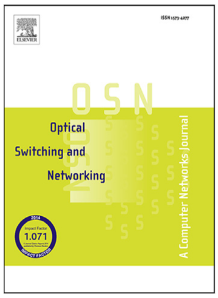
Journal Pre-proof



Protection techniques using Resource Delayed Release for SDN-based OTN over WDM networks

Shideh Yavary Mehr, Byrav Ramamurthy

PII: S1573-4277(23)00033-4
DOI: https://doi.org/10.1016/j.osn.2023.100762
Reference: OSN 100762

To appear in: *Optical Switching and Networking*

Received date : 22 June 2023
Revised date : 24 August 2023
Accepted date : 26 August 2023

Protection Techniques using Resource Delayed Release for SDN-based OTN over WDM Networks

Shideh Yavary Mehr
Department of Computer Science
University of Wisconsine-Milwaukee
Email: yavaryme@uwm.edu

Byrav Ramamurthy
School of Computing
University of Nebraska-Lincoln
Email: byrav@cse.unl.edu

***Abstract*—The availability and reliability of optical backbone links are very important to ensure the efficient operation of the Internet. To address the issue of data loss due to optical link failures, there is a need for an optimal recovery strategy so that the traffic can be rerouted on a backup path to the destination. This paper builds on top of our prior research efforts [1], [2] which introduced the concept of Resource Delayed Release (RDR) by adding a new state called "idle state" which begins when the channel has completed carrying its services so that the next request can be carried immediately instead of waiting for a new channel to be established. While RDR improves the network performance by reducing the service provisioning time and blocking probability, it does not handle link failures which are quite common in optical networks. Therefore, enhancing RDR with protection strategies will make the network more reliable and thus we investigate this topic in this work.**

In this paper, we evaluate four different protection methods for single link failure recovery in WDM networks (Path Protection (PP), Partial Path Protection (PPP), Segment Protection (SegP) and Link Protection (LP)) with two different routing approaches namely Shortest Path (SPath) and Greedy (G) algorithm under uniform and non-uniform traffic generated using real traffic traces collected from a local Internet Service Provider (ISP). Special attention while evaluating these protection strategies was paid to the optimization of the amount of remaining bandwidth. The performance evaluation of the network under uniform and non-uniform traffic was done over the NSFNet and COST239 topologies by employing the metrics of link and network utilization, Blocking Probability (BP), Bandwidth Blocking Probability (BBP), Recovery Time (RT) and Service Provisioning Time (SPT). Our results show that the PPP method performs the best in terms of reducing BP, BBP, and SPT compared with PP, LP, and SegP in all three topologies while utilizing RDR.

***Index Terms*—Link Protection; Path Protection; Partial Path Protection; Resource Delayed Release (RDR); Segment Protection; Wavelength Division Multiplexing (WDM).**

I. Introduction

One of the goals of Wavelength Division Multiplexing (WDM) optical networks is meeting the increasing bandwidth demands of the Internet. A major catastrophe that often occurs is a single optical link failure that results in the failure of traffic delivery across the route to which the link belongs. This results in the dropping of millions of calls as well as the disconnection of the Internet services [3], [4], [5], [6], [7].

While RDR improves the network performance by reducing the service provisioning time and blocking probability, it does not handle link failures which are quite common in optical networks. Therefore, enhancing RDR with protection strategies will make the network more reliable and thus we investigate this topic in this work.

To address this issue, a reliable protection method that reroutes the traffic from the damaged path towards the intended destination is needed. A survivable telecommunication backbone network requires a very fast path restoration when failures happen and many works have focused on techniques such as the minimization of path restoration times and protection of path lengths and maximization of the restored bandwidths [8]. This work evaluates and compares different types of protection methods to maximize the utilization of the amount of remaining bandwidth. We mainly compare four methods, namely, Partial Path Protection (PPP), Path Protection (PP), Segment Protection (SegP) (up to 3 segments), and Link Protection (LP).

Resource Delayed Release (RDR) approach was introduced in [1], by adding a new state called "Idle" to the optical channel. The main goal behind adding this state is to keep all the resources in standby mode for a certain amount of time. In other words, when an optical channel finishes its services, it is not removed immediately. The state of the channel switches to idle for a specific period of time. This time which is called delay time allows the channel to carry any new request that arrives during this period. The main idea for comparing the aforementioned four single link failure recovery methods on RDR was motivated by RDR's capability to improve the network utilization as presented in our previous efforts [1], [3]. Therefore, we theorize and later demonstrate with our results that the four protection methods perform better when used in tandem with RDR and consequently make the network more reliable. The aforementioned four protection methods are implemented during the network design phase and before any link failure happens. Simulation results are presented comparing the four protection methods under varying dynamic traffic loads to closely resemble the non-deterministic nature of the real Internet traffic.

We chose the RDR strategy as a baseline to build and integrate the aforementioned four protection methods because RDR was shown to improve some important network metrics such as the Network Utilization (NU), Service Provisioning Time (SPT), Link utilization (LU), Blocking Probability (BP), and Bandwidth Blocking Probability (BBP). The BP represents the likelihood of a being dropped due to lack of network resources [9]. The sum of the bandwidth blocked divided by the sum of the total bandwidth requested gives the BBP, while SPT is the duration of the time it takes to carry any requests from the source to its destination, and Recovery Time (RT) is the time that it takes for the rerouted traffic to reach its destination after a link is disconnected from the network. The percentage of the network bandwidth which is used at a particular traffic load defines NU. LU is the percentage of the capacity that is used [10], [11]. We analyze the performance, and reliability of the four protection mechanisms using the network metrics such as the SPT, BP, BBP, and RT. Under the assumed dynamic traffic conditions, all the protection methods dynamically search for the backup paths and will configure those paths with corresponding wavelengths before failures happen. The configuration of each protection method is based on the real-time network status [12].

Fixed-bandwidth OTN services are considered the underlying network technology in this work. We assume uniform as well as non-uniform traffic distributions over the NSFNet, and COST239 topologies [13]. We expect to have better network performance for different protection methods while using RDR versus RDR without any failure protection methods. Our simulation results demonstrate that our expectation was correct. Additionally, BBP was shown to be significantly reduced when any of the four protection methods are integrated into the RDR compared to RDR without any failure protection strategies. The SPT and BP results show that LP performs slightly worse compared to the SegP, PP, and PPP algorithms.

