Protection Techniques For Wavelength Division Multiplexing Networks using Resource Delayed Release Strategy

Shideh Yavary Mehr and Byrav Ramamurthy
Department of Computer Science and Engineering
University of Nebraska-Lincoln, Lincoln, NE 68588, USA
Email:{syavarymehr, byrav}@cse.unl.edu
(Invited Paper)

2021 International Conference on Computer Communications and Networks (ICCCN) | 978-1-6654-1278-0/21/$31.00 ©2021 IEEE | DOI: 10.1109/ICCCN52240.2021.9522195

***Abstract*—Network availability is an important requirement in an optical telecommunication network. To overcome a disconnection, preparing a backup path before failure happens is required to reroute the affected traffic. This prevents any failure causing a significant amount of data loss or interruption in Wavelength Division Multiplexing (WDM) networks. Resource Delayed Release (RDR) is a new idea to improve the Service Provisioning Time (SPT) by adding the concept of idle optical channels. In earlier work [1] we proved that the delay in the removal of an idle optical channel helps the next service request to be carried immediately.**

In this paper, we address the problem of single link failure in WDM networks by comparing different protection methods when applied to the RDR strategy. We investigate and compare three algorithms that are mostly intended for maximization of the amount of remaining bandwidth over a damaged network. They are: Path Protection (PP), Link Protection (LP), and Partial Path Protection (PPP) [2]. The objective of this work is to apply the above protection methods on the RDR strategy to determine which method provides the best network performance in terms of Bandwidth Blocking Probability (BBP), Blocking Probability (BP), Service Provisioning Time (SPT), and recovery time (RT). Our simulation results show high network efficiency when using the RDR strategy with the PPP method for uniform traffic distribution. The highest BBP is when we do not apply any protection on RDR. When PPP is utilized there is a reduction of 58% in BBP, of 64% in BP, and of 40% in SPT. Additionally RDR with PPP results in the lowest RT measured.

***Index Terms*—Service Provisioning Time; Software Defined Networks; Wavelength Division Multiplexing (WDM);**

I. Introduction

One of the advantages of using Wavelength Division Multiplexing (WDM) over competing solutions such as time division multiplexing or slot division multiplexing is upgraded network capacity [3]. WDM provides the ability to carry a large amount of bandwidth over a single fiber [4], [5]. Therefore, a failure in a single physical link can lead to a large loss of data. Due to the volume of data transferred, any failure, can result in the disruption of telephone calls and internet service over a wide area. Such failures may happen in WDM networks, with the potential to cause the loss of millions of calls [4], [3], [6], and it is necessary to consider protection and restoration algorithms in the design of modern communication networks.

In this paper, we incorporate protection algorithms to the Resource Delayed Release (RDR) strategy discussed in [1]. Briefly, the RDR strategy adds the concept of idle optical channels. When an optical channel is not delivering any services, it is marked as an idle channel and not immediately removed. This allows a grace period during which, if another request can use this path, we can immediately use the existing channel instead of being forced to create a completely new channel. Since the RDR strategy resulted in reduced SPT, BP, and BBP, we have chosen to analyze the effects of different protection mechanisms on RDR under uniform traffic distributions. We also investigate if the RDR method is still efficient in terms of common network performance metrics. Finally, we study which protection method chosen is most suitable with the RDR strategy. The protection approaches in this work will configure the backup paths and corresponding wavelengths in advance of a failure. To make adding or dropping connected nodes easier we use the Mesh network topology, specifically, the National Science Foundation (NSF) topology [6]. The three algorithms: path protection, partial path protection [2], and link protection were implemented during the network design stage before a failure occurs. Simulations have been done under dynamic traffic. In dynamic traffic, we dynamically search for the paths based on the real time network status.

