with a link disjoint protection path. RASP allows partial link disjoint protection which improves the probability of finding a protection path (PP). When a backup protection path is required, the cost of each link is computed using Eq. 11:

$$c_{ij} = \begin{cases} -\ln \xi a_{ij} & \text{,if } ij \in WP \\ -\ln a_{ij} & \text{,if } SW_{ij \notin WP} \neq 0, \\ +\infty & \text{,if } SW_{ij \notin WP} = 0, \end{cases} \quad (11)$$

The main difference between Eq. 10 and Eq. 11 is that consideration is given to whether a specific link has been used in the working path of the connection. A link disjoint parameter, ξ, is introduced which is defined between 0 and 1. ξ is used to determine how disjoint the resulting protection path is. CSP uses a value of zero for ξ resulting in a cost of ∞, when $ij \in WP$. This excludes all working path links from the search, resulting in fully link disjoint protection paths. RASP uses a non-zero value for ξ which results in a higher cost for all $ij \in WP$ but does not exclude it from the search for a protection path. RASP assumes a value of 0.01 for ξ and will attempt to find a disjoint path but if one is not possible will attempt to find a path that is partially disjoint by utilizing protection bandwidth on one or more of the working path links.

In this way, the use of ξ does not allow RASP to favour a non-disjoint or partially disjoint path, but permits one should there be no alternative. ξ, therefore increases the probability of finding a suitable PP for a WP that is unreliable. Once a possible backup path is found, RASP will again calculate the availability of the path pair to ensure that it meets the availability requirement of the connection before being established. In the case of CSP, the path pair is established immediately, without any verification of reliability.

g. Proposed Algorithms for Shared path Protection

1 General process followed by CSP and RASP Pseudocode:

```
Start;
Initialize Network parameters and load traffic matrix;
Label l1:
Receive request;
Arrival or termination?;
If termination
{
Terminate request;
}
If Arrival
{
Provision request if possible;
End of traffic?;
If No
{
Goto Label l1;
}
If Yes
{
Calculate performance parameters;
}
}
End;
```

2 RASP Arrival request pseudocode:

```
Start;
Adjust cost matrix for WP calculation;
Find WP(Dijkstra);
Fail to find WP?;
If Yes
{
Block request and record block type;
End;
}
If No
```

```
{
Calculate availability of WP(Awp);
Awp>Areq ?;
If Yes
{
Wavelength assignment and update WP links;
End;
}
If No
{
Adjust cost matrix for PP calculation;
Find PP(Dijkstra);
Fail to find PP?;
If Yes
{
Block request and record block type;
End;
}
If No
{
Calculate availability of WP/PP pair(App);
App <Areq ?;
If Yes
{
Block request and record block type;
End;
}
If No
{
Wavelength assignment and update WP links;
Wavelength assignment and update PP links;
}
}
}
}
End;
```

3 CSP connection arrival procedure Pseudocode:

```
Start;
Adjust cost matrix for WP calculation;
Find WP(Dijkstra);
Fail to find WP;
If Yes
{
Block request and record block type;
End;
}
If No
{
Adjust cost matrix for PP calculation;
Find PP(Dijkstra);
Fail to find PP;
If Yes
{
Block request and record block type;
End;
}
If No
{
Wavelength assignment and update WP links;
Wavelength assignment and update PP links;
}
}
End;
```

4 RASP connection termination procedure Pseudocode:

```
Start;
Does request have a PP;
If Yes
{
Find WP and PP;
Remove WP and PP wavelengths and update link status;
End;
}
If No
{
Find WP;
Remove WP wavelengths and update link status;
End;
}
```

5. CSP connection termination procedure Pseudocode:

```
Start;
Find WP and PP;
Remove WP and PP wavelengths and update link status;
End;
```

IV. IMPLEMENTATION

SONET is a TDM system with 125μs time slot, and the delay of a SONET path is proportional to the path length. Thus, the path with the shortest length achieves the least delay. In other words, here program aims to find the shortest path for protection path.

When the link stateinformation is stale, the working path or the protection path may not be really feasible, forone or

more links on the paths may have available bandwidth. Figure 6 shows the shortest path. Here, values are pre-inserted in the program to tell how shortest path concept works.Two different network architecturesare made through program in which we have to find out the shortest path from Node1 to Node6, based on path cost values. The program calculates the shortest path based on shortest path cost values.

