IOSR Journal of Engineering (IOSRJEN)
e-ISSN: 2250-3021, **p**-ISSN: 2278-8719
Vol. 3, Issue 4 (April. 2013), ||V3 || PP 41-48

Robust Algorithms for wdm Mesh Networks

C.Janani[1], S.Sarala[2], Assistant professor R.Augastiny[3],
[1, 2, 3] Sri Manakula Vinayagar Engineering College, Department of ECE, Madagadipet, Puducherry, India.

Abstract: Excess capacity (EC) is the unused capacity in a network. We propose EC management techniques to improve network performance. Our techniques exploit the EC in two ways. First, a connection preprovisioning algorithm is used to reduce the connection setup time. Second, we use protection schemes that have higher availability and shorter protection switching time. Specifically, depending on the amount of EC available in the network, our proposed EC management techniques dynamically migrate connections between high-availability, high-backup-capacity protection schemes and low-availability, low-backup-capacity protection schemes. Thus, multiple protection schemes can coexist in the network. The four EC management techniques studied in this paper differ in two respects: when the connections are migrated from one protection scheme to another. Specifically, Lazy techniques migrate connections only when necessary, whereas Proactive techniques migrate connections to free up capacity in advance. Partial Backup Reprovisioning (PBR) techniques try to migrate a minimal set of connections, whereas Global Backup Reprovisioning (GBR) techniques migrate all connections. We develop integer linear program (ILP) formulations and heuristic algorithms for the EC management techniques improve the network performance by exploiting the EC in wavelength-division-multiplexing (WDM) mesh networks.

Keywords: *Availability,excesscapacity(EC),protection,reprovisioning,robustness,wavelength-division-ultiplexing (WDM).*

I. INTRODUCTION

In an optical network employing wavelength-division multiplexing (WDM), the failure of a single fiber link may lead to tremendous data loss since a single fiber link can carry a huge amount of data (on the order of terabits per second). A path that carries traffic during normal operation is known as a primary path. When a working path fails, the lightpath is rerouted over a backup path. In a connection-oriented mesh network such as a telecom backbone network, a traffic demand is typically satisfied by provisioning a primary path, and higher service availability is provided by provisioning a backup path to protect the resources used in the primary path. The network resource utilization varies both spatially and temporally as new connections are set up and existing connections terminate. Hence, at any given time, the network has some unused capacity, which is called excess capacity (EC). Excess capacity management techniques exploit the EC to improve the network performance. Connection setup time, protection switching time, and availability are three important network performance metrics. Connection setup time (ST) is the time required for provisioning a primary path and one or more backup paths upon receiving a connection request. During operation, if a link or a node along the primary path fails, the connection switches to a backup path. The time required to switch from the primary path to the backup path is called protection switching time (PST). Finally, availability of a connection is defined as the ratio between the duration for which the connection is available (i.e., the connection is carrying traffic) and the connection holding time. Some existing protection schemes (e.g., dedicated protection) offer short PST and high availability, but suffer under high-volume traffic. Some others (e.g., shared protection) can more efficiently exploit EC under high load by sacrificing availability and offering longer PST. EC utilization can be optimized using different protection schemes according to the amount of available EC.EC is exploited to increase connections' availabilities by adding more backup capacity to existing connections, but no other quality metrics, such as PST or ST are considered. an EC management scheme was proposed that allows sharing capacity among connections in path oriented differentiated servicesnetworks.EC management techniques are proposed that exploit EC to improve all the three above-mentioned performance metrics. Specifically, our contribution is twofold. First, we present a connection preprovisioning algorithm that decreases the connection setup time by reserving capacity, whenever possible, for primary and backup paths in advance. Second, we present four mixed-protection schemes that exploit EC to improve protection switching time and availability. Our proposed EC management techniques differ in two respects: when connections are migrated from one protection scheme to another, and which connections are migrated. Specifically, Lazy techniques migrate connections only when necessary, whereas Proactive techniques migrate connections in advance to free up capacity. Partial Backup Reprovisioning (PBR) techniques try to migrate a subset of connections, whereas Global Backup Reprovisioning (GBR) techniques migrate all connections.