Comparison metrics include Blocking Probability (BP) meaning that the chance that a call will be denied service due to lack of resources. Bandwidth Blocking Probability (BBP) means the total bandwidth blocked over the total bandwidth requested, Service Provisioning Time (SPT) is the time it takes to carry a call, and Recovery Time (RT) is the time between when a link is disconnected from network and when the rerouted traffic reaches the destination node. Analysis was performed under three service durations of 60, 300, and 1500 (time slices). We used fixed bandwidth OTN services. Our simulation results prove the better network performance in terms of BBP, BP, SPT, and RT for different protection algorithms while using RDR under uniform traffic distributions. In using RDR with any protection, BBP is decreased compared to when we use RDR method without any protection due to increased bandwidth requirements. Based on simulations, we observe that SPT and BBP were slightly increased for link protection when compared to the path and partial path protection algorithms. In comparison to using the RDR method without protection all tested methods gave better results.

The rest of this paper is organized as follows: Background and related work are defined in Section II. RDR strategy with protection methods are shown in Section III. We present the simulation results in Section IV. Section V completes the paper and outlines our future work.

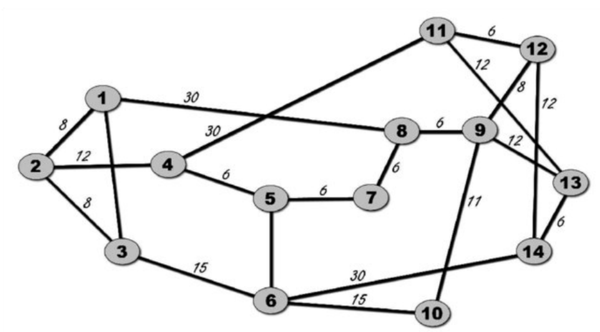


Fig. 1: NSFNET Topology. 14 nodes, 22 links

II. Background and Related Work

Data communication via optical transport networks relies heavily on fiber link and network node interaction. Therefore any fiber link failure can cause huge amounts of data loss. Such an event is extraordinarily difficult to predict. To prevent a loss of data in such an event, it is necessary to have some protection methods applied during the design of the network. In [2], the authors proposed a new protection method called PPP. In this method, each possible link failure along a primary path receives a different precomputed restoration path. One of the advantages of this method is re-use of operational segments of the original primary path in the protection path. They compared their proposed method with Path Protection (PP) method. They showed that PPP gave better results than PP.

In [5], the authors used two protection techniques, shared backup path protection and 1 + 1 path protection in elastic optical networks. Their objective function contains minimization of required spare capacity and maximization of the number of link Frequency Slots (FSs). In their work they considered tunable transponders for conditions such as using the same set of FSs for working and protection lightpaths. To maximize restoration levels on the affected flows with consideration of limited FS capacity on each fiber link, they applied the bandwidth squeezed restoration method. Their results showed that the proposed Shared Backup Path Protection (SBPP) method has better performance than the traditional 1 + 1 path protection approach in terms of lower spare capacity and improving spare capacity redundancy for proposed method (SBPP).

The authors in [7], proposed a new shared segment protection method for both node and link protection. They also compared their proposed method with the basic shared segment protection in NSF mesh topology [6]. They proved that their method is very efficient in terms of low cost because the cost of the number of ports in their method is highly related to the number of overlapping segments. However, in the basic shared segment protection method, cost does not relate to the overlapping segments. They also proved that their proposed method can protect 100% of any single node failure in the case of node protection. And, in case of dual link failure protection, their proposed method covers about 50%.

A. *Our contributions can be summarized as follows:*

(1) We are the first to study RDR under protection against a single link failure in WDM optical networks and to propose the best protection method (PPP).
(2) We compare the Path, Link and Partial Path protection models and evaluate the tradeoff between the resolution time and the effectiveness, in terms of bandwidth utilization, BP and SPT.
(3) Adding new metric BBP.
(4) Investigate the best protection methods in the RDR strategy to dramatically decrease recovery time and minimize blocking probability.
(5) Dynamically change the delay time when we have a heavy traffic.

III. Protection Methods for RDR Strategy

A. *RDR Strategy*

The RDR strategy proposed in [1], is an efficient method to reduce BBP, SPT, and BP by adding the concept of the idle state. The idle state starts when the channel completes carrying its current service. The reason for this state is to avoid frequent optical end-to-end circuit removal. During the idle state the optical channel and its resources are in standby mode for the certain amount of time called "delay time". Any new request is carried out by the idle channel immediately without spending time for channel establishment.

