

Mechanism for handling- Multi link failure in SLICE

Rakesh Praneeth Konduru, Niharika Deekonda, Prakash Chourasia
Department Of Computer Science
Georgia State University

I. PROBLEM STATEMENT

IN optical networks, link failure may cause huge loss in terms of throughput. The word Survivability in networks refer to the capability to maintain an adequate level of service even in case of a failure in the network. There can be two approaches that solve link failures in networks Protection and Restoration. Protection plans the backup path/routes well in advance that can be used in case of failures. Restoration solves failures by locating free wavelength channels for backup after a failure occurs [5].

The shared-path protection (SPP) algorithm is been proposed as a solution on foundation of Protection schemes, but it did not consider the load balancing when computing the paths. Also it is useful and effective for single-link failure only. Through our research we came to know that for multi-link failures, SPP algorithm cannot recover efficiently, especially when the primary path and backup path both fail simultaneously.

Tremendous research has been done in networks to solve the problems of both single and multi-link failures. Restoration schemes are very efficient with respect to capacity requirements and because it can dynamically choose the backup path after a failure and offers better multiple failure survivability.

In this paper we are proposing a new solution for multi-link failure which is considering the dynamic load balancing and computing the backup paths in advance and thus providing the protection scheme for multi-link failure for which SPP was not so efficient. And we came to conclusion that in case of a link failure in SLICE networks, multi-link failure recovery mechanisms work better as compared to single-link failure recovery methods.

II. INTRODUCTION

We discussed about the criticality of sending data across networks in a consistent and scalable manner. Due to the increase in the immense amount of data traffic volume, there are high chances for link failures

to take place. To overcome these failures, a number of single-link-failure recovery methods have been proposed [1]. These methods can handle failures in only single links. Hence, we extended our research to study recovery methods in multiple-links too.

Tremendous research has been done in this area out of which two different strategies, named enhanced shared-path protection (ESPP) algorithm and self-organizing shared-path protection (SSPP) algorithm, have been proposed and they have considered different load balancing schemes in WDM networks.

However WDM does not provide flexible bandwidth, so while traffic self-adaptive restoration effective use of bandwidth is not possible in WDM. Therefore, the architecture of the spectrum-sliced elastic optical path network, named SLICE has been considered. And restoration scheme named bandwidth squeezed restoration (BSR) scheme is been used for fixing the link failure with limited bandwidth resources.

So far, we aim at available bandwidth sufficiency in the case of multi-link failures while we do not focus on the insufficiency of available bandwidth as backup path of the affected traffic. Therefore, in SLICE architecture, by introducing a conventional load balancing and a novel recovery algorithm for multi-link failures named dynamic load balancing shared-path protection (DLBSPP) algorithm is proposed.

To tolerate multi-link failures in SLICE, traffic self-adaptive restoration (TSAR) mechanism is adopted to restore the traffic affected by the failures. We are going to compare and research, the conventional SPP algorithm, DLBSPP algorithm in terms of lower blocking probability (BP), better spectrum utilization ratio (SUR) and higher failure restoration ratio (FRR). This report is made to provide a detailed understanding of the various link-failure-recovery methods and their actual working on a simulator.

III. LITERATURE REVIEW

Spectrum-sliced elastic optical path network (SLICE), is a spectrum-efficient and scalable optical transport

network architecture. This network architecture is designed to work efficiently with high volume data traffic by appropriately allocating network resources. The SLICE architecture provides a fractional bandwidth service by enabling the sub wavelength, super wavelength and multiple-rate data traffic accommodation. There are several other wavelength routed optical path networks that are currently being used, in which even though the traffic between an end node pair is less than the entire capacity of the wavelength, it still require full allocation of wavelength capacity to an optical path between the end-node pair. SCILE architecture alleviates the fixed-sized allocation of optical bandwidth issues of the current optical path networks.

SPECTRUM ASSIGNMENT IN SLICE

Figure 1 shows on how SLICE assigns the Spectrum to achieve its promise on providing fractional bandwidth service. From its ability to contract and expand in contrary to the existing rigid optical paths, stems the name elastic optical path of the optical paths in SLICE. Provided frequency slots of 100GB each assigned to an optical network, if only a fractional amount of bandwidth is requires, SLICE can allocate just enough optical bandwidth to accommodate the client traffic. Where as in conventional rigid networks the whole bandwidth is allocated no matter how much the client request is, due to which a lot of resources are wasted. This process of provisioning the fractional bandwidth service is achieved by enabling the creation of sub-wavelength optical path by Slicing down the bandwidth. Just like the link aggregation technology in packet networking, SLICE enables the creation super-wavelength optical path contagiously combined in optical domain. This feature in SLICE is called Layer one (L1) link aggregation, which can be realized by optical orthogonal frequency-division multiplexed (OFDM) SLICE transponders. Thus slice efficiently allocates the bandwidth to multiple data bit rates in the optical domain in contrast to the current rigid network architectures.