The following list summarizes the main contributions of this paper:

- For the four protection methods, namely, LP, PP, PPP and SP, we present the routing computation and implementation details, recovery computation timing, and network capacity assignment (Part III-C).
- We present performance comparisons for the four protection methods under uniform and non-uniform traffic (synthetically generated based on the traffic traces from a local Internet Service Provider (ISP) based in the midwestern United States) with respect to the BP, BBP, SPT, LU, NU, and RT (Part IV-B and Part V).
- We study and evaluate different protection methods under two different routing approaches in terms of RT, LU, and NU (Part IV-F, G).

The organization of the rest of the paper is as follows. Section II covers the related work. Section III covers the four protection methods and two routing algorithms. Section IV presents the simulation results. Section V concludes our work.

II. Related Work

A wide variety of reasons can cause link failures which result in degraded performance and loss of huge amounts of data. Numerous studies show the prediction of fiber link failures is difficult and in some cases is not accurate. Therefore, even while using restoration methods we will lose some data. The best way to eliminate data loss is to apply some protection methods in the design stage of the network [14], [15].

In [16], a new model based on Support Vector Machine (SVM) and double exponential smoothing (DES) was proposed. Their method is used for failure prediction in optical networks. Their prediction model is focused on risk-aware models in optical networks which combines the SVM method and DES. Their proposed model has a protection plan to predict the risk of equipment failure. Their results showed that the average prediction accuracy is 95% to predict an equipment failure. They proved that their DES-SVM method significantly improves traditional risk-aware models in terms of failure prediction. Their model also helps to enhance the stability of the optical network.

The paper in [9], introduces an analytical and practical model to evaluate the availability of a WDM network under multiple link failures with shared link connections. Their analytical model is based on all the information for all possible combinations of the unshared protection paths. A set of shared paths for each protection path is the only factor that their proposed model needs. The results of the paper under multiple link failures show the survivability of WDM networks using shared connections.

The authors in [12], proposed a heuristic method called segment shared protection (SSP) to protect dual link failures. Their proposed method includes a few steps. In the first step is SSP calculates a least-cost working path for any request and then divides the working path into multiple overlapped segment paths. In last step, SSP calculates the two least-cost and link disjoint backup paths for an individual segment. In their method if any fiber link does not overlap with two segment paths then the corresponding backup path of those segments will share the same reserved backup wavelength. In their work they reviewed the protection switching time. Their simulation results have been done under dynamic traffic load and shows the accuracy of their model. The results prove that SSP is a reliable model to protect against dual link failures.

Our motivation is to investigate which protection method and which routing method from the literature performs best with the RDR strategy under both uniform and non-uniform traffic load.

III. Methodology

The NSFNet topology with 14 nodes and 22 links is used as the model for our simulations (see Fig 1). The capability of full wavelength conversion is assumed. Each link has 16 wavelength channels with capacity of 100G for each. K-shortest path (k = 4) [17] and G algorithm based on our objective criteria was used. First Fit algorithm was used for the wavelength assignment. Even though WDM optical networks have extremely improved the reliability and stability of data communication, they are vulnerable when optical components fail. Single and multiple physical link failures are the most common occurring failures [13]. Since fiber networks provide a massive bandwidth, any failure causes the loss of a huge amount of data. So, it is important to identify the failure and setup the backup paths. The backup paths will forward the traffic to the destination. In other words, the backup paths reroute around the failed link [18].

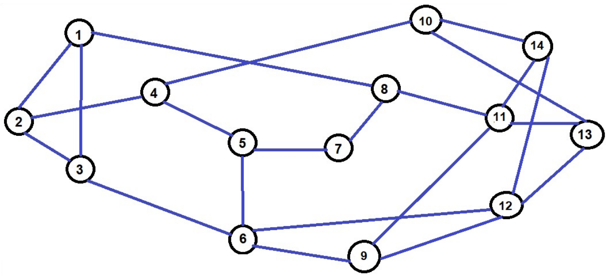


Fig. 1: NSFNet Topology

A. RDR Method

The proposed method, RDR [2], is an effective method for reducing some network parameters such as BBP, SPT, and BP by adding a new state called "idle state" in an optical channel. When an optical channel completes carrying its current request, instead of being removed it switches to an idle state. The Idle state is maintained in the control layer and changes in the device layer does not require any. The reason for adding an idle state is to avoid channel re-establishment after teardown. An idle state is another definition of standby mode because in this state, the channel and its resources are active and ready to carry the next request. The time that the channel and its resources are active is called "delay." If during the delay time a new request arrives, it will be transmitted immediately. In general, when an optical channel completes its job, it will be removed. For any new requests, a new channel has to be established. Approximately 10 seconds are needed for the channel establishment. Most of that time will be spent for the power equalization phase [19], [20], [21]. The time for a new channel establishment results in a higher SPT and BP. The RDR method intends to remove the time taken for the power equalization. In other words, if there is any new request arrivals during the delay time period that request is immediately carried up by one of the idle channels. Figure. 12 shows the setup process for the working and backup paths in OTN over WDM networks employed with RDR.

B. Protection Strategies

One of the optical network failures is a link failure. This type of failure happens due to different issues such as fiber cut. A high-reliability standard can be achieved by adding layers of redundancy and resiliency with the use of advanced protection and restoration methods. To increase the performance of the network and resolve link failure, failure detection has to be done as quickly as possible and services have to be rerouted around the affected paths. Deployment of any protection method has to be applied in the network design stage to decrease recovery time. In this paper, we will focus on four different protecting methods, which are described next.

1) Path Protection (PP): This protection is one of the basic protection methods that requires the backup path to be entirely link-disjoint from the corresponding working path. However, when a failure occurs and a disjoint path is not available, blocking probability increases due to dropping the request. Figure 2, shows the working path (dashed blue line (4,5,7,8,11)) and corresponding backup path (bold orange line (4,2,3,6,9,11)). This method needs global network information which results in a higher latency in the whole system [13]. In our approach with using RDR, the protection mechanism is activated when a link failure happens. The traffic will traverse the backup path once link (4,5) fails.