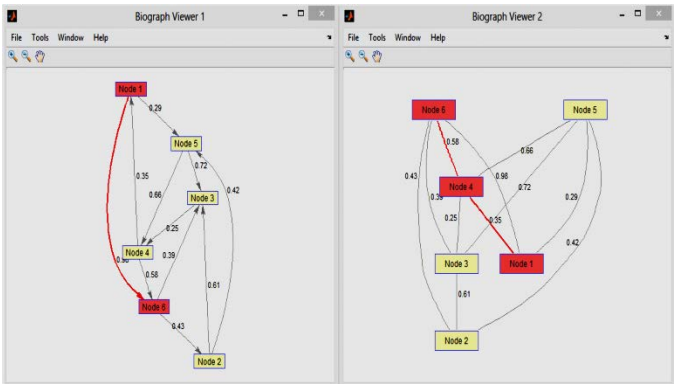

Figure 6: Shortest Path Algorithm

Here Figure 7, using the successional algorithm, which uses bellman ford algorithm, program finds the shortest path in multi-node network. Before, going for shared path protection, we need to find the shortest from each of the nodes present in the network. Find the shortest path from source to target in the cropped network topology by Bellman-Ford algorithm. The selected shortest path can guarantee the shortest delay. The successional algorithm terminates when it finds the two paths (working path and protection path) and successfully reserves bandwidth requirement along them.

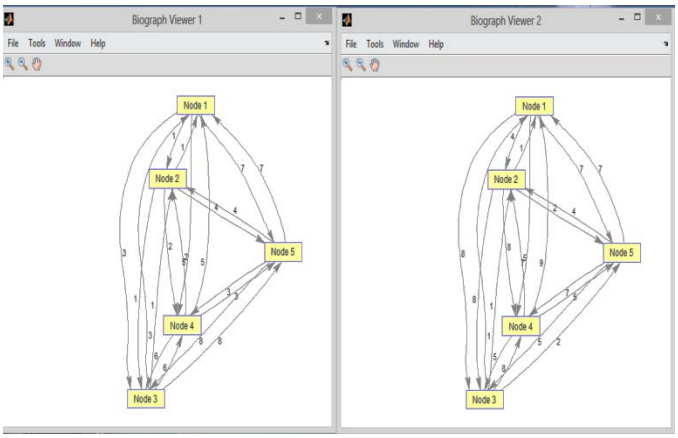

Figure 7: Bellman Ford Algorithm

Figure 8, makes user entered network architecture consists of various nodes. The aim of the program is to form a protected shared path of the network. A routing algorithm is used to establish an appropriate path from a source to a destination.There are two main objectives of network routing. One is to maximize network throughput byproviding as many connections as possible. The other is to minimize the cost of these paths,by providing least cost paths.Both CSP and RASP has been employed for shared-backup path protection.

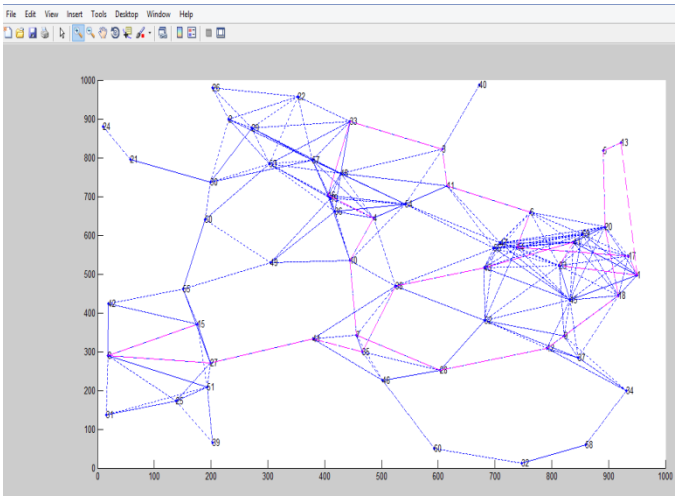

Figure 8: CSP and RASP

Satisfying a connection request may also involve finding a suitable backup path. RASP,being a reliability aware algorithm, is able to establish a working path without protection ifthe availability of the working path is greater or equal to the availability requirement of theconnection. CSP does not consider reliability requirements and compensates by routing everyconnection with a link disjoint protection path. RASP allows partial link disjoint protectionwhich improves the probability of finding a protection path (PP).

There are six graphs (Figure 9 to Figure 14) output by the program. This program aims for the performance evaluation of the shared path protection algorithm.