Protection and Restoration: In a wavelength-routed network, a connection between a source node and a destination node is called a lightpath. A lightpath is an optical channel that may span multiple fiber links to provide an all-optical connection between two nodes. In the absence of wavelength converters, a lightpath would occupy the same wavelength on all fiber links that it traverses. Two lightpath on a fiber link must be on different wavelength channels to prevent the interference of the optical signals. The failure of a network component such as a fiber link can lead to the failure of all the lightpaths that traverse the failed link. Since each lightpath is expected to operate at a rate of several gigabytes per second, a

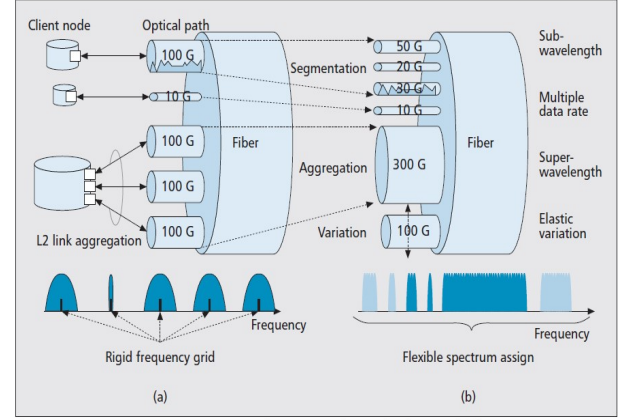


Figure 1. Spectrum assignment in SLICE: a) conventional optical path network; b) SLICE.

failure can lead to a severe data loss. Although higher protocol layers [such as asynchronous transfer mode (ATM) and Internet protocol (IP)] have recovery procedures to recover from link failures, the recovery time is still significantly large (on the order of seconds), whereas we expect that restoration times at the optical layer will be on the order of a few milliseconds to minimize data losses [2]. Furthermore, it is beneficial to consider restoration mechanisms in the optical layer for the following reasons [3]: 1) the optical layer can efficiently multiplex protection resources (such as spare wavelengths and fibers) among several higher layer network applications, and 2) Survivability at the optical layer provides protection to higher layer protocols that may not have built-in protection. There are several approaches to ensure fiber network survivability. Survivable network architectures are based either on dedicated resources or on dynamic restoration. In dedicated-resource protection, the network resources may be dedicated for each failure scenario, or the network resources may be shared among different failure scenarios. In dynamic restoration, the spare capacity available within the network is utilized for restoring services affected by a failure. Generally, dynamic restoration schemes are more efficient in utilizing capacity due to the multiplexing of the spare-capacity requirements and provide resilience against different kinds of failures, while dedicated-resource protection schemes have a faster restoration time and provide guarantees on the restoration ability.

This study examines different approaches (illustrated in the above figure) to survive link failures. These approaches are based on two basic survivability paradigms:

- 1) path protection/restoration
- 2) link protection/restoration
- **Path protection/restoration:**

In path protection, backup resources are reserved during connection setup, while in path restoration;

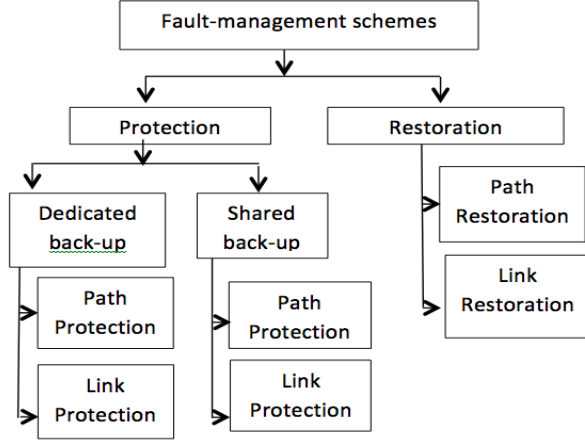


Fig. 1. Fault-Management Schemes

backup routes are discovered dynamically after the link failure. When a link fails [illustrated in Fig.2], the source node and the destination node of each connection that traverses the failed link are informed about the failure via messages from the nodes adjacent to the failed link, as illustrated in Fig.4.

– Dedicated-path protection:

In dedicated path-protection (also called 1:1 protection), the resources along a backup path are dedicated for only one connection and are not shared with the backup paths for other connections.

– Shared-path protection:

In shared-path protection, the resources along a backup path may be shared with other backup paths. As a result, backup channels are multiplexed among different failure scenarios (which are not expected to occur simultaneously), and therefore, shared-path protection is more capacity efficient when compared with dedicated-path protection.

– Path Restoration:

In path restoration, the source and destination nodes of each connection traversing the failed link participate in a distributed algorithm to dynamically discover an end-to-end backup route. If no routes are available for a broken connection, then the connection is dropped.

- **Link protection/restoration:** In link protection, backup resources are reserved around each link during connection setup, while in link restoration, the end nodes of the failed link dynamically discover a route around the link. In link protection/restoration [illustrated in Fig. 3], all the connections that traverse the failed link are rerouted around that