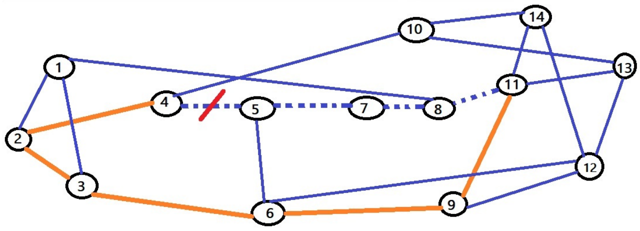


Fig. 2: Illustration of PP mechanism

2) Partial Path Protection (PPP): The partial path protection (PPP) method is the generalization of the PP method. In this method some segments of the working path could be reused in the backup path. It means when there is no link-disjoint backup path for a working path, the partial link disjoint backup path is preconfigured. PPP method selects end-to-end backup paths using local information about network failures. Consider the working path (2,1,3,6,9,11) in Fig. 3. If the link (1,3) fails, PP method cannot be used to find any link-disjoint backup path. In this special case, PPP method can protect all the link failures. We can have the maximum disjoint path (2,1,8,11) as protection path (see Fig. 4). This is efficient when the degree of the network is low in the overall network. The main characteristic of the PPP method is to use the

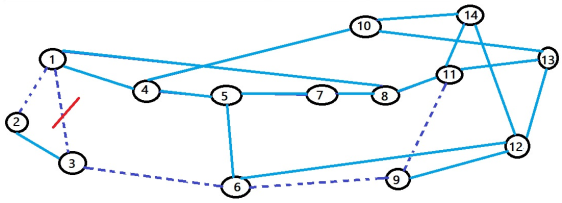


Fig. 3: An illustration of how the PP method fails to find a link-disjoint backup path.

local information to create a backup path when a link failure occurs in a working path. The creation of a backup path is done ahead of time. Figure 4 shows the corresponding backup paths for each working path. It is shown that each backup path is computed for the individual links for the working path of (4,5,7,8,11). The link (4,5) of the working path can utilize the

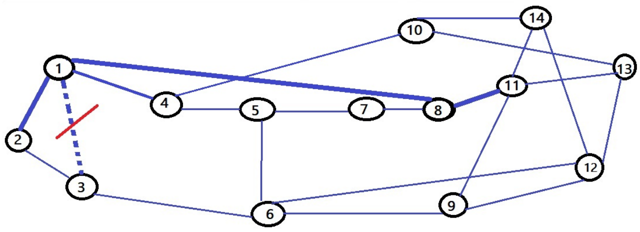


Fig. 4: An illustration of how PPP method can create backup paths for failed links.

computed backup path of (4,2,3,6,12). Also, each link of the working path (4,5,7,8,11) and the corresponding backup path are shown in Table I and Fig. 5. Essentially, the PPP approach can be deemed helpful through its ability to improve network management and provide a faster form of restoration.

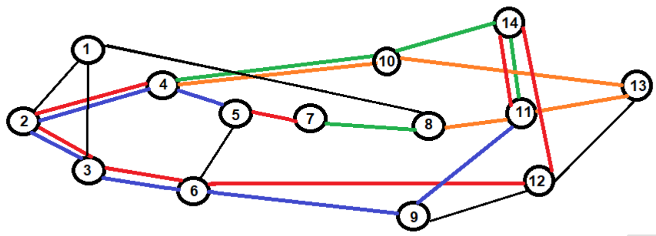


Fig. 5: PPP scheme.

TABLE I: The working and the corresponding backup paths

Working Link	Corresponding backup path	Color
(4,5)	(4,2,3,6,9,11)	Blue
(5,7)	(4,2,3,6,12,14,11)	Red
(7,8)	(4,10,14,11)	Green
(8,11)	(4,10,13,11)	Orange

3) Segment Protection (SegP with k=3): Segment based protection provides protection backup paths in segments. The working and backup paths will be separated within segments unlike path and link-based protection where a backup path and links are reserved as protection for the working path or links [12]. Segment protection provides protection through segments of the working path. In Fig. 6 the working path is shown as the green line (1,8,11,13).

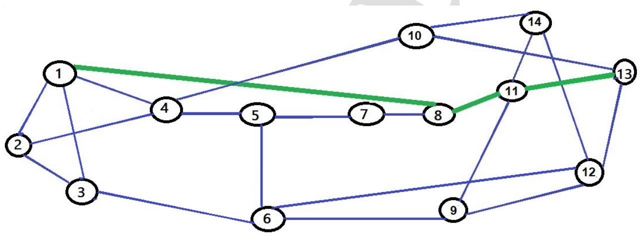


Fig. 6: SegP scheme.

4) Link Protection (LP): Link protection is another basic method of protection that has a higher restoration time. The link protection method when compared to segment and path protection is less efficient in terms of network and link utilization [18] while it is easy to implement. In this method when a link (4,5) fails (illustrated in Fig. 7), the backup path (4,2,3,6,5) protects the failed link using the same wavelength used for the failed link (4,5). In the case that the wavelengths are not available on the backup route, the affected traffic will then be discarded. Due to the nature of this method, local information would be enough to implement this type of protection. This is the advantage of link protection.

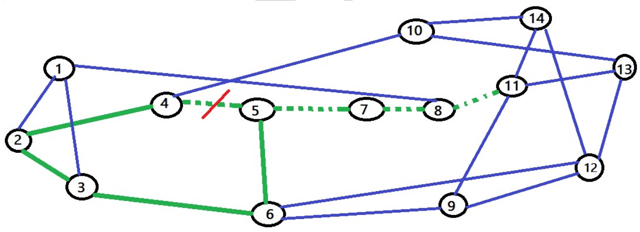


Fig. 7: LP scheme.

C. Routing Algorithms

1) Shortest path (Spath) algorithm: The shortest path (SPath) algorithm uses fewer physical links and can be implemented as a heap of Dijkstra's algorithm [22], [23]. In SPath method, some algorithms such as Dijkstra's algorithm, which is a polynomial-time algorithm is used to find the working and backup paths. Even though for a given request, SPath method uses more resources, it results in a better efficient bandwidth utilization for a sequence of calls. We see that SPath routing is more effective than a G approach (described next). The reason for this result is because SPath method encourages protection sharing and uses the less links.

2) Greedy (G) algorithm: The greedy algorithm is a generic method to problem-solving that selects the option that is locally optimal at each stage in the hopes of locating a global optimum. Although it does not ensure the best answer, it is frequently employed as a heuristic for resolving optimization issues. In other words, the G method is a chooses the locally optimal solution at each stage, whereas the shortest path algorithm is used to determine the shortest path between two nodes for routing. The G method is used for optimization problems because it considers the wavelength utilization of the links in determining the backup paths. Therefore it needs intensive computing power. For each call arrival, the G method minimizes the number of wavelengths which is used for the working and backup path jointly and selects a least-cost path as the working path. Previously unused wavelengths are used to establish the working and backup paths jointly. In other words, when a single link failure needs only one protection path on any wavelength then the used wavelengths can be

TABLE II: Comparison of protection methods' results on the NSFNET topology.