The number of requests rejected is an important parameter that has to be evaluated. So, probability of blocking vs Traffic intensity is plotted using some standard values, for network architecture of various nodes

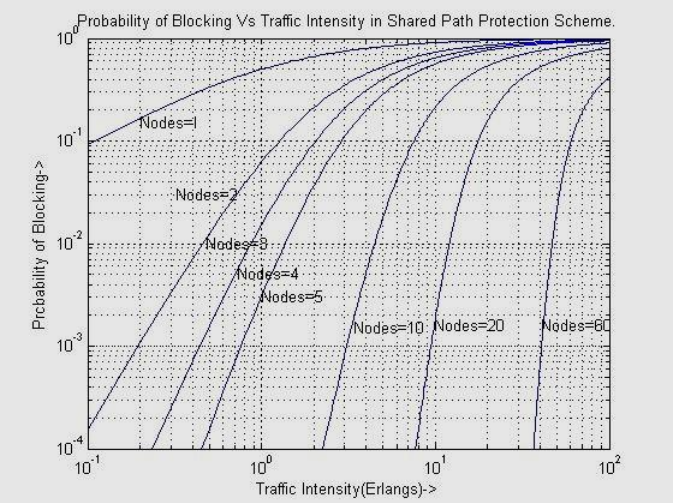

Figure 9: Blocking Probability Vs. Traffic Intensity

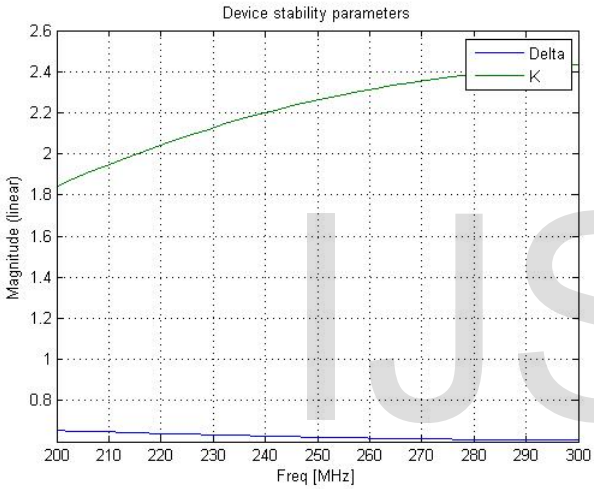

Figure 10: Magnitude vs. Frequency

Since, the algorithms are actually implemented on nodes which are actually electronic systems. We should consider the effect on nodes too. So, multiple graphs has been plotted taking in consideration the Centre frequency (Hz), Transducer gain target (dB), Max noise figure target (dB)Source impedance (Ohm), Reference impedance (Ohm), Load impedance (Ohm), Lower band edge,Upper band edge, Frequency (radians/sec). This also Analyzethe unmatched amplifier.

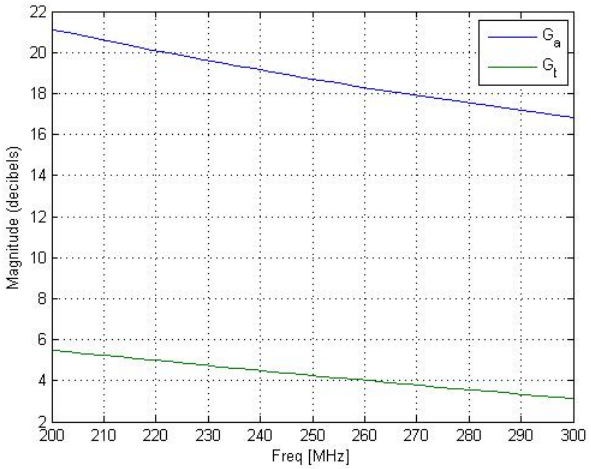

Figure 11: Magnitude vs. Frequency

Two graphs has been plotted regarding the bandwidth utilization and throughput. The alpha factor is some value between 0 and 1, and it refers to the relative weight of a trail.