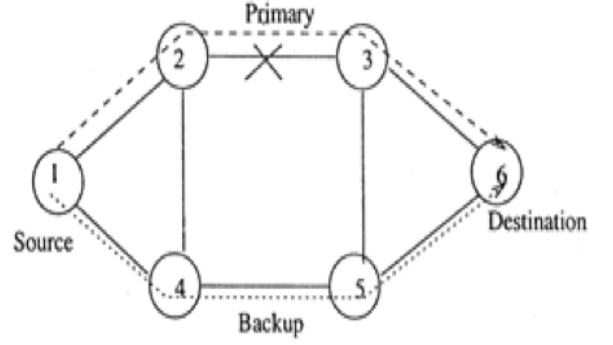


Fig. 2. Path Protection

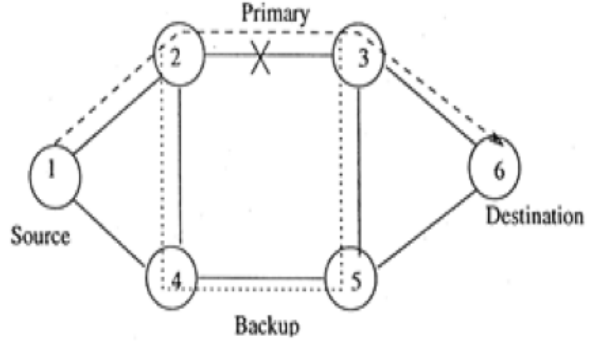


Fig. 3. Link Protection

link, and the source and destination nodes of the connections are oblivious to the link failure.

– Dedicated-link protection:

In dedicated-link protection, at the time of connection setup, for each link of the primary path, a backup path and wavelength are reserved around that link and are dedicated to that connection. In general, it may not be possible to allocate a dedicated backup path around each link of the primary connection and on the same wavelength as the primary path.

– Shared-link protection:

The back-up resources reserved along the back-up path may be shared with other back-up paths. As a result, backup channels are multiplexed along different failure scenarios.

IV. PREVIOUS WORK

Case of Single link Failure:

• BSR (Bandwidth Squeezed Restoration)

This is one of the commonly used methods, owing to its simplicity. In fixed-bandwidth optical networks,

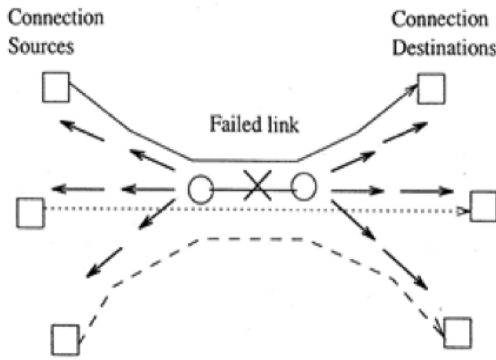


Fig. 4. Communicating failures via messages

failed optical path can be recovered only if the detour route has a bandwidth equal to or greater than the failed route. But in SLICE networks, failed path can be recovered even if the bandwidth is not greater than or equal to the failed path. The bandwidth of failed optical path is squeezed using elastic feature of SLICE in order to ensure minimum connectivity. This feature of manipulating the bandwidth based on the requirements is known as Bandwidth Squeezing, i.e. in this method, the bandwidth is squeezed/compressed based on the availability and used. The entire mechanism of BSR works on this principle. This is the BSR method.

Principle of BSR Method: In any traffic network, there are three kinds of traffic that is possible. Green traffic, yellow traffic and red traffic. Any traffic that can be easily transmitted even during a failure is known as the Green Traffic, i.e. there is a guarantee that this traffic can be transmitted. Any traffic that cannot be transmitted over the network in case of a network failure, no matter what, is known as the Red Traffic. Any traffic that is attempted to be transmitted as much as possible during a failure is called yellow traffic. There are no limits or constraints on yellow traffic. Based on different network capabilities, different amounts of yellow traffic are transmitted over the network. The aim of BSR is to transmit as much yellow traffic as possible during a network failure.

Using this BSR scheme of recovery, there are three possible patterns in which the data can be recovered[2] They are:

- FBPR (Full Bandwidth Guaranteed Recovery)
- PBGR (Partial Bandwidth Guaranteed Recovery)
- BER (Best-effort Recovery)

Depending on, the specified bandwidth allocation function and the best-effort bandwidth allocation function, the three patterns are determined. The first function, the specified bandwidth allocation

function determines the amount of bandwidth that the back up will use.

– **FBGR**(Full Bandwidth Guaranteed Recovery):

This was one of the first patterns that was discovered. This pattern allocates the same amount of recovery bandwidth as that of the working path bandwidth. FBGR is considered as a special case of PBGR as it uses a function according to which full bandwidth is recovered.

– **PBGR**(Partial Bandwidth Guaranteed Recovery):

Another one of the primitive or initial methods that was developed and used was the PBGR. In this method, only a partial amount of the total working bandwidth is allocated as the recovery/back-up bandwidth instead of all of the bandwidth. Unlike the previous method, since only certain amount of bandwidth is allocated here, the FBGR is considered to be a derivative to this method.

Both of the above methods work on the assumption that there are sufficient amount of back-up resources, if not for the entire bandwidth, then at least for the specified amount of bandwidth. Due to this, there is a need to reserve the backup resources before setting up the working paths. If a failure still takes place, and there is no sufficient amount of bandwidth that has been stored as a back-up resource, then the entire recovery method will fail.

– **BER** (Best-effort Recovery):

BER is a much-advanced mechanism that was developed later as compared to the previous two. In this method, bandwidth as a back-up resource is allocated based on the back-up path route and the available resources in that route. Hence, as long as the available bandwidth is sufficient enough for the working path, all the remaining bandwidth is allocated to the back-up resources as the back-up bandwidth. This process is implemented until the limit for the bandwidths is reached [2]. BSR is an effective process owing to its cost-effectiveness and high survivability as a restoration scheme in case of a network failure.