II. EXISTING WORK

1. Protection Schemes in WDM Mesh Networks

Protection schemes can be generally divided into two categories based on the resource that is being protected: path protection and link protection. In path protection, a link-disjoint or node-disjoint backup path is reserved during connection setup. The connection can switch to the backup path if a link or node on the primary path fails. Link protection schemes require reserving a backup path for each link on the primary path during connection setup. When a failure occurs on a link of the primary path, data is rerouted along the backup path of the failed link. Based on the above classifications, there are four types of protection schemes: Dedicated Link Protection (DLP), Dedicated Path Protection (DPP), Shared Link Protection (SLP), and Shared Path Protection (SPP). Ideally, a protection scheme should provide high availability, short setup time (of primary and backup paths), and short protection switching time (from primary to backup) in case of failure.

1.1 Path protection/restoration:

In path protection, backup resources are reserved during connection setup, while in path restoration; backup routes are discovered dynamically after the link failure. When a link fails 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 in Fig.1.

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.

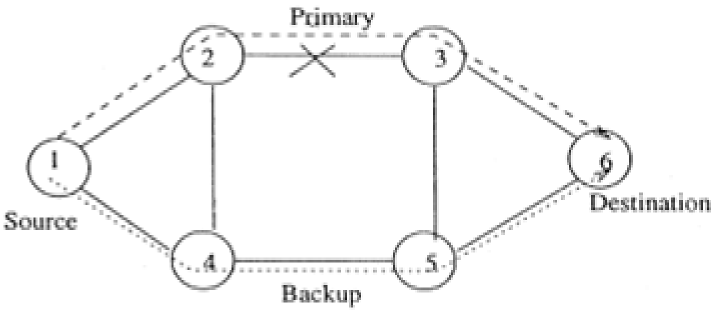

Fig 1: Path Protection

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.

1.2 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 all the connections that traverse the failed link are rerouted around that link, and the source and destination nodes of the connections are oblivious to the link failure in Fig.2.

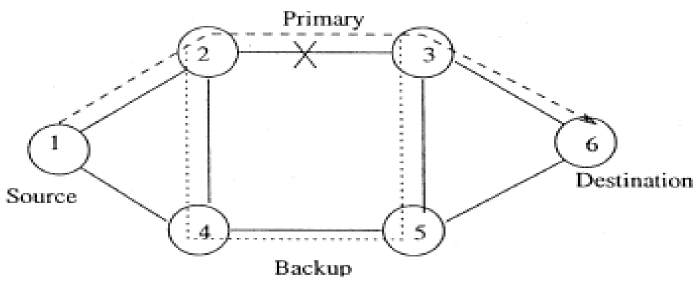

Fig 2: Link protection

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: In shared-link protection, the backup resources reserved along the 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-link protection is more capacity-efficient when compared with dedicated Link protection.

2. Backup Reprovisioning

Network state changes every time one of the following events occurs : 1) a new request arrives; 2) an existing connection terminates; 3) a network failure occurs; or 4) a failed link/node is repaired; 5) when the network is upgraded. Backup resources are usually provisioned when primary resources are established. However, the initially provisioned backup resources may not be optimal under the changed network state. Thus, reprovisioning of backup resources may be needed. Some approaches consider reprovisioning both primary and backup paths some only consider reprovisioning backup paths (e.g., some propose periodic backup reprovisioning and some are event driven .In our approach, we take only event-driven backup reprovisioning into consideration since primary path reprovisioning and periodic reprovisioning may cause unnecessary interruption to traffic on existing connections. Therefore, in the rest of this paper, reprovisioning refers to "backup reprovisioning".