Approaches	PrimaryPath	Recovery Time (ms)	Protected working Links	Backup Path
RDR+PPP	(1,3,6,12)	44	(6,12)	(1,8,11,13,12)
			(3,6)	(1,8,11,9,12)
			(1,3)	(1,2,3,6,12)
RDR+PP	(1,3,6,12)	58		(1,8,11,9,12)
RDR+SegP	(1,3,6,12)	72	(1,8,9,13)	(1,2,4,5,7,8)
RDR+LP	(1,3,6,12)	80	(6,12)	(6,9,12)
			(3,6)	(3,2,4,5,6)
			(1,3)	(1,2,3)

used again [24]. When a protected solution is not found, the G method does not make a routing. Also, the G method selects paths with no protection sharing and no potential to harm network resources utilization.

IV. Simulation Results

To evaluate the protection methods, we simulate SegP, LP, PP, and PPP methods using RDR strategy with the two routing methods namely, SPath and G algorithms. 88 wavelengths with the capacity of 100G were used for each fiber. First fit algorithm is used for for wavelength assignment. SPath (K=4) and G algorithms are used for the routing problem. Each simulation contains 300,000 service requests. A few measurements such as SPT, BP, BBP and RT were used to compare the performance of each protection methods. To achieve the 95% confidence interval, all the simulations results have been done multiple times.

A. Uniform Traffic Data

For uniform traffic we use NSFNET [14] topology. In uniform simulations, the source and destination are randomly selected. Poisson traffic model has been used to generate the interval time and service duration for each service request. Also, the service times are exponentially distributed.

B. Non-Uniform Traffic Data

The non-uniform traffic is generated based on the traffic traces from a local Internet Service Provider (ISP) based in the midwestern United States. Table III was generated based on the probability of different source-destination pairs. In other hands Table III provides the probability (or likelihood) of communication occurring between a source and destination at any given time from the non-uniform traffic dataset.

C. Protection methods comparison

We evaluated survivable routing for RDR strategy in WDM networks using PPP, PP, LP and SegP methods under uniform and non-uniform traffic using both the SPath and G routing algorithms. The simulations have been done for different service duration of 60, 300, and 1500 ms. The overall average results are taken from the simulation over a series of iterations to achieve 95% confidence. As we expected to have a better performance on the PPP method. We can see that the highest values of BP, SPT, and BBP belong to the LP method. The lowest values of those metrics belong to the PPP method. LP, SegP and PP have respectively higher BP, SPT, and BBP than PPP method. Figures 13, and 14 demonstrate the performance of all four protection methods on RDR strategy under uniform and non-uniform traffic respectfully. As we have seen, the PPP protection method shows lower BP, BBP and SPT under both traffic distribution. Although under non-uniform the values for those metrics are a little bit higher. Figures 8, 9, 10, and 11 show the results of the two other metrics we evaluated in this work. Our evaluation demonstrates that the PPP method has the highest LU and NU compare with the other methods and also the SPath routing algorithm outperforms G algorithm.

The metrics that were evaluated in this work are namely LU, NU, SPT, BBP, BP under two different types of traffic, uniform and non-uniform. Different values for the ratio, OTN_10G, OTN_40G, and OTN_100G have been used for the simulation.

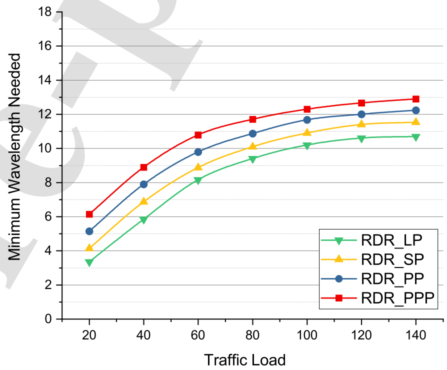


Fig. 8: Link Utilization using SPath.

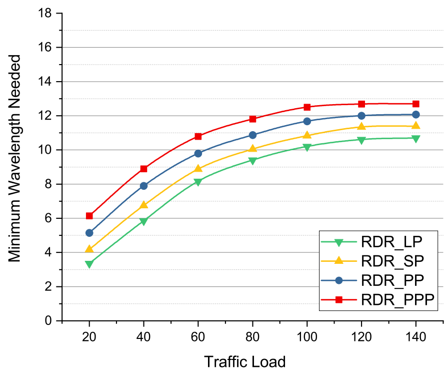


Fig. 9: Link Utilization using Greedy algorithm.

D. Recovery Time analysis

One of the main concerns of the WDM network is the survivability of the network after the event of any failure. Also, the recovery time for restoring all the services has been the source of attention recently. Recovery time (RT)

TABLE III: Non-Uniform transition matrix based on real data.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	0	0.187738272	0.127308417	0.109407478	0.078110521	0.074528658	0.072086693	0.067087638	0.063280186	0.048463825	0.045365086	0.042525105	0.042107282	0.041990841
2	0.327261609	0	0.105440472	0.090614402	0.064693367	0.061726766	0.05970426	0.055563901	0.05241046	0.040139126	0.037572661	0.035220508	0.034874455	0.034778015
3	0.31166296	0.148078896	0	0.086295343	0.061609812	0.058784612	0.056858507	0.052915494	0.04991236	0.038225928	0.035781792	0.033541752	0.033212193	0.03312035
4	0.307323734	0.146017221	0.099016685	0	0.06075203	0.057966164	0.056066877	0.052178762	0.049217439	0.037693716	0.035283609	0.033074756	0.032749786	0.032659222
5	0.30002068	0.142547356	0.096663712	0.08307175	0	0.056588691	0.054734537	0.050938817	0.048047866	0.036797985	0.034445151	0.032288788	0.03197154	0.031883128
6	0.299206937	0.142160727	0.096401532	0.082846435	0.059147494	0	0.054586082	0.050800656	0.047917546	0.036698178	0.034351726	0.032201211	0.031884824	0.031796652
7	0.298654687	0.141898339	0.096223603	0.082693524	0.059038325	0.056331043	0	0.050706893	0.047829104	0.036630444	0.034288322	0.032141777	0.031825974	0.031737964
8	0.297530487	0.141364203	0.095861396	0.082382248	0.058816092	0.056119001	0.054280237	0	0.047649065	0.036492559	0.034159253	0.032020789	0.031706174	0.031618496
9	0.296679918	0.140960076	0.095587352	0.082146737	0.058647951	0.055958571	0.054125063	0.050371608	0	0.036388236	0.0340616	0.031929249	0.031615534	0.031528106
10	0.293415781	0.139409203	0.094535679	0.081242941	0.058002694	0.055342902	0.053529567	0.049817409	0.046990101	0	0.033686847	0.031577956	0.031267693	0.031181227
11	0.292742171	0.139089154	0.094318648	0.081056427	0.057869534	0.055215848	0.053406676	0.04970304	0.046882223	0.035905265	0	0.031505461	0.03119591	0.031109643
12	0.29212752	0.138797118	0.094120614	0.080886238	0.057748029	0.055099916	0.053294542	0.049598682	0.046783788	0.035829877	0.033538943	0	0.03113041	0.031044324
13	0.292037309	0.138754256	0.094091549	0.08086126	0.057730196	0.0550829	0.053278084	0.049583366	0.046769341	0.035818813	0.033528586	0.031429603	0	0.031034737
14	0.292012179	0.138742316	0.094083452	0.080854302	0.057725228	0.05507816	0.053273499	0.049579099	0.046765316	0.03581573	0.033525701	0.031426898	0.031118119	0