• **SPP (Shared Path Protection):**

Another another kind of recovery methods for overcoming single-link failures in connection-oriented networks is the Shared Path Protection. Though the functionality of this mechanism is similar to that of dedicated protection, the SPP has higher efficiency as it has better network utilization capacity. In shared path protection, multiple protection (back-up) paths can be established

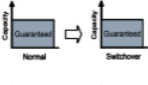

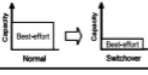
Recovery behavior		Function	
		Specified bandwidth allocation	Best-effort bandwidth allocation
Full bandwidth guaranteed recovery		Yes	No
Partial bandwidth guaranteed recovery		Yes	No
Best-effort recovery		No	Yes

Fig. 5. Recovery Behaviors For Various Service classes[2]

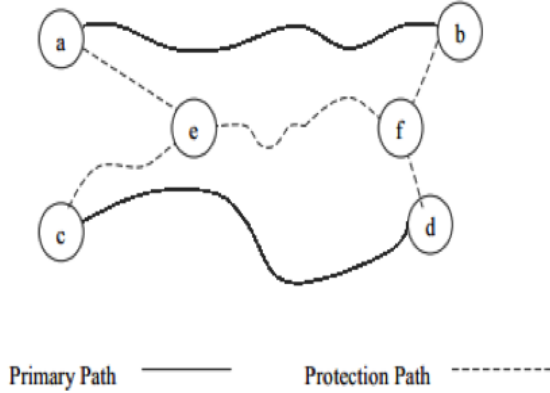


Fig. 6. Shared Path Protection[2]

which share the same resources. Hence, the necessity for separate resources for separate paths is not present for this recovery path.

In the diagram, it can be seen that, ab and cd are the primary paths while using nodes e and f, shared paths have been established between the nodes a and b; and c and d.

By using this technique, decent amount of protection can be provided for the network with the minimal number of resources available. Hence, the network utilization can be increased. This is one head-down advantage that the shared path protection has, over the dedicated path protection. This has led to increased popularity of this mechanism and its increased usage in the all-optical DWDM networks.

Though SPP has higher efficiency compared to the dedicated path protection methods, it has defects of its own. When using shared paths as back-up paths for the network, it has to be kept in mind that, when a shared back-up path is chosen as a recovery path for a certain

pair of nodes, the other set of node which use this same path for recovery cannot use this any longer and will have to re-route through a different path. If alternates are available, then this issue can be taken care of, but, otherwise, this can be a real problem. Also, since more than one primary paths have the same recovery paths, if, by any chance, the shared recovery path fails, then both those primary paths will have to look for a different path and re-route their data.

Though all the above-discussed methods prove their efficiency in single-link failures, when it comes to multi-link failure recovery methods, they have their own setbacks. Issues like blocking probability, spectrum utilization ratio and failure restoration ratio are better addressed using multi-link failure-recovery methods (DLBSPP), than by using these single-link failure recovery methods.

Case of Multi-link Failures:

Shared-path protection was one of the algorithms that are proposed in case of single link failure, but it failed to consider the load balancing while calculating the paths. Also, shared-path protection algorithm cannot efficiently recover when both working and backup path fail simultaneously. Then to confirm highly survivable and spectrally efficient bandwidth, a new restoration scheme was proposed, Bandwidth squeezed restoration (BSR). This algorithm or scheme ensures that the best effort is recovered even when the available bandwidth resources are not sufficient in the course of failure recovery. So, we would like to extend this topic and discuss more in case of multi-link failures too i.e. failing of both working and backup path simultaneously. However, the SPP algorithm that is proposed in case of single link failures does not recover efficiently in case of multi-link failures. A new recovery algorithm is proposed for multi link failures to restore traffic efficiently named Dynamic Load Balancing Shared Path Protection (DLBSPP). This algorithm uses the main idea of dynamical load balancing, spectrum resources sharing of backup path and traffic self-adaptive restoration (TSAR) mechanism [6].

V. PROPOSED WORK

DLBSPP Algorithm:

This algorithm was proposed to compute the working or primary path and the link-disjoint shared backup path. To search and allocate the available spectrum resources this DLBSPP algorithm has employed First Fit (FF) and Random Fit schemes (RF). The First Fit

scheme searches for the available spectrum resources and considers the lower numbered resource over the higher numbered resource and allocates the first available one. Whereas, the Random Fit scheme searches the space of the spectrum resources to determine the set of available resources on the particular route. Among those available resources, any one is chosen randomly. This is how both these schemes work to assign a spectrum resource to any link.

Inputs:

The SLICE architecture is explained as a graph G with a set of nodes, links/edges and available bandwidth slots. It can be denoted as,

$G(V, L, F)$

Where, $V = \{v_1, v_2, v_3, \dots, v_n\}$ set of nodes which are set with bandwidth-variable optical cross-connects (BV-OXCs) function.

$L = \{l_1, l_2, l_3, \dots, l_n\}$ set of links or edges.

$F = \{\omega_1, \omega_2, \omega_3, \dots, \omega_n\}$ set of available frequency or bandwidth slots.