Without RDR optical channels that no longer carry any service will be removed. This takes a small amount of time and prevents channel reuse. Therefore we must spend another small chunk of time to reestablish the channel if it is needed again. These two times are inefficient for the system and result in high SPT. In the RDR strategy by keeping the channel in idle state, the amount of time wasted due to these small delays will be reduced. A typical work flow for the service Setup request and backup path in OTN over WDM networks with RDR strategy is presented in Fig. 7.

Our algorithm first selects the primary path, using a Kshortest path route. It then selects the protection paths using a Kshortest path algorithm in which wavelengths already assigned for protection can be used at no cost. We term the whole of the second heuristic, involving the choice of primary and of protection paths, the Kshortest path approach (KSP). We observe that the KSP approach is not only significantly simpler computationally than the greedy approach, but also more effective in terms of blocking probability. This result may seem surprising at first. However, since protection paths can share bandwidth, while primary paths cannot, it is reasonable to select the most economical primary first, as done by KSP, rather than consider primary and protection bandwidth jointly, as done by the greedy algorithm. The KSP approach, by selecting the primary path first, in effect prioritizes the efficient use of primary path resources over protection resources.

In a modern optical network, incorporating layers of redundancy and resiliency using advanced protection and restoration techniques leads to a very high reliability standard. Network failures can be immediately detected and services automatically re-routed around the affected paths. To reduce recovery time, protection methods have to be deployed at the first stage of network design. Optical communication networks require both protection and restoration mechanisms to achieve minimal service interruptions. In this paper we investigate the protection algorithms. Our approach in all protection methods is to reduce the bandwidth blocking probability. To obtain the protection needed to overcome failure in our WDM network, we configure backup and corresponding paths in advance [8].

1) Path protection: In Fig. 2, The working path is shown as the dashed, blue line (4, 5, 7, 8, 11). The corresponding backup path is shown by the bold, orange line (4, 2, 3, 6, 9, 11). In our graph, if a link, such as (4, 5) fails, then the protection mechanism is activated and traffic will traverse the backup path.

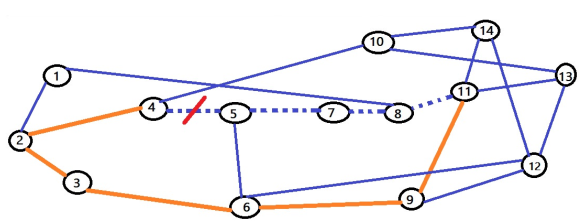


Fig. 2: Path protection scheme

2) Link protection: Through the use of a localized protection loop, all of the links in the protection algorithm's working path are protected. In the event that any of the paths fail, traffic will then be rerouted from the failed link. The algorithm utilizes a set of disjoint links to serve as a backup path for any failed links. The only condition is that these disjoint links on the backup path share the same wavelengths as the failed link. As demonstrated in Fig. 6 wavelengths are shared between the protected link (4, 5) and the backup path bold green line (4, 2, 3, 6, 5) used by the algorithm. In the event that the wavelengths aren't shared, or that the path is not available, traffic will then be discarded and the link will fail. Due to the algorithm only requiring local instead of global network information, there is a case to be made that, although generally less efficient than the path protection algorithm, it is still very viable.

3) Partial Path protection: As a way to accommodate static traffic load, Wang, Modiano, and Medard propose a partial path protection algorithm [9]. In order to protect a working path, a partial link disjoint must be preconfigured in the event there is not, disjoint backup path available. This backup path can't be found in the working path (2,1,3,6,9,11) of Fig. 3. However, in Fig. 4 a partial path protection algorithm is utilized, and the maximum disjoint backup path (2,1,8,11) is assigned. This is most effective when a lower degree, lightly connected network is being utilized. Figure 4 also illustrates that the partial path protection algorithm is capable of protecting against all link failures in a working path except if the link (2,1) itself fails.