III. EXPLOITING EXCESS CAPACITY MANAGEMENT

Connections arrive, hold for a while, and terminate, so the traffic load and the amount of EC fluctuate. Protecting connections with a high-availability protection scheme might be problematic because, when traffic increases, the network resources might soon get exhausted due to high capacity requirement. Reprovisioning of backup resources of connections (or a subset of connections) by using a more capacity-efficient protection scheme helps to solve this problem. This kind of reprovisioning will free some EC in the network and allow us to protect new connections using high-availability protection scheme. When there is a large amount of EC, DLP is the best option in terms of availability and PST. When there are not enough resources to protect new connections with DLP, the backup resources of connections can be reprovisioned by DPP, which is more resource efficient than DLP and can still provide high availability and PST, to create some EC for new connections. As traffic increases, some connections might still be rejected because of lack of capacity or because reprovisioning using DPP might not be feasible. In this case, backup resources can be reprovisioned by using an even more resource efficient protection scheme, e.g., SLP. Note that SPP requires less capacity than DPP and DLP, but SLP's PST and availability performance are better than SPP, so we prefer SLP for the second round of reprovisioning.
Each connection is set up with DLP. However, connections might experience DPP-reprovisioning, or SLP-reprovisioning, or both. EC can be managed efficiently by using such reprovisioning mechanism. Our EC management approach will provide DLP protection to connections as long as possible and high QoS (high availability, short PST) is expected. However, the long setup time of DLP has to be solved. Fortunately, by exploiting the EC in the network with a preprovisioning algorithm, we can overcome this limitation of DLP. EC management problem is dynamic. However, two static mechanisms, preprovisioning and backup reprovisioning, are rerun to manage the EC.

1. Preprovisioning Algorithm

Preprovisioning is a mechanism that reserves dedicated-link protected wavelengths on each link, as much as possible, for future connection requests. Since, by using preprovisioning, there is no need to provision/configure backup path capacity for DLP. The main drawback of DLP namely, long connection setup time is overcome.

Algorithm 1: Preprovisioning

i. Update cost of the links: C(e)=W(e)-F(e) if F(e)=0,then C(e)=∞ and add infinite-cost links to Ls.
ii. Take the maximum-cost link e (where € Ls) and choose a free wavelength *w* on e.
iii. Compute a backup path *b* for wavelength w on e with two-step algorithm by using cost function C(e).
iv. If no backup path is found, add e into Ls and go to step 5.
v. Reserve capacity for backup path *b* and configure OXCs on *b*.
vi. If | Ls| = |E| , go to next step , otherwise go to step 1.
vii. Update cost of the links: C(e)=W(e)-R(e) if R(e)=0,then C(e)=∞.

Provisioning Process: When a connection request arrives, the shortest-path algorithm, based on the updated link costs computed at Step 6 of Algorithm 1, returns a path formed by a sequence of protected wavelengths on each link. When the connection is set up on this path, there is no need to configure backup paths for DLP because any reserved wavelength on each link has a preconfigured backup path due to preprovisioning. Thus, the setup time of connections will be equal to setup time of primary path. The preprovisioning algorithm is executed: 1) When a connection terminates since some occupied capacity gets freed.2) When a failure occurs since some reserved resources on the failed link are not accessible. 3) When a failed link is repaired. The costs of links are updated after a connection is established.

2. EC-Aware Backup Reprovisioning

The backup reprovisioning techniques in aim to optimize backup resources without changing the protection scheme. In our approach, backup reprovisioning does not only optimize backup resources, but also migrates connections to amore resource-efficient protection. The EC-aware backup reprovisioning problem can be split into three sub problems: When to Reprovision: Lazy and Proactive Approaches: The optimal solution to the "when to reprovision" is a complex scheduling problem, and it would which is not feasible for dynamic traffic. Here, we propose two approaches: Reprovisioning can be triggered:1)When a connection request arrives (by checking if there is enough capacity to protect connection with DLP).2) After the connection is established (by reorganizing the EC for future connection requests). We call the two approaches as Lazy and Proactive, respectively.