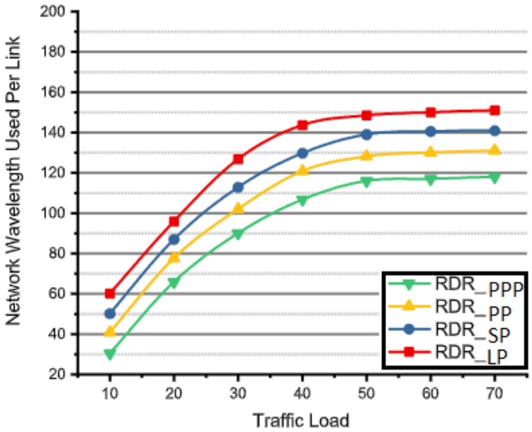


Fig. 10: Network Utilization using SPath.

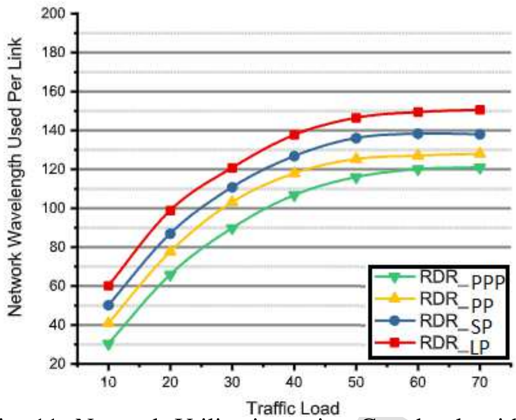


Fig. 11: Network Utilization using Greedy algorithm.

TABLE IV: Comparison of all Protection Methods based on SP and Greedy algorithm.

	LP	SP	PP	PPP
Greedy approach	Worst	Inferior	Inferior	Medium
SP approach	Inferior	Medium	Medium	Best

is a metric that shows how quickly the network can be recovered after a failure. RT is the time between when a link is disconnected from the network until the rerouted traffic reaches its destination. We summarized our results regarding the recovery time for each protection in Table II. A comparison of RT for different protection methods shows that the PPP approach has a significantly lower time to recover the system after a failure happens. Since PPP approach selects a new path that is completely disjointed from the failed link therefore the recovery time reduces. The PP, SegP, and LP methods have an increasing RT, respectively.

E. *Link Utilization and Network Utilization*

The minimum wavelength that a channel is needed to fulfill all incoming requests at a particular network traffic load is called Link Utilization (LU). While, Network Utilization (NU) is defined as the network resources are being used at a specific traffic load. The simulation results comparing the performance of Shortest Path and Greedy routing algorithms (see Figs. 8, 9, 10, and 11) show the the number of channels allocated for each network link and in other words present the wavelength utilization of each link. SPath-PPP outperforms others due to attempting to fulfill the protection requirement with the minimum number of wavelengths. As we can see, the traffic loads of less than 40 Erlangs result in an underutilized wavelength channel. On the other hand, at the higher traffic loads, the wavelength channels are fully used at each fiber. The comparison between all those figures, we see that SPath algorithm outperforms G algorithm in all four protection methods.

F. *Results Comparison*

Our comparison results for uniform traffic (see Fig. 13) showed that the PPP method performs the best in terms of reducing BP, BBP, and SPT when compared with PP, SegP, or LP methods. Table IV, present the best performance of the PPP combined with the SPath routing algorithm. The other combinations such as G-PP, G-PPP, and G-LP, G-SegP perform worse than when we use those protection methods with the SPath algorithm. Figs. 13 and 14 show that the lowest BP, SPT, and BBP belong to SP-PPP when compared with the other combinations. WDM networks transmit an extremely large data rate. Therefore due to traffic fluctuation, there will be a chance for dropping requests. In this work, we use nonuniform traffic to validate that PPP method outperforms better than other protection methods. Figure 14 shows the simulation result of four protection methods under non-uniform traffic. As we expected, we found out that the PPP method outperforms the other methods in terms of SPT, BP, BBP. Due to the nature of the SPath algorithm and characteristic of PPP method which is intrinsically flexible. Although, in case of non-uniform the average SPT and average of BP, BBP are a little bit higher than the average value under uniform traffic. PP, SegP, and LP methods show better quality in the results, respectively.

Figure 15 shows the simulation result of two different routing approaches namely Shortest Path (SPath) and Greedy (G) algorithm under three different service duration parameters (60, 300, and 1500) for non-uniform traffic. In this simulation the two protection methods which proved better network performance while utilizing RDR were compared. As we can see, in all 3 different service durations, the lowest value of SPT, BP and BBP belongs to the scenario of using SPath algorithm with PPP protection method. The reason that SPath routing is more effective than a G approach is because SPath provides a better efficient bandwidth utilization for a sequence of calls, encourages protection sharing, and uses the less links.

V. Conclusion

We examined various protection methods against the single link failure issue for optical networks under uniform and non-uniform traffic. We also evaluated the efficiency of each protection method under both uniform and non-uniform traffic, utilizing RDR method. Also, we used two different routing algorithms, namely the SPath and G method. Our simulations were done under two different topologies, namely, NSFNet and COST239. Our results show that very similar performance improvements were obtained when RDR with protection methods were used in both the topologies. Also, our results show that the PPP method performs the best in terms of reducing BP, BBP, and SPT compared with PP, LP, and SegP in both topologies while utilizing RDR.

Acknowledgments

This work was supported in part by the U.S. National Science Foundation grant (NSF CNS–1817105).
This paper appeared in the proceedings of the ICCCN2021 Conference[3].

References

[1] S. Yavary Mehr, B. Ramamurthy, Y. Zhou, B. Guo, and S. Huang, "Performance of resource delayed release strategy in software-defined OTN over WDM networks for uniform and non-uniform traffic," *Optical Switching and Networking*, vol. 44, p. 100663, 2022.

[2] 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.