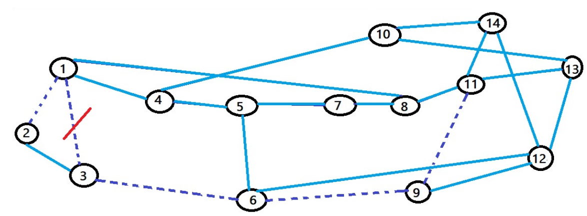


Fig. 3: Path protection can not be implemented in this case

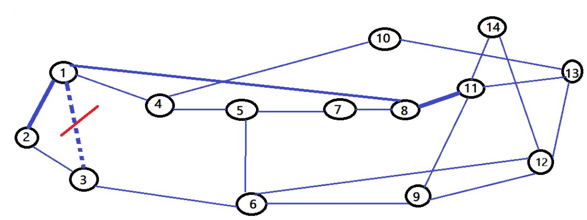


Fig. 4: As illustrated, the partial path protection algorithm compensates for the case when the path protection algorithm is unable to be used.

One aspect of the partial path protection algorithm is the creation of backup paths in the event of any given link failure in the working path, which are calculated ahead of time, but are not reserved. The only event that would trigger the utilization of any of these is if there is a link failure during computation. Figure 5 illustrates each of the corresponding backup paths for each of the links on the path (4, 5, 7, 8, 11). As an example, for the protected link (4, 5) the corresponding protection path (4, 2, 3, 6, 9, 11) is shown with a wide green line, protect link (5, 7) with the corresponding protection path (4, 2, 3, 6, 12, 14, 11) is shown with a blue dashed line, protected link (7, 8) is shown with the protection path (4, 10, 14, 11) is shown with the orange dashed line, and finally, the protected link (8, 11) is show with the protection path (4, 10, 13, 11) is shown with the purple dashed line. Because traffic is rerouted through the all link disjoint backup path, the algorithm does not need to locate any failed elements. However, the partial path algorithm is capable of finding the failed element. In turn, this means that this algorithm may be helpful as it makes restoration faster and more efficient for network managers.

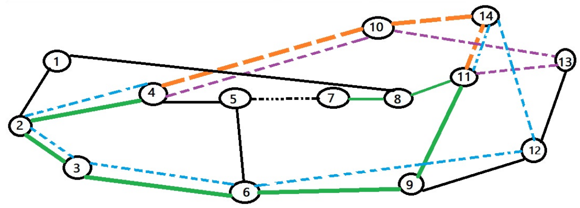


Fig. 5: Partial path protection

TABLE I: Simulations Results on the NSFnet Network Model

Algorithm	Working Path	RT (ms)	Protected Working Links	Backup Path
RDR+ PPP	(1, 3, 6,12)	66	(6,12)	(1,8,11,13,12)
			(3,6)	(1,8,11,9,12)
			(1,3)	(1,2,3,6,12)
RDR+ PP	(1, 3, 8, 12, 18)	90		(1,8,11,9,12)
RDR+ LP	(1,3,6,12)	120	(6,12)	(6,9,12)
			(3,6)	(3,2,4,5,6)
			(1,3)	(1,2,3)

IV. Simulation Results

Three algorithms are implemented here: a path protection algorithm, partial path protection algorithm, and a link protection algorithm. Additionally two simulations are run prior in order to evaluate proposed RDR strategies with protection methods. In each set of simulations run, certain performance measures like service provisioning time, bandwidth blocking probability, and blocking probability are taken in order to assess the RDR type. In each of the service requests mentioned, the source and destination pairs are selected randomly. The Poisson traffic model is used to generate variables like service duration and interval time for each of the requests. Also, link failures are randomly generated. For the simulation topology we use NSFNET (14 sites with 22 links) [10], under the assumption that the wavelength capacity is 100G and each fiber contains 80 wavelengths. In each case, first fit is used as the assignment method and KShortest Path (K=4) is used for routing. Also, 200,000 service requests for each simulation were generated. A stable network state was attained to extract the statistical data. To achieve the 95% confidence interval, all the results were computed over multiple simulations.