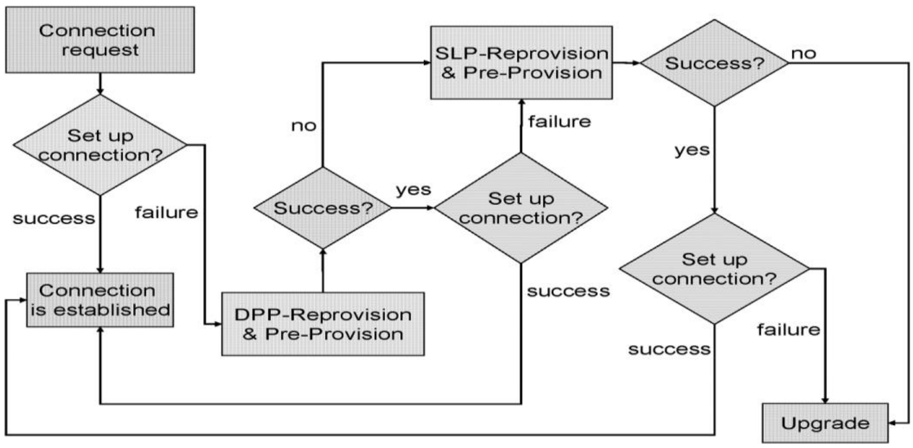

Fig 3: Lazy Approach

Lazy approach: After the cost update at the end of the preprovisioning, the infinite-cost links indicate that there are not reserved wavelengths for a primary path of a new connection. If the cost of the shortest path of a connection request is infinity, EC needs to be increased (by reprovisioning) to accommodate the new connection with DLP as shown in Fig.3. The disadvantage of Lazy approach is that a connection that triggers reprovisioning is setup only after the completion of reprovision(s). EC management techniques differ in two respects: when connections are migrated from one protection scheme to another, and which connections are migrated. Specifically, Lazy techniques migrate connections only when necessary.

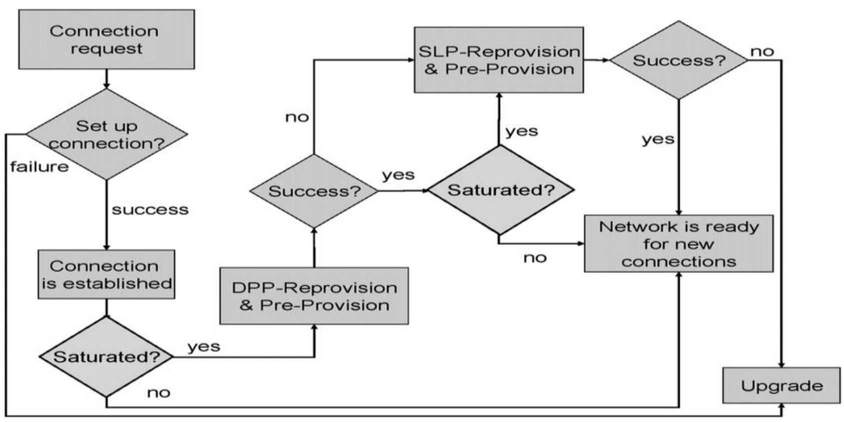

Fig 4: Proactive Approach

Proactive approach: In the Proactive approach, reprovisionings are performed before a connection request faces capacity exhaustion. The admission process of a connection for the Proactive approach. When a connection request arrives, a primary path can be found and the connection is established . After the establishment of the connection, the network is checked if any updated link cost is infinity (link costs are updated in the prereprovision process based on the number of wavelengths on the link that are reserved for primary resources). If this is the case, the network is flagged as "saturated," and reprovisioning is performed to free some EC. The definition of "saturated network" might be a very strict condition and may cause frequent, early, and possibly unnecessary upgrade. Thus, we relax the definition by saying "if more than percent of the links' updated costs are infinity, then the network is saturated."β is the saturation threshold and has to be a reasonably small percentage. Another important advantage of Proactive over Lazy is that reprovisioning does not affect the setup time. However, the main drawback of Proactive is its complexity since each link of the topology has to be continuously monitored to decide if reprovisioning is needed.
What to Reprovision: GBR versus PBR. GBR reprovisions all the connections' backup resources, while EBR reprovisions only a subset of connections, namely those that are "vulnerable", i.e., it must be reprovisioned to avoid service interruption. We propose Partial Backup Reprovisioning (PBR), which reprovisions only those connections protected by DLP for DPP-reprovisioning and the connections protected by DLP or DPP for SLP-reprovisioning. For GBR, all connections' backup resources are reprovisioned.
How to Reprovision: ILP Formulations and Heuristics: The objective of the reprovisioning phase is to achieve effective capacity utilization so that the amount of EC freed after reprovisioning is maximized.