[3] S. Yavary Mehr and B. Ramamurthy, "Protection techniques for wavelength division multiplexing networks using resource delayed release strategy," in *2021 International Conference on Computer Communications and Networks (ICCCN)*. IEEE, 2021, pp. 1–6.

[4] C. Lu, G. Luo, S. Wang, and L. Li, "A novel shared segment protection algorithm for multicast sessions in mesh WDM networks," *ETRI journal*, vol. 28, no. 3, pp. 329–336, 2006.

[5] P. K. Agarwal, A. Efrat, S. K. Ganjugunte, D. Hay, S. Sankararaman, and G. Zussman, "The resilience of WDM networks to probabilistic geographical failures," *IEEE/ACM Transactions on Networking*, vol. 21, no. 5, pp. 1525–1538, 2013.

[6] A. Mayoral, V. López, O. Gerstel, E. Palkopoulou, Ó. G. de Dios, and J. P. Fernández-Palacios, "Minimizing resource protection in IP over WDM networks: Multi-layer shared backup router," *Journal of Optical Communications and Networking*, vol. 7, no. 3, pp. A440–A446, 2015.

[7] T. H. Dao, "On optimal designs of transparent WDM networks with 1+1 protection leveraged by all-optical xor network coding schemes," *Optical Fiber Technology*, vol. 40, pp. 93–100, 2018.

[8] H. Saini and A. K. Garg, "Protection and restoration schemes in optical networks: a comprehensive survey," *International Journal of Microwaves Applications*, vol. 2, no. 1, 2013.

[9] M. M. A Azim and M. N. Kabir, "Availability analysis of shared backup path protection under multiple-link failure scenario in WDM networks," *Annals of Telecommunications-Annales des Télécommunications*, vol. 70, no. 5, pp. 249–262, 2015.

[10] D.-R. Din and J.-S. Huang, "Multicast backup reprovisioning problem for hamiltonian cycle-based protection on WDM networks," *Optical Fiber Technology*, vol. 20, no. 2, pp. 142–157, 2014.

[11] L. Guo, H. Yu, and L. Li, "Segment shared protection for survivable meshed WDM optical networks," *Optics Communications*, vol. 251, no. 4, pp. 328–338, 2005.

[12] N. Merayo, J. C. Aguado, P. Fernández, R. M. Lorenzo, and E. J. Abril, "Design of VNF-mapping with node protection in WDM metro networks," in *Broadband Communications, Networks, and Systems: 10th EAI International Conference, Broadnets 2019, Xi'an, China, October 27-28, 2019, Proceedings*, vol. 303. Springer, 2019, p. 285.

[13] R. Goscien, K. Walkowiak, M. Klinkowski, and J. Rak, "Protection in elastic optical networks," *IEEE Network*, vol. 29, no. 6, pp. 88–96, 2015.

[14] R. J. Pandya, "Survivable virtual topology search with impairment awareness and power economy in optical WDM networks," *International Journal of Communication Networks and Distributed Systems*, vol. 25, no. 1, pp. 1–20, 2020.

[15] X. Zhang, H. Wang, and Z. Zhang, "Survivable green IP over WDM networks against double-link failures," *Computer Networks*, vol. 59, pp. 62–76, 2014.

[16] Z. Wang, M. Zhang, D. Wang, C. Song, M. Liu, J. Li, L. Lou, and Z. Liu, "Failure prediction using machine learning and time series in optical network," *Optics Express*, vol. 25, no. 16, pp. 18 553–18 565, 2017.

[17] J. M. Simmons, "Dynamic optical networking," in *Optical Network Design and Planning*. Springer, 2014, pp. 349–399.

[18] J. Ali, G. Lee, B. Roh, D. K. Ryu, and G. Park, "Software-defined networking approaches for link failure recovery: A survey," *Sustainability*, vol. 12, no. 10, p. 4255, 2020.

[19] Y. Li, Y. Zhao, J. Zhang, G. Gao, X. Yu, H. Chen, C. Yu, Q. Zhou, J. Mi, R. Jing, J. Li, and C. Zhang, "First field trial of virtual network operator oriented network on demand (NoD) service provisioning over software defined multi-domain optical networks with multi-vendor OTN equipment," in *Asia Communications and Photonics Conference 2015*. Optical Society of America, 2015, p. AM4A.6.

[20] M. Garrich, A. Bravalheri, M. Magalhaes, M. Svolenski, X. Wang, Y. Fei, A. Fumagalli, D. Careglio, J. Solé-Pareta, and J. Oliveira, "Demonstration of dynamic traffic allocation in an SDN-enabled metropolitan optical network test-bed," in *International Conference on Optical Network Design and Modeling*, May 2016, pp. 1–6.

[21] T. Szyrkowiec, M. Santuari, M. Chamania, D. Siracusa, A. Autenrieth, V. Lopez, J. Cho, and W. Kellerer, "Automatic intent-based secure service creation through a multilayer SDN network orchestration," *J. Opt. Commun. Netw.*, vol. 10, no. 4, pp. 289–297, Apr 2018. [Online]. Available: http://jocn.osa.org/abstract.cfm?URI=jocn-10-4-289

[22] S. Yuan, J. P. Jue *et al.*, "Shared protection routing algorithm for optical network," *Optical Networks Magazine*, vol. 3, no. 3, pp. 32–39, 2002.

[23] D. B. A. Teixeira, C. T. Batista, A. J. F. Cardoso, and J. d. S Araújo, "A genetic algorithm approach for static routing and wavelength assignment in all-optical wdm networks," in *EPIA Conference on Artificial Intelligence*. Springer, 2017, pp. 421–432.

[24] 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.

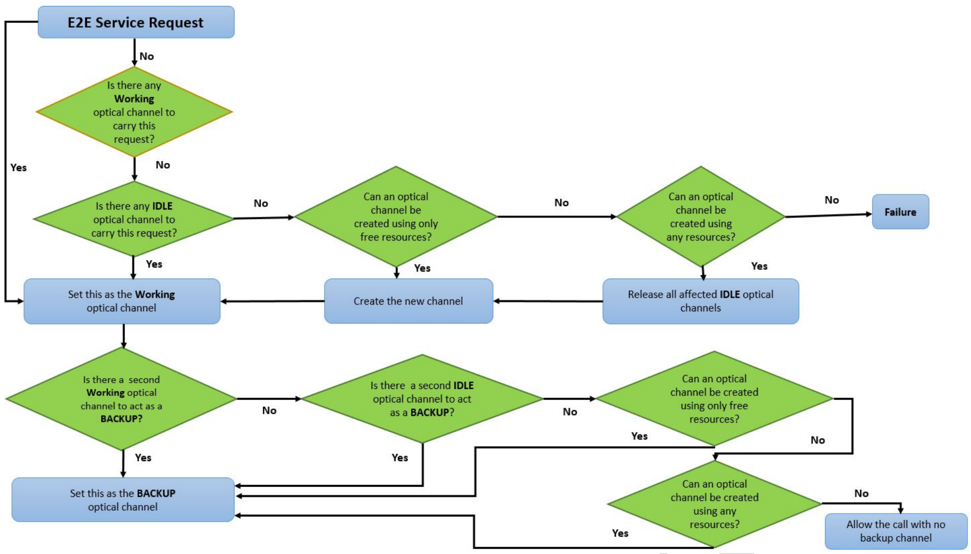


Fig. 12: Typical workflow of RDR strategy with the backup protection.