A. Protection vs without protection

Since the communication-based network relies on fiber link and network node interaction, any failure on the fiber link can lead to huge amount of data loss. Due to this fact, we expect that when we do not have any protection method, and a failure happens, some calls may be dropped, and as a result we lose some bandwidth. The service provisioning time also increases. So it is necessary to have protection algorithms. The protection algorithms will try to adjust all changes in the network at any moment. So the protection method helps to adjust and reconfigure any new changes to guarantee most of the connections are being rerouted to the destination nodes quickly. So, based on this, BBP and BP should decrease based on different types of protection algorithm. Also, this reconfiguring by protection methods helps ensure that all nodes are still connected, and therefore the service provision time will decrease. As we see in the simulation result on Fig. 8, we have the highest value in SPT, BP and BBP when we don't have any protection methods. And this is due to how the protection approaches configure the backup paths and corresponding wavelengths in advance of a failure. Before failure happens the affected path will be rerouted to a backup path. Then we will have a reduction to the number of calls, and based on using RDR method, the SPT decreases and the affected path will be carried.

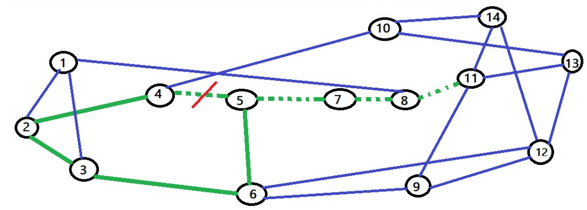


Fig. 6: Link protection scheme

B. Comparing three types of protection algorithm

Figure 8 presents the effect of different protection methods on RDR strategy in terms of SPT, BBP, BP under uniform traffic distributions. In the simulations, the traffic request ratio OTN_10G : OTN_40G : OTN_100G) is 1:1:1. Sub-figures a, b and c from Fig. 8 present the BBP comparison between 4 cases. RDR strategy without any protection methods, and RDR method with various protections (link, path and partial path) methods. Comparisons for these various strategies have been evaluated under three different service duration parameters (where TS is 60, 300, and 1500). Based on these results, the highest value of BBP belongs to the method of RDR without protection. The lowest value of BBP is shown when we use PPP method, both PP and LP methods have respectively higher values of BBP than PPP method. Compared between PP and LP, PP method has shown the better performance than the LP method. Respectively, Sub-figures d, e and f from Fig. 8 present SPT comparison results, and sub-figures g, h and i present BP comparison results. Those comparisons have been done between four cases: RDR strategy without any protection methods, and RDR method with various protections (link, path and partial path) methods. Simulations under service duration 60, 300, and 1500 show that the highest value of SPT and BP belongs to the method of RDR without protection method. The lowest value of SPT and BP is when we use PPP method. PP, SP and LP have respectively higher BP and SPT than PPP. PPP method potentially reconfigures all the lightpaths, as a result of which we have the lowest blocking probability. Since the wavelength available on the backup path is not the same as that of a failed link in link protection method, traffic is blocked. Therefore we have the higher BP and BBP on link protection than path protection [10].

C. Recovery Time Analysis

We compare the recovery times for path, link and partial path protection schemes. Since for these three protection algorithm we use end-to-end protection schemes then recovery is performed based on a simple failure notification. To evaluate the recovery time we consider the time between when a link is disconnected from the network and when the rerouted traffic reaches the destination node. Simulation results in regards of recovering time based on using different protection method are summarized in Table I. As we see in the Table I, the recovery time for the PPP method is significantly lower than PP or LP methods while utilising the RDR method because of the fact that resources are better utilized. Relative to the PP and LP methods, the partial protection algorithm finds an entirely new path disjoint only to the failed link, dramatically reducing the recovery time. In the PP and LP methods, the new paths are disjoint to all links in the original path. Also we observed that when the number of hops increase then the recovery time increases by utilizing resources more efficiently [11], [12], [13], [14], [15].