Algorithm2: Backup Reprovisioning algorithm

i. Identify the set of connections whose backup resources are to be reprovisioned (T_{rp}) and randomly Generate | K| sequences.
ii. Take sequence k in K.
iii. Take connection t in k and discover the backup path(s) with two step algorithm [4] by using cost function C(e).
iv. If a finite-cost backup path is found, go to step 5. Otherwise set the capacity requirement of sequence to infinity, add k to k', and go to step 8.
v. Provision the backup path and add t to T'_{rp}
vi. If $|T'_{rp}| < |T_{rp}|$,take the next connection in the sequence and go to step 3, otherwise go to step 7.
vii. Compute the capacity requirement for sequence k and add k to k' and empty T'_{rp}.

If |K'| < |K| , take the next sequence in K and go to step 2, otherwise find the sequence in K that requires minimum finite capacity and reprovision backup resources of connection in that sequence. If there is not finite-capacity-required sequence, reprovisioning fails.

IV. SIMULATION ANALYSIS

We simulate the Lazy and Proactive approaches with reprovisioning by using the heuristics for all traffic profiles. We also simulate single-protection-scheme approaches: DPP-provision and SLP-provision, which also perform reprovisioning when capacity exhaustion occurs. Lazy-GBR, Proactive-GBR, and single-protection schemes are also studied using ILP. Obviously, reprovisioning of connections gives our approaches a certain advantage. For a fair comparison, we also allow DPP- and SLP-provision approaches backup reprovisioning when there is not enough capacity to provision either primary path or backup path(s).

1. Lazy Versus Proactive and GBR versus PBR

***A) Average Fraction of Time a Connection is protected by Different Protection Schemes*:** In both Lazy and Proactive approaches, each connection is established with DLP. However, due to network capacity exhaustion, connections might experience DPP and/or SLP protection. For all traffic profiles and for both GBR and PBR, Proactive enables the utilization of DLP for a shorter time than Lazy since early reprovisioning is applied to avoid blocking connections and/or long setup times in Fig.5. Similarly, connections that are protected by DPP face SLP-reprovisioning earlier in Proactive than in Lazy. The frequency of reprovisioning in Proactive is higher than in Lazy.

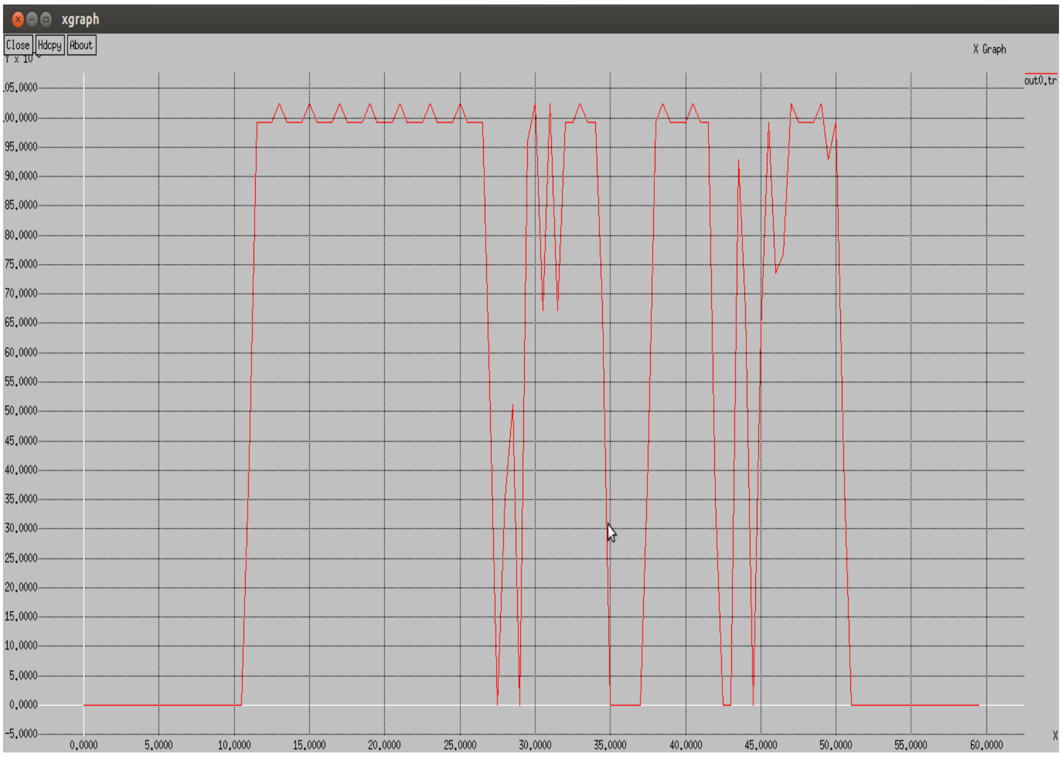

Fig 5: Lazy Approach

The main results from the comparison between GBR and PBR are as follows:

1) The average time durations for which a connection is protected by DLP in both approaches are very close.
2) PBR maintains DPP longer than GBR.
3) PBR provides more frequent reprovisioning than GBR. The main advantage of PBR, when there are SLP and DLP connections, is that it only DPP reprovisions the DLP connections, and not those DPP and SLP. After DPP reprovisioning, there are DPP and SLP connections. On the contrary, GBR attempts to reprovision all connections with DPP and, if it fails, all connections are reprovisioned by SLP. In this case, sharing in GBR is more than in PBR, which affects availability and PST.

B) Availability: Increasing sharing reduces availability more than having long backup paths. Reprovisioning also affects availability since reprovisioning backup paths makes them shorter in Fig.6. Traffic profiles in which Lazy or Proactive do not introduce SLP reprovisioning. However, for low-volume traffic, PBR provides higher availability than GBR since PBR keeps connections protected by DPP more than GBR.

C) Protection Switching Time (PST) and Setup Time (ST): PSTs of our approaches are close to average PST. However, in Lazy, those (few) requests that trigger reprovisioning are established only after reprovisioning(s) is completed, so that their STs are higher. Note that, in Proactive, connections do not trigger reprovisioning. . We simulate the Lazy and Proactive approaches with both GBR and PBR reprovisioning by using the heuristics for all traffic profiles. We also simulate single-protection-scheme approaches: DPP-provision and SLP-provision, which also perform reprovisioning when capacity exhaustion occurs. Lazy- GBR, Proactive-GBR, and single protection schemes are also studied using ILP. The following sections are organized as follows. A comparison between the proposed approaches and the traditional approaches are made in terms of metrics such as availability, PST, and ST. Connection setup time, protection switching time, and availability are three important network performance metrics. Connection setup time (ST) is the time required for provisioning a primary path and one or more backup paths upon receiving a connection request. During operation, if a link or a node along the primary path fails, the connection switches to a backup path. The time required to switch from the primary path to the backup path is called protection switching time (PST). Finally, availability of a connection is defined as the ratio between the duration for which the connection is available (i.e., the connection is carrying traffic) and the connection holding time. Specifically, Lazy techniques migrate connections only when necessary, whereas Proactive techniques migrate connections in advance to free up capacity. Partial Backup Reprovisioning (PBR) techniques try to migrate a subset of connections, whereas Global Backup Reprovisioning (GBR) techniques migrate all connections.