For every connection request between source and destination, a bandwidth is required and the same number of frequency slots is assigned to both working path and backup path.

Constraints:

Following are the constraints that any shared path looks for when assigning a frequency slot resource:

Spectral Continuity constraint: According to this constraint, the same spectral resource should be allocated in all the links along the path it traverses.

Spectral Consecutiveness constraint: According to this constraint, on each link an allocated spectrum must be chosen from contiguous frequency slots in the frequency domain.

Consider, there are 6 frequency slots on each edge or link in the above diagram used for illustration of spectral continuity constraint and spectral consecutiveness constraint. The numbers mentioned on each link represent the frequency slots that are free or available. Considering each connection request requires three frequency slots to traverse from source to destination. The first $CR1(A,D,3)$ have to choose the shortest distance from source A to destination D as primary path using three frequency slots. So, it chooses the shortest route A-B-C-D as working path and a set of common frequency slots (3,4,5) are used on every link along this path as reserved spectrum resources. Since the three frequency slots (3,4,5) on each link A-B, B-C and C-D are not only all the same spectrum but also contiguous frequency domain. Therefore, this proves that $CR1(A,D,3)$ successfully establishes connection

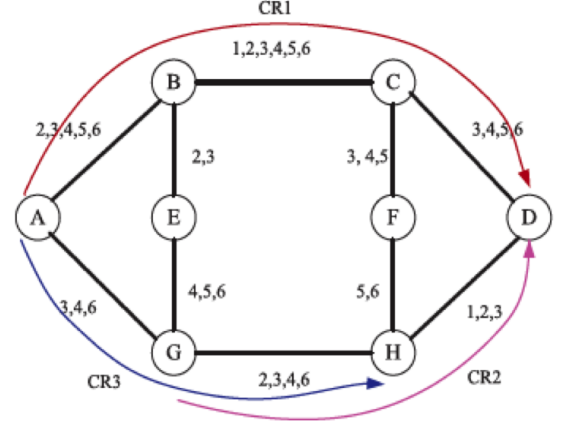


Fig. 7. Illustration of Spectral continuity and consecutiveness constraints[9]

satisfying both the spectral continuity constraint and spectral consecutiveness constraint. Let us now check the same for other connection requests if they are satisfying both these constraints. The second $CR2(G,D,3)$ has to traverse from Source G to destination D using the shortest path and three frequency slots. It chooses the shortest path G-H-D as the working path, and the frequency slots (2,3,4) and (1,2,3) that correspond to links G-H and H-D respectively are used for the reserved spectrum resources. This connection request cannot be routed successfully though the path G-H-D since they are not using the same spectrum along this path and the frequency slots, which are used also, are not consecutive. So, this request failed to satisfy both the spectral continuity constraint and spectral consecutiveness constraint. The third $CR3(A,H,3)$ has to traverse from Source A to destination H using the shortest path and three frequency slots. It chooses the shortest path A-G-H as the working path, and frequency slots (3,4,6) on links A-G and G-H are used for the reserved spectrum resources. This connection request cannot be established successfully since the used frequency slots are not continuous which fails the spectral consecutive constraint. So, while assigning the frequency slots always these two constraints should be satisfied.

To compute the routes:

Dijkstras algorithm is used to compute the paths from a given source to destination. And, the reservation of spectrum resources considers the two constraints that are described while assigning the bandwidth slot resource.

Dynamic load balancing:

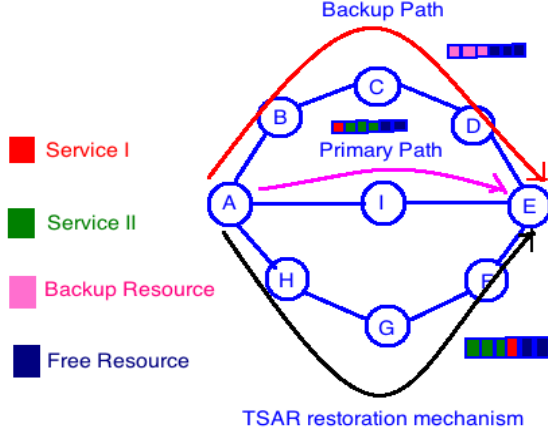


Fig. 9. TSAR restoration mechanism

for primary path, the first frequency slot is reserved for backup spectrum resource. Next, Service II also selects the shortest path A-I-E as its primary path and reserves second, third, fourth frequency slots as the spectrum resources. Since it can share the resources, for the backup path A-B-C-D-E Service II reserves first, second and third frequency slots as the backup spectrum resources. The color-coding pink resembles the backup resources in the diagram.

When the Links from I to E and D to E interject simultaneously, using the SPP algorithm these connection requests will be dropped. However, if the DLBSPP algorithm using TSAR mechanism is implemented then it calculates the new recovery route from A to E, A-H-G-F-E. According to TSAR mechanism, first the dense granularity is recovered so in this case Service II is recovered reserving the first, second, third frequency slots as spectrum resources. And then the Service I also selects the same recovery route A-H-G-F-E and the fourth frequency slot is reserved as the spectrum resource. This way the multi-link failures are recovered efficiently using the DLBSPP algorithm with TSAR mechanism.

VI. SIMULATION

Network Simulation is a technique where a program is used to model the behavior of a network. This can be done either by calculating the interaction between the different network entities using mathematical formulas, or actually capturing and playing back observations from a production network. The reason behind performing simulation is to evaluate the performance of a network.