V. Conclusion and Future work

We have evaluated the problem of single link failure in WDM networks by comparing three different protection methods using the RDR strategy. We also investigated and compared the efficiency of each method using RDR strategy. Our evaluations have been done under uniform traffic. As we expected from the PPP method, we found out that PPP is a more flexible solution in comparison to PP or LP. PPP outperforms PP and LP in terms of BBP, BP and SPT. Moreover, the PP approach performs better than LP method. However, LP, PP and PPP had a better performance in terms of BBP and BP than using RDR without any protection methods. The advantages of using PPP method over PP and LP appear in the network management. In using the PP method the localization of the failure is not a main factor, and the main factor in this method is the source and destination update upon a failure occurring in the primary path. In the LP method, it is necessary that any nodes adjacent to the failure know the local information. In this approach path by path protection is not necessary. Our results show that PPP method outperforms the other methods.

Our future work will be to use ANN machine learning methods to predict the failure and create a backup path based on the result. Also, we will use machine learning to generate a good estimate of t_{delay}. We will investigate a different routing algorithm, such as greedy approach, in non uniform traffic to see if a better fairness result can be achieved. We will also add a few restoration algorithms. These restoration algorithms will help to find alternative paths in case the provided protection algorithms cannot recover from the failure within the system. We will use another metric, "vulnerability ratio", to describe the performance of our algorithms in the context of random single link failures and time complexity of PP or PPP algorithms.

Acknowledgments

This work was supported in part by the U.S. National Science Foundation grant (NSF CNS-1817105).

References

[1] Y. Zhou, B. Ramamurthy, B. Guo, and S. Huang, “Resource delayed release strategy for dynamic and fast end-to-end service provisioning in SDN-enabled OTN over WDM networks’,” in *2017 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*, 2017, pp. 1–6.

[2] H. Wang, E. Modiano, and M. Medard, “Partial path protection for WDM networks: end-to-end recovery using local failure information,” in *Proceedings ISCC 2002 Seventh International Symposium on Computers and Communications*, 2002, pp. 719–725.

[3] N. Kitsuwan, S. McGettrick, F. Slyne, D. B. Payne, and M. Ruffini, “Independent transient plane design for protection in openflow-based networks,” *J. Opt. Commun. Netw.*, vol. 7, no. 4, pp. 264–275, Apr 2015. [Online]. Available: http://jocn.osa.org/abstract.cfm?URI=jocn-7-4-264

[4] S. Suthaharan, N. Ravithas, and A. F. Sharfana, “Wavelength conversion scheme for dedicated protection in WDM optical networks,” in *2017 IEEE International Conference on Industrial and Information Systems (ICIIS)*, 2017, pp. 1–6.

[5] G. Shen, Y. Wei, and S. K. Bose, “Optimal design for shared backup path protected elastic optical networks under single-link failure,” *J. Opt. Commun. Netw.*, vol. 6, no. 7, pp. 649–659, Jul 2014. [Online]. Available: http://jocn.osa.org/abstract.cfm?URI=jocn-6-7-649

[6] https://en.wikipedia.org/wiki/National_Science_Foundation_Network#/media/File:NSFNET-backbone-T1.png.

[7] B. Jaumard, N. Nahar Bhuiyan, S. Sebbah, F. Huc, and D. Coudert, “A New Framework for Efficient Shared Segment Protection Scheme for WDM Networks,” in *10th INFORMS Telecommunications Conference*, Montréal, Canada, May 2010. [Online]. Available: https://hal.inria.fr/inria-00482121

[8] D. Ghoshal, K. Wu, E. Pouyoul, and E. Strohmaier, “Analysis and prediction of data transfer throughput for data-intensive workloads,” in *2019 IEEE International Conference on Big Data (Big Data)*, 2019, pp. 3648–3657.

[9] S. Ramamurthy, L. Sahasrabuddhe, and B. Mukherjee, “Survivable WDM mesh networks,” *J. Lightwave Technol.*, vol. 21, no. 4, p. 870, Apr 2003. [Online]. Available: http://jlt.osa.org/abstract.cfm?URI=jlt-21-4-870

[10] https://en.wikipedia.org/wiki/National_Science_Foundation_Network#/media/File:NSFNET-backbone-T1.pn.