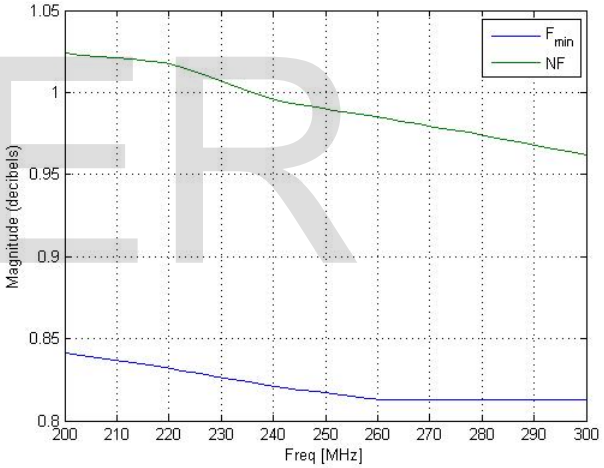

Figure 12: Magnitude vs. Frequency

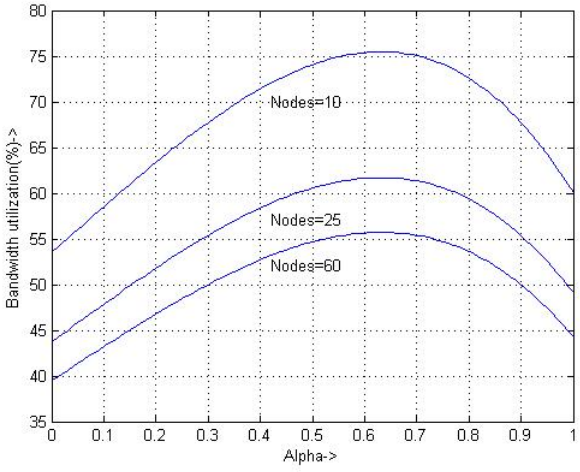

Figure 13: Bandwidth utilization Vs. Alpha

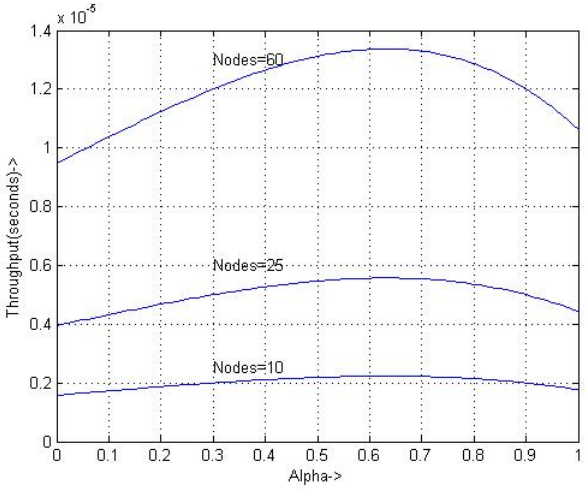

Figure 14: Throughput Vs. Alpha

Here, in each experiment, the following parameters are considered:
a) Weighted number of service requests accepted;
b) Number of service requests rejected;
c) Number of trails created;
d) Percentage of the total bandwidth consumed to satisfy theaccepted requests.

V. RESULTS

The performance of the described algorithms is evaluated, and the results obtained using Matlab are provided in this section. The comparisons were performed on the following:

- Probability of blocking Vs Traffic Intensity
- Bandwidth Utilization Vs Alpha
- Throughput Vs Alpha

The service requests are randomly generated and the performance of the algorithms is evaluated by running little iteration, each with different sets of networks, which are simulated.
This is roughly the distribution of bandwidth requirements for services received by a well-knownnational service provider (VSNL).
The number of requests rejected is an important parameterthat has to be evaluated. However, since different service requestsare for different bandwidth rates, they cannot be treatedequally.

- *Computational Complexity:*

The computational complexity of Conventional Algorithm is, O (KV(V^2+(E+V)logV)) where V is the number of network nodes, E is the number of edges, and K is the number of distinct paths. The complexity of the proposed algorithm is isO(KV(E+V)logV).

- Comparison between Probability of blocking Vs Traffic Intensity:

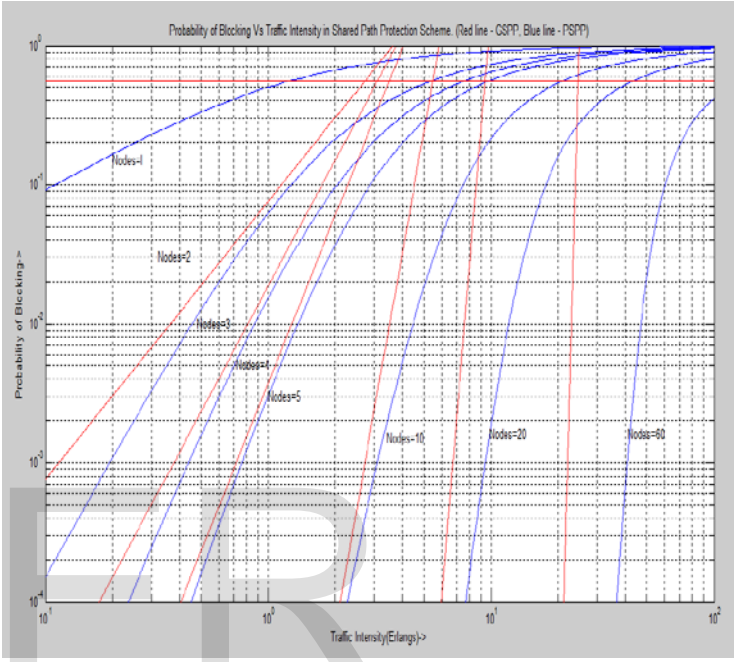

Figure 15: Blocking Probability vs. Traffic Intensity

In figure 15 there is a comparative study between the existing algorithms Vs. proposed algorithm. At different nodes a blocking probability Vs Traffic intensity.

- *Comparison between Bandwidth Utilization Vs Alpha:*

In figure 16 there is a factor which is important i.e. Bandwidth vs. Alpha. This is also improved by the proposed algorithm shown in Section IV. Figure 16 shows comparative view of proposed vs. existing algorithm.

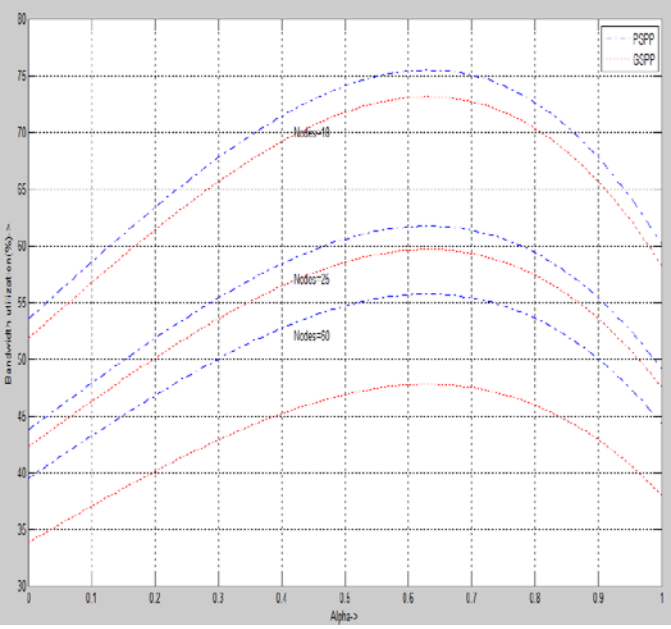

Figure 16: Throughput Vs. Alpha

Making comparisons between GSPP Algorithm and PSPP Algorithm performance, using some standard values, in blocking probability, throughput and bandwidth utilization; it is clearly observed that PSPP Algorithm is better than GSPP Algorithm in all performance criteria.

VI. Conclusion

In this paper we have implemented and proposed the new algorithms for shared path protection. In this paper we have proposed the criteria for the evolution and optimization of the bandwidth oriented structure. The proposed algorithms are providing better throughput, blocking probability and optimization of bandwidth than other existing algorithms.Blocking probability is 0.2 for 10 nodes 10 Er traffic and 0.3 for 60 nodes 10 Er traffic. Bandwidth Utilization is 75% for 10 nodes and 55% for 60 nodes at full load condition. Throughput is 1.4 x 10^{-5}Secs for 60 nodes and 0.6 x 10^{-5}Secs for 25 nodes.

REFERENCES

[1] Satish M B, Savitha C, Dr. M Z Kurian, "Implementation of ATM Packets Over MPLS Network on FPGA" *International Journal of Computer & Organization Trends* ,Vol. 3 Issue 5, June, 2013.

[2] RohithRamkumar, H.A.Chan, "VCAT Differential Delay Minimization for Delay Sensitive Multiservice Networks", 2006.

[3] Joji Philip, Sailesh Kumar, Sunil Shukla, Raja Venkatesh,, "Architecture for Flow Control and Input Buffering on High Speed Interfaces"*Paxonet Communications*, CA, USA, 2007

[4] Jin Y. Yen, "Finding the K Shortest Loopless Paths in a Network", *Management Science*, Vol. 17, No. 11, Theory Series (Jul., 1971), pp. 712-716.