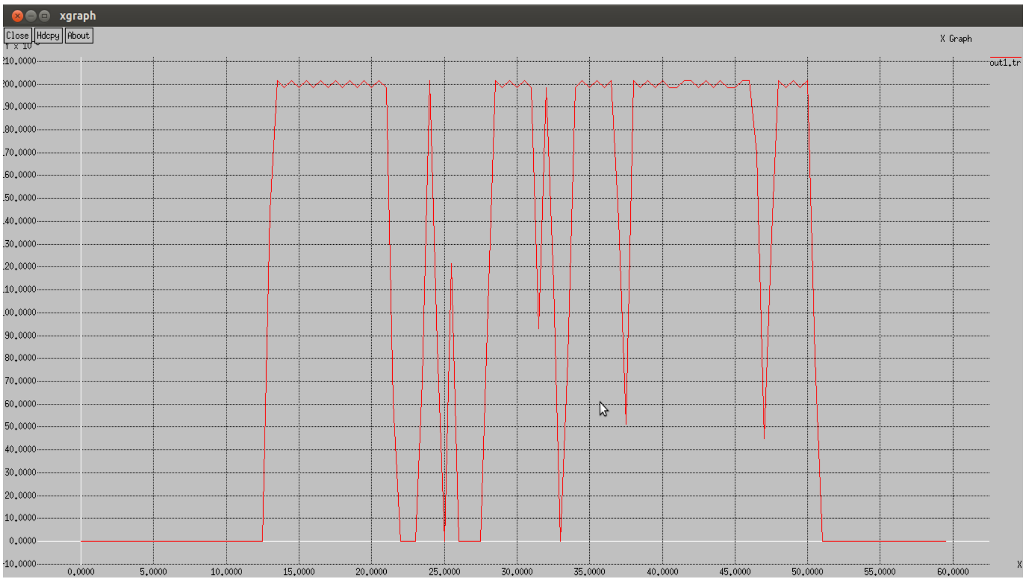

Fig 6: Proactive Approach

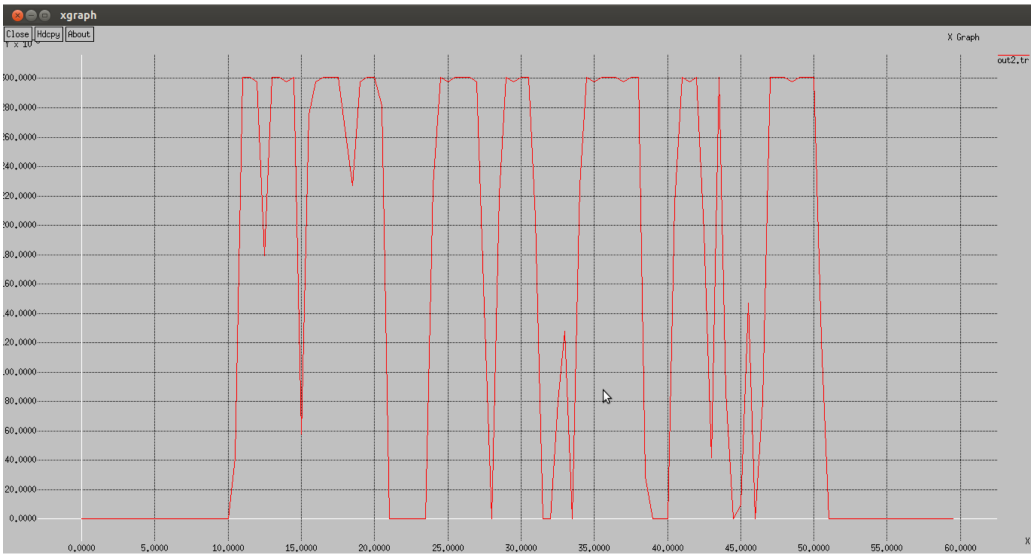

Fig 7: Global Backup Reprovisioning (GBR)

2. Mixed Protection versus Single Protection

The proposed approaches are (Lazy-GBR, Lazy-PBR, Proactive-GBR, and Proactive-PBR) are first compared to traditional protection schemes such as DPP-provision and SLP-provision. We also compare to DLP provision because network resources would get exhausted quickly and results would not be very meaningful. Obviously, reprovisioning of connections gives our approaches a certain advantage. For a fair comparison, we also allow DPP- and SLP-provision approaches backup reprovisioning when there is not enough capacity to provision either primary path or backup path(s) in Fig .7. Also, we call our approaches “mixed-protection” and traditional approaches as “single-protection.”

A) Availability: For availability comparison, we take *Lazy-PBR* as a representative of mixed approaches since the availability results of the mixed approaches are very close to each other. The availability results for *Lazy-PBR*, DPP-provision, and SLP-provision approaches. Mixed protection approaches provide higher availability than SLP-provision for all traffic profiles and are also higher than DPP-provision for the first four traffic profiles in which neither of the mixed-protection approaches introduce SLP reprovisioning. However, because of increasing sharing, the mixed approach reduces the availability such that DPP provision provides higher availability in Fig.8. For heavy traffic, when it is not possible to provide DPP to every connection. Lazy-PBR works well and provides more availability, which is higher than that provided by SLP provision.

B) Protection Switching Time (PST): The PSTs of the Mixed-protection approaches are very close to one another. Thus, we take their average and compare to single protection approaches. Mixed-protection approaches provide shorter PST since some of the connections are protected by DLP.