[11] D. K. Tyagi, V. K. Chaubey, and P. Khandelwal, “Routing and wavelength assignment in WDM network using IWD based algorithm,” in *2016 International Conference on Computing, Communication and Automation (ICCCA)*, 2016, pp. 1424–1429.

[12] A. Tomassilli, B. Jaumard, and F. Giroire, “Path protection in optical flexible networks with distance-adaptive modulation formats,” in *2018 International Conference on Optical Network Design and Modeling (ONDM)*, 2018, pp. 30–35.

[13] R. T. Koganti and D. Sidhu, “Analysis of routing and wavelength assignment in large wdm networks,” *Procedia Computer Science*, vol. 34, pp. 71–78, 2014, the 9th International Conference on Future Networks and Communications (FNC’14)/The 11th International Conference on Mobile Systems and Pervasive Computing (MobiSPC’14)/Affiliated Workshops. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1877050914009028

[14] W. Kmiecik and K. Walkowiak, “Survivable overlay multicasting in WDM optical networks with dual homing architecture,” in *2014 International Conference on Optical Network Design and Modeling*, 2014, pp. 19–24.

[15] V. M. Bhadrashetti, G. Pathak, S. B. Tantry, P. Biswagar, M. Sachin, and S. P. Nagesh, “Performance analysis of routing and wavelength assignment in optical networks,” in *2019 1st International Conference on Advanced Technologies in Intelligent Control, Environment, Computing Communication Engineering (ICATIECE)*, 2019, pp. 287–290.

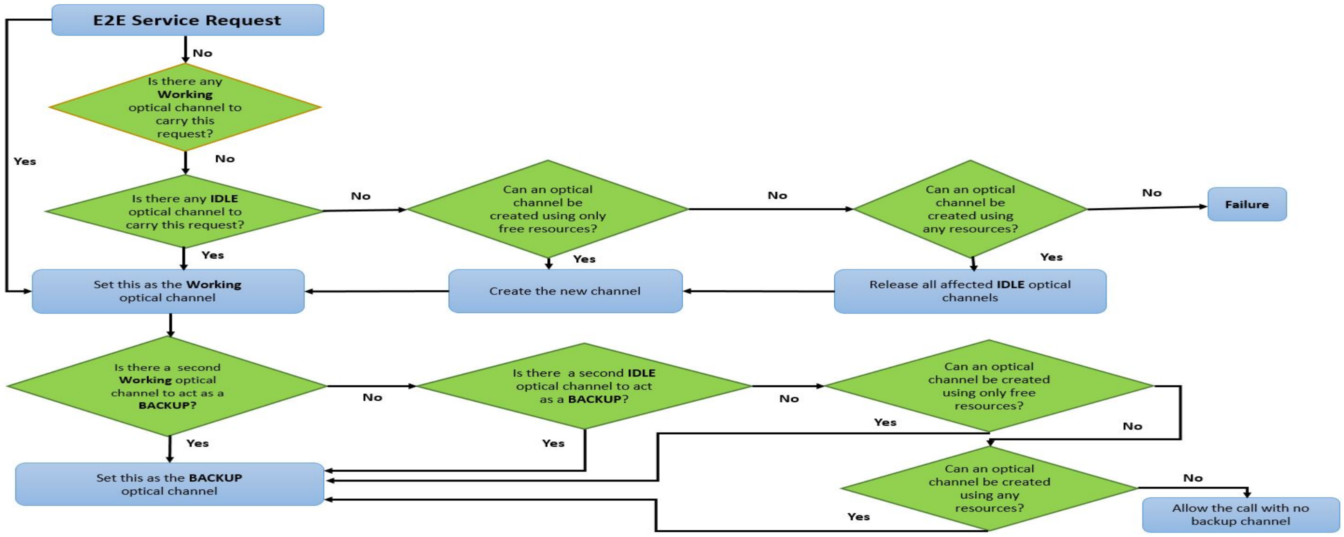
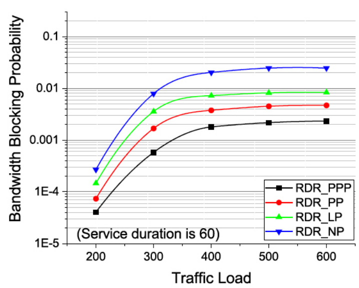
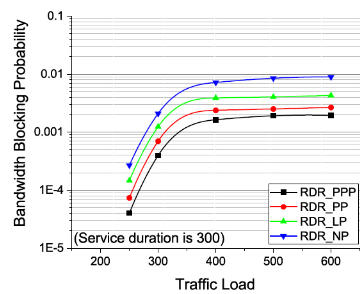