To perform network simulation on any network, network simulators have to be used. Using programming languages we can do these. Few of the most popular

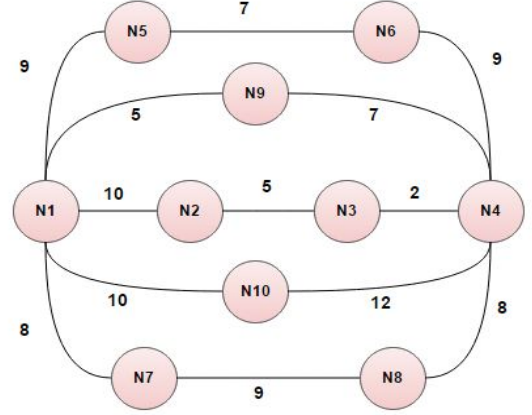


Fig. 10. Network we considered for simulation

languages that are used for network simulation are C, C++ and JAVA. Since establishing a real network every time its performance has to be evaluated, simulation is used. A network simulator is a software that can be used to study the behavior of a network without the actual presence of the network. By using these simulators, the performance of the network(s) can be analyzed. Using simulation in networks is a very common method used by even scientists to perform research work and analyze the various networks.

We adopted the below network with 10 nodes and 13 links to compare the conventional SPP algorithm and DLBSPP algorithm in case of multi link failures. With our simulation we prove that the throughput is high in DLBSPP algorithm compared to SPP algorithm. We assumed that bandwidth (or frequency slots) is sufficient at all links in our network in case of multi-link failures. We simulated our network in JAVA and to find the shortest path we used Dijkstras algorithm. The number of frequency slot is evenly distributed for each connection request traversing from source to destination. And the reserved spectrum resource for each connection request must satisfy both spectral continuity constraint and spectral consecutiveness constraint. Frequency slots are assigned based on the First Fit and Random Fit schemes in the pair of primary path and link disjoint shared backup path. By analyzing multiple scenarios of link failures in the network we will show the performance of both SPP and DLBSPP algorithm. There are three cases that we considered.

Case 1: Choosing the Primary Path

In our network, after performing Dijkstras algorithm the shortest route from source A to destination D is A-I-D. So, this route is considered as the primary or working

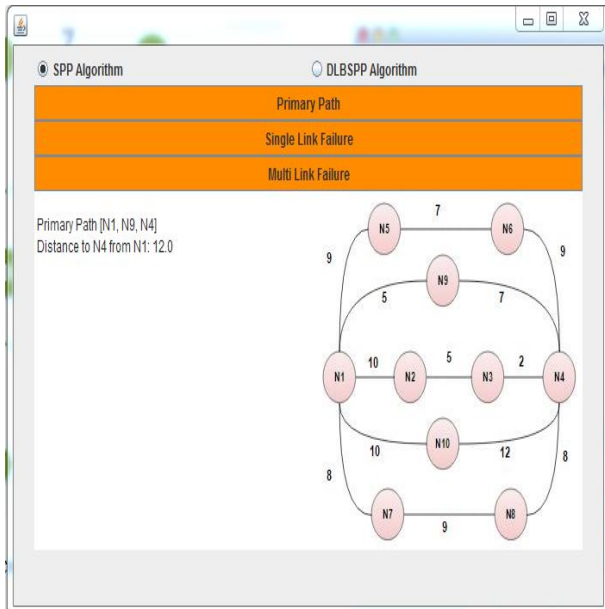


Fig. 11. Primary Path in SPP algorithm

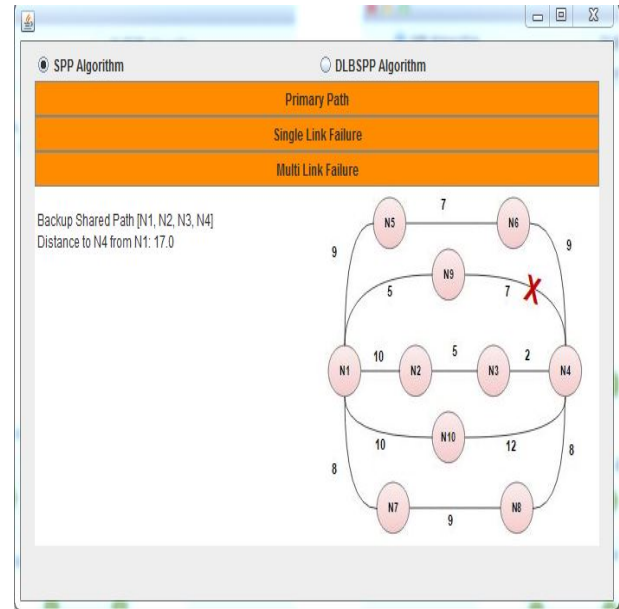


Fig. 13. Shared backup Path chosen when a link in primary path fails in SPP algorithm