[5] Yuchun Guo1, Fernando Kuipers2 and Piet Van Mieghem, Link-disjoint paths for reliable QoS routing ,*INTERNATIONAL JOURNAL OF COMMUNICATION SYSTEMS,* Int. J. Commun. Syst. 2003; 16:779–798 (DOI: 10.1002/dac.612)

[6] Bill Lin, Gjalt de Jong, Carl Verdonck, Sven Wuytack, FranckyCatthoor, "Background Memory Management for Dynamic Data Structure Intensive Processing Systems" IMEC, 1996.

[7] KeyanZhu Jing Zhang and Biswanath Mukherjee, "Inverse Multiplexing in Optical Transport Networks with the Support of SONET/SDHVirtual Concatenation", IEEE, 2004.

[8] Kuan Chou Loh, "SIMULATION AND PERFORMANCE ANALYSIS OF ROUTING IN SONET/SDH", *DATA COMMUNICATIONS NETWORK (DCN)*,IEEE. Dec. 2006

[9] Kuan Chou Loh, "Understanding Virtual Concatenation and Link Capacity Adjustment Scheme in SONET/SDH" ,Thesis NAVALPOSTGRADUATESCHOOLMONTEREY, CALIFORNIA ISSN, 2012.

[10] MadanagopalRamachandran, N. Usha Rani,and Timothy A. Gonsalves, "Path Computation Algorithms for Dynamic Service Provisioning With Protection and InverseMultiplexing in SDH/SONET Networks", IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 18, NO. 5, OCTOBER 2010

[11] "Types and characteristics of SDH network protection architectures,"ITU-T, Recommendation G.841, 1998.

[12] A. E. Ozdaglar and D. P. Bertsekas, "Routing and wavelength assignmentin optical networks," *IEEE/ACM Trans. Netw.*, vol. 11, no. 2, pp.259–272, Apr. 2003.

[13] H. Zang, C. S. Ou, and B. Mukherjee, "Path-protection routing andwavelength assignment (RWA) in WDM mesh networks under ductlayerconstraints,"

IEEE/ACMTrans. Netw., vol. 11, no. 2, pp. 248–258,Apr. 2003.

[14] X. Chu, B. Li, and Z. Zhang, "A dynamic RWA algorithm in a wavelength-routed all-optical network withwavelength converters," in *Proc.IEEE INFOCOM*, Apr. 2003, pp. 1795–1804.

[15] M. Alanyali and E. Ayanoglu, "Provisioning algorithms for WDM opticalnetworks," *IEEE/ACM Trans. Netw.*, vol. 7, no. 5, pp. 767–778,Oct. 1999.

[16] S. Janardhanan, A. Mahanti, D. Saha, and S. K. Sadhukhan, "A routingand wavelength assignment (RWA) technique to minimize the numberof SONET ADMs inWDM rings," in *Proc. 39th HICSS*, Jan. 2006, pp.1–10.

[17] G. Shen and W. D. Grover, "Performance of protected working capacityenvelopes based on p-cycles: Fast, simple, and scalable dynamicservice provisioning of survivable services," *Proc. SPIE*, vol. 5626, pp.519–533, Feb. 2005.

[18] M. Kodialam and T. V. Lakshman, "Dynamic routing of bandwidthguaranteed tunnels with restoration," in *Proc. IEEE INFOCOM*, Mar.2000, pp. 902–911.

[19] J. Q. Hu, "Diverse routing in optical mesh networks," *IEEE Trans.Commun.*, vol. 51, no. 3, pp. 489–494, Mar. 2003.

[20] A. Todimala and B. Ramamurthy, "IMSH: An iterative heuristic forSRLG diverse routing inWDMmesh networks," in *Proc. 13th ICCCN*,Oct. 2004, pp. 199–204.

[21] A. Todimala and B. Ramamurthy, "A heuristic with bounded guaranteedto compute diverse paths under shared protection in WDM meshnetworks," in *Proc. IEEE GLOBECOM*, Nov. 2005, pp. 1915–1919.

. Deepak Dhadwal ,currently pursuing PhD from manav rachna international university.9818161442 Email:deepakdhadwal.007@gmail.com

. Ashok Arora ,currently working as executive dean in manav rachna international university,Email:ashok.mriu@gmail.com

. VR Singh currentlyworking as Director at Prabhu dayal memorial school of technology and management.Bahadurgarh