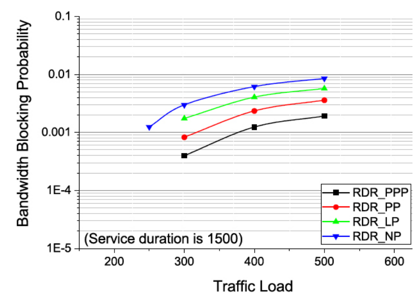
Fig. 7: Typical workflow of RDR strategy with the backup protection.



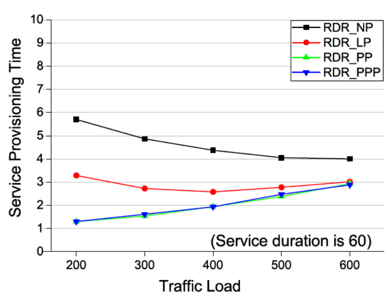
(a)



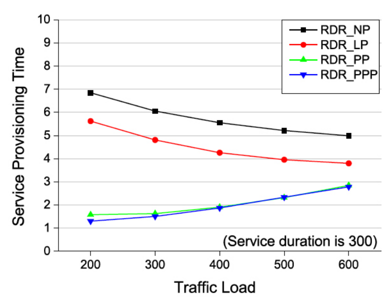
(b)



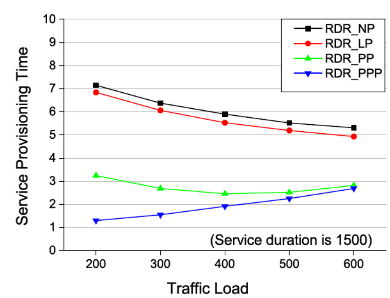
(c)



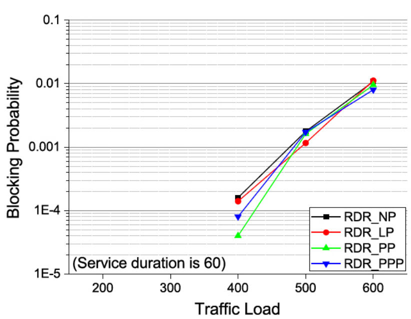
(d)



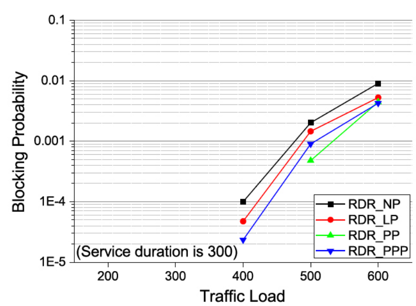
(e)



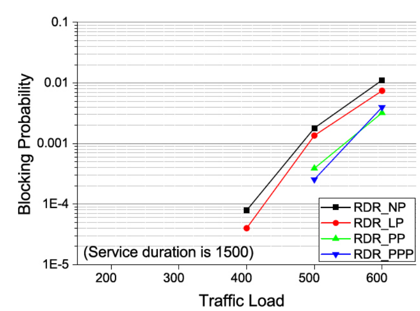
(f)



(g)



(h)



(i)

Fig. 8: Uniform traffic; Sub-figures a, b, c: Comparing BBP under service duration of 60, 300 and 1500; Sub-figures d, e, f: Comparing SPT under different traffic durations; Sub-figures g, h, i: Comparing BP under different service durations.