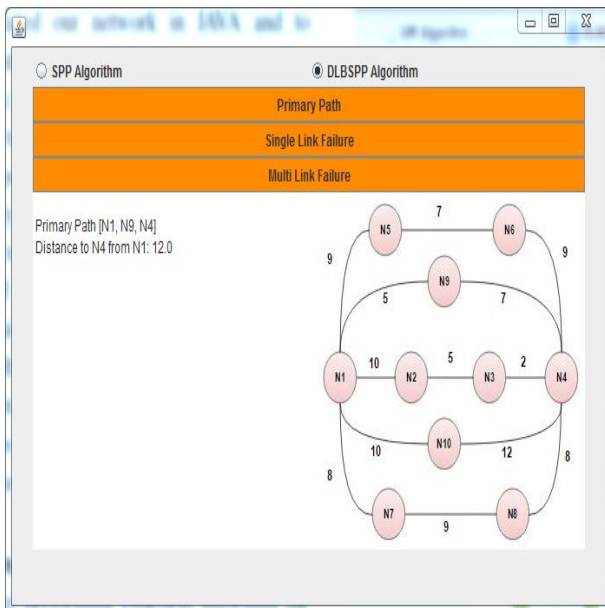


Fig. 12. Primary Path in DLBSPP algorithm

path. Both SPP and DLBSPP use this algorithm to find the shortest path as the primary path from source to destination. Figures 11 and 12 show the primary path in case of both SPP and DLBSPP algorithm.

The red color path in the screen shots indicates that it is the primary or working path from source A to destination D.

Case 2: When a link in Primary Path fails

We now see how the conventional SPP algorithm and DLBSPP algorithm work in case the primary path A-I-D

fail. Considering the failure in the link from I to D, both the SPP and DLBSPP search for the backup shared path from where the same connection request can be routed without loss of data. This backup shared path from same source to same destination is the link disjoint path to the primary path and is again found using the Dijkstras algorithm. In the network that we considered, A-B-C-D is the next shortest path and this is link disjoint to the primary path A-I-D. So, this route is taken as the shared backup path in case of both conventional SPP algorithm and DLBSPP algorithm. Below are the screen shots how they route using the backup shared path from A to D via the route A-B-C-D.

The X on the link indicates the link failure and the route cannot be made successfully anymore on that way. The red color path indicates that it is now considered as the primary path from source A to destination D.

Case 3: When links in both the primary and shared backup path fail

Using Dijkstras algorithm, the next shortest path from source A to destination D is obtained. In the network that we considered, A-J-D is the next shortest path. So, when both the primary path and shared backup path have link failures, the conventional SPP algorithm fails to send the connection request and it drops. There is loss of data in SPP algorithm. But, when we consider the DLBSPP algorithm, it searches for the next shortest route and sends the data instead of dropping the request.

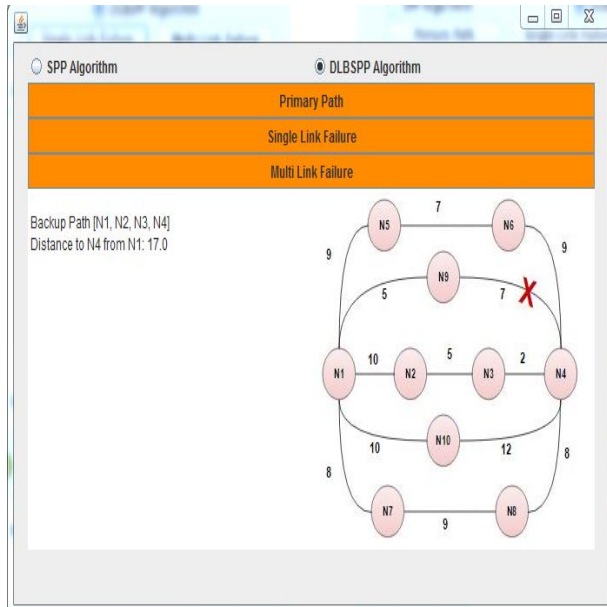


Fig. 14. Shared backup Path chosen when a link in primary path fails in DLBSPP algorithm

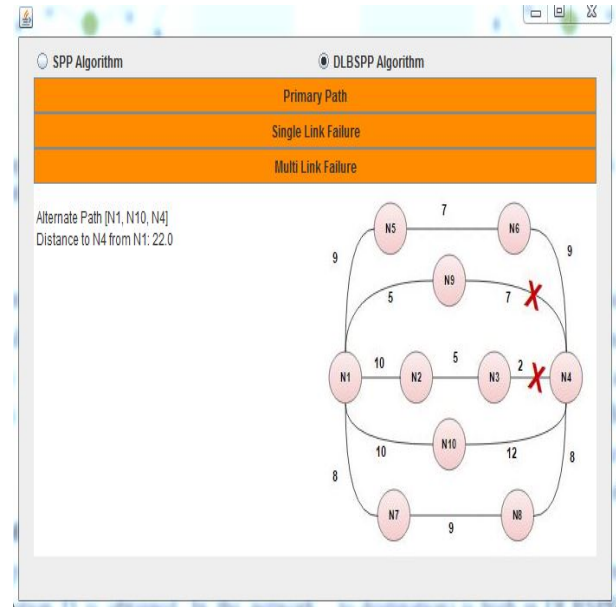


Fig. 16. Alternate Path chosen when link in both primary and shared backup path fail in DLBSPP algorithm