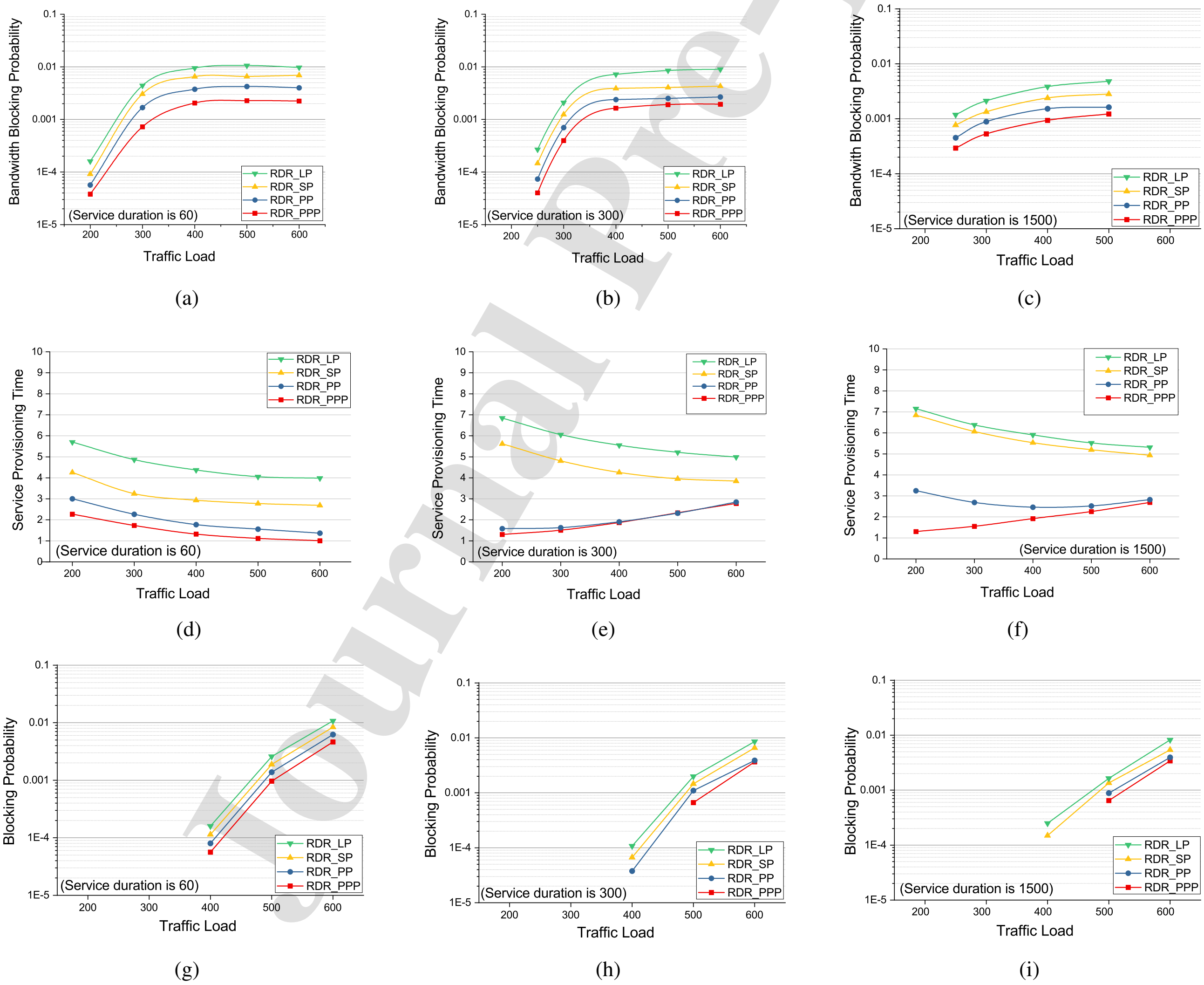


Fig. 13: SPT, BBP, and BP comparison under uniform traffic with service duration of 60, 300 and 1500.