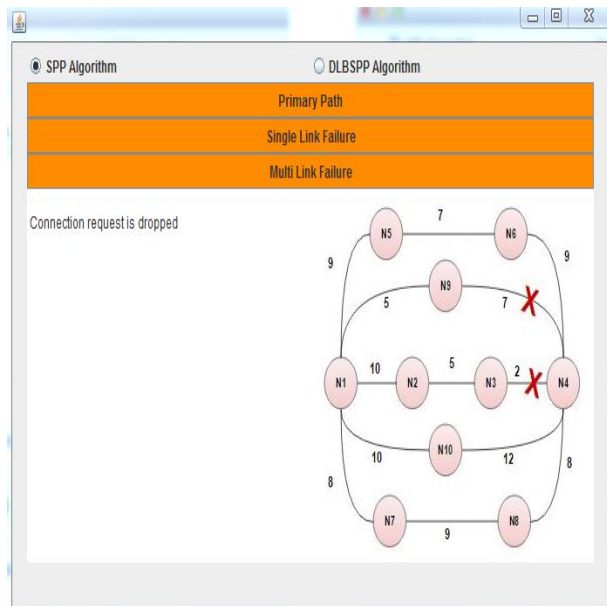


Fig. 15. Connection request dropped when link in both primary and shared backup path fail in SPP algorithm

Therefore, throughput (traversing the data from source to destination) is high in DLBSPP algorithm when compared to SPP algorithm. DLBSPP always sends the data successfully till it finds the alternate path. Below screen shots show how these algorithms perform in case of both primary and shared backup path fail simultaneously.

VII. CONCLUSION

In this paper, we discussed the possible problems with the large networks. Introduced the SLICE networks com-

paring how better it is when compared to standard WDM networks. We then brought up the consequences of link failures in the network while sending the data from source to destination and how they can be recovered using the survivability schemes. Then discussed about the protection and restoration schemes that are present for both path and link failures. We have two scenarios in link failures: single link failure and multi link failure. Then clearly discussed about the methods to handle single link failures and the drawbacks that each of these methods have: BSR (Bandwidth Squeezed Restoration) and Shared Path Protection (SPP). None of these methods of single link failure can recover data in case of multi link failures. So, we introduced the new algorithm DLBSPP (Dynamical load balancing shared path protection) that adopts TSAR scheme (Traffic Self-Adaptive Restoration) to calculate new routes for carrying the affected traffic in multi-link failures. Each of these algorithms adopt Dijkstras algorithm to calculate the shortest route from source to destination. For spectrum allocation, first fit and random fit schemes are used. From the simulation of our network, we calculated and proved that throughput is high in DLBSPP algorithm compared to the conventional SPP algorithm. Thus, the DLBSPP algorithm has much spectrum efficiency and much better survivability than SPP algorithm.

VIII. MILESTONES

- Problems with large amount of data in networks
- Introduction to SLICE Networks

- Loss of data during transmission
- Need for Survivable schemes
- Different kinds of link-failures
- Types of recovery methods
- Working on simulation
- Implement SPP and DLBSPP algorithms
- Compare the pros and cons of these algorithms
- Conclusion of our research

IX. REFERENCES

- 1) Sone, Y.; Watanabe, A.; Imajuku, W.; Tsukishima, Y.; Kozicki, B.; Takara, H.; Jinno, M., "Bandwidth Squeezed Restoration in Spectrum-Sliced Elastic Optical Path Networks (SLICE)," , IEEE/OSA Journal of Optical Communications and Networking, vol.3, no.3, pp.223,233, March 2011
- 2) Sone, Y.; Watanabe, A.; Imajuku, Wataru; Tsukishima, Yukio; Kozicki, B.; Takara, H.; Jinno, M., "Highly survivable restoration scheme employing optical bandwidth squeezing in spectrum-sliced elastic optical path (SLICE) network," Optical Fiber Communication - includes post deadline papers, 2009. Conference on OFC 2009., vol., no., pp.1,3, 22-26 March 2009
- 3) Yuan, S.; P. Jue, Jason., Shared Protection Routing Algorithm for Optical Networks.
- 4) Mrs. Sirak, S.; Mr. Kumar, Ajay.; Mrs. Rinku Badgujar, Network Simulation Tools Survey, ,International Journal of Advanced Research in Computer and Communications Engineering, vol.1, issue.4, pp.201,210, June 2012.
- 5) 5. Mallika, and Neeraj Mohan, Multiple Link Failure in Optical Network
- 6) Bowen Chen*, lie Zhang, Yongli Zhao, Chunhui LV,Wei Zhang, Yuan GU,Shanguo Huang,Wanyi Gu, "A Novel Recovery Algorithm for Multi-link Failures in Spectrum-Elastic Optical Path Networks"
- 7) Shengli Yuan, Jason P. Jue, Shared Protection Routing Algorithm for Optical Network
- 8) Takara, H. ; Kozicki, B. ; Tsukishima, Yukio ; Sone, Y. ; Matsuoka, S ; Jinno, M., NIT Corporation, "Spectrum-efficient and scalable elastic optical path network: architecture, benefits, and enabling technologies"
- 9) Bowen Chen*, lie Zhang, Yongli Zhao, Chunhui LV,Wei Zhang, Yuan GU,Shanguo Huang,Wanyi Gu, "Multi-link failure restoration with dynamic load balancing in spectrum-elastic optical path networks".