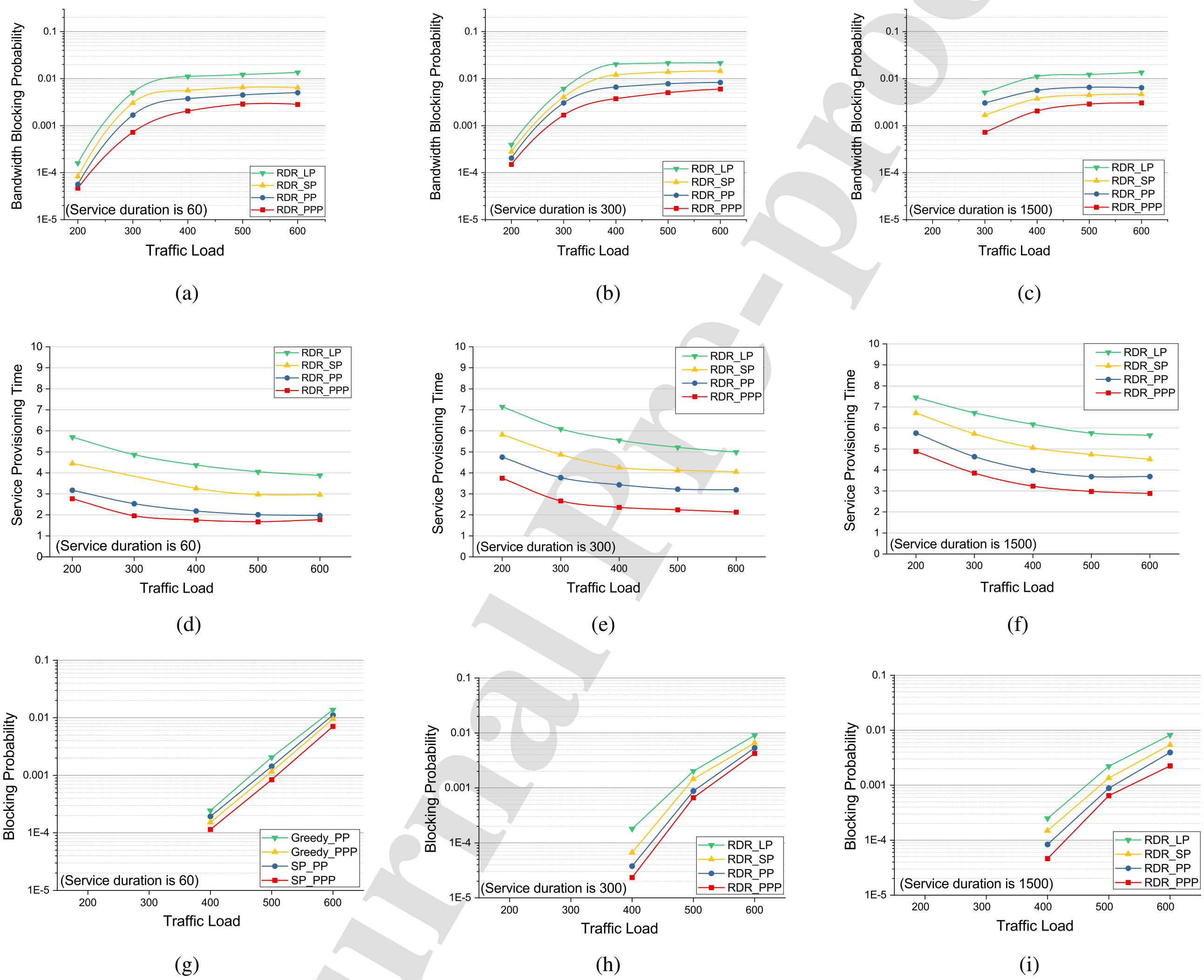


Fig. 14: SPT, BBP, and BP comparison under non-uniform traffic with service duration of 60, 300 and 1500.

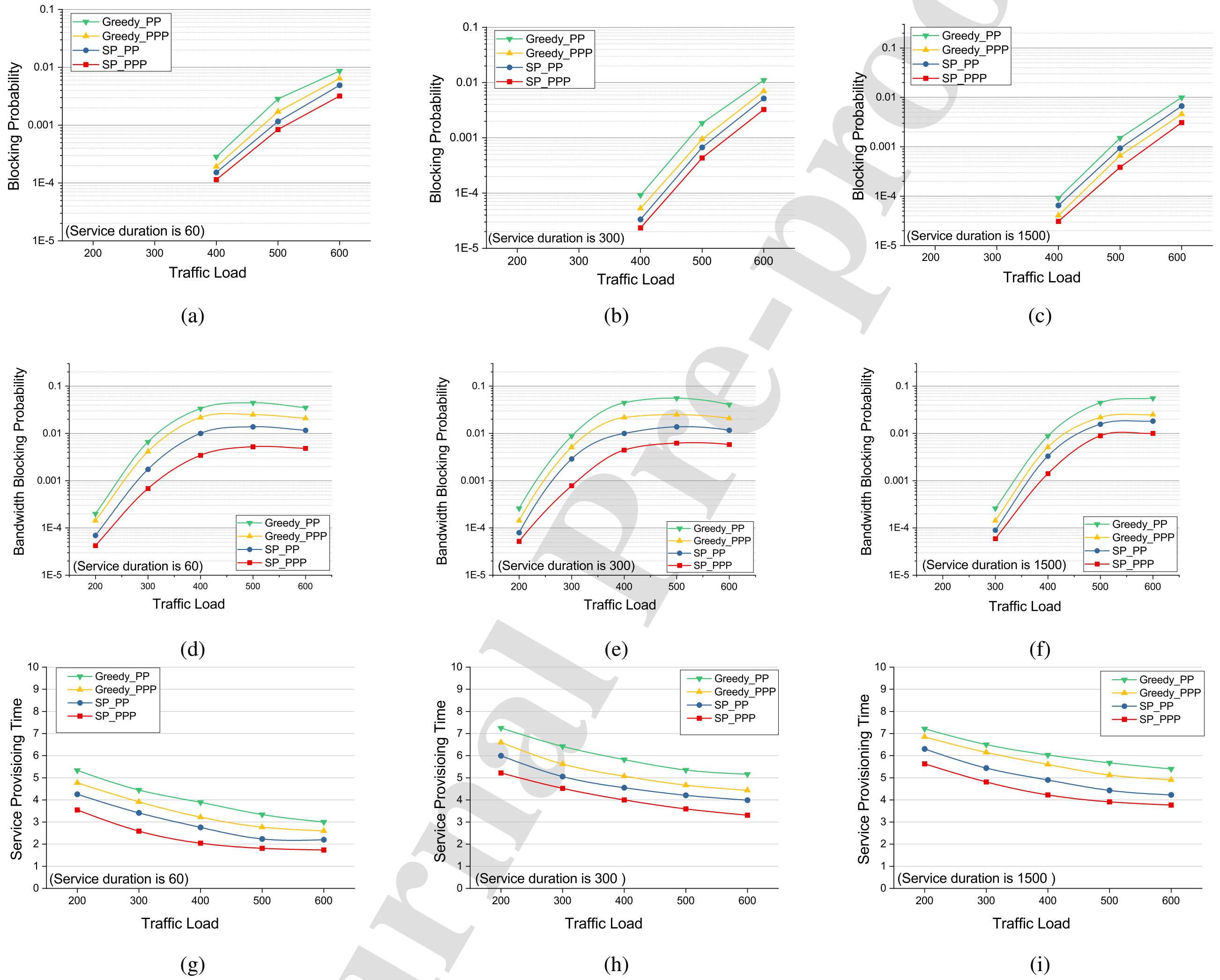


Fig. 15: Comparing BP, BBP, and SPT using two different routing algorithm, Greedy method and Shortest Path method under different service durations.

June,21, 2023

Declaration of interests

☐ The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

☒ The authors declare the following financial interests/personal relationships which may be considered as potential competing interests:

Byrav Rammaurthy reports financial support was provided by National Science Foundation.

We confirm that this work is not currently under consideration for publication elsewhere. And there is no conflict of interest.

Sincerely,

Shideh Yavary Mehr
Computer Science,
University of Wisconsin-Milwakuee,
E338, EMS building,
2200 E Kenwood Blvd
Milwakuee, WI 53211
USA