C) Connection Setup Time (ST): The traffic volume does not significantly affect ST. Even though some connections are protected by DLP in mixed-protection approaches, the preprovisioning algorithm reduces the setup time significantly. In both mixed protection and SLP-provision, setup time is equal to time to provision primary path because, in both approaches, backup paths do not need to be configured.

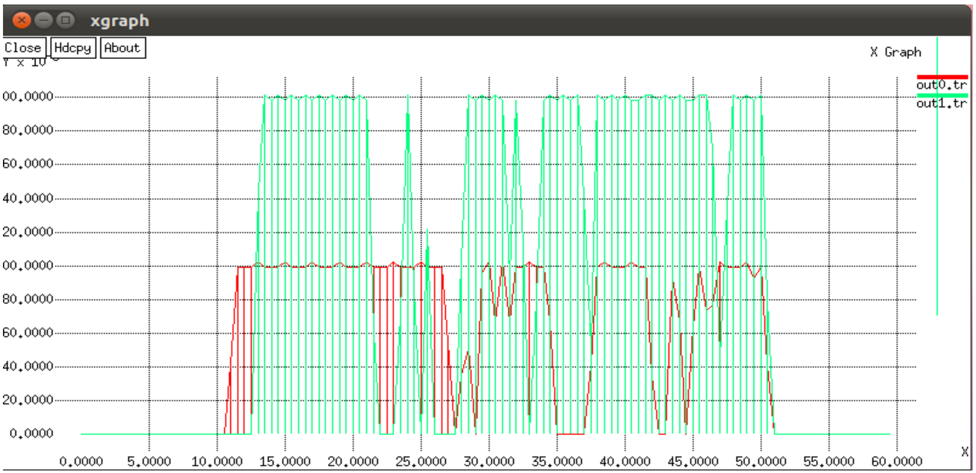

Fig 8: Comparison of Lazy and Proactive

V. CONCLUSION

The capacity utilization in a network may fluctuate in time. When the traffic load is low, excess capacity can be exploited to provide better services to customers. When plenty of excess capacity is available, protecting connections with Dedicated Link Protection (DLP) is advisable because of its shortest protection switching time and highest availability compared to other protection schemes. Two main limitations of DLP are: 1) high capacity requirement 2) long setup time. Our results show that our approaches have best performance in terms of availability when the traffic volume is low and in terms of short PST and ST (by preprovisioning) for any traffic volume. Even when our approaches do not show better performance than dedicated protection, they can be deployed when dedicated protection cannot. When to reprovision: Lazy shows better performance than Proactive in terms of availability by having a few connections suffer longer setup because of reprovisioning. What to reprovision: PBR provides higher availability than GBR while GBR is more resource-efficient. How to reprovision: Our proposed heuristics provides very close performance results to ILP in a time-efficient way. Hence, Lazy-PBR-Heuristic is a good choice for reprovisioning among the proposed solutions in order to obtain high availability, short ST, and short PST.

REFERENCES

[1]. F. Dikbiyik, L. Sahasrabuddhe, M. Tornatore, and B. Mukherjee,"Exploiting excess capacity for improved robustness in optical WDM backbone mesh networks," in Proc. OFC, San Diego, CA, Mar. 2011 pp. 1–3.

[2]. L. Song, J. Zhang, and B. Mukherjee, "A comprehensive study on backup-bandwidth reprovisioning after network-state updates in survivable telecom mesh networks," IEEE/ACM Trans. Netw., vol. 16, no. 6, pp. 1366–1377, Dec. 2008.

[3]. M. Batayneh, S. Rai, S. Sarkar, and B. Mukherjee, "Efficient management of a telecom network's excess capacity: A traffic-engineering approach," in Proc. ECOC, Berlin, Germany, Sep. 2007, pp.1–2.

[4]. B. Mukherjee, Optical WDM Networks. New York: Springer, 2006.

[5]. Y. Cheng and W. Zhuang, "Dynamic inter-SLA resource sharing in path-oriented differentiated services networks," IEEE/ACM Trans. Netw., vol. 14, no. 3, pp. 657–670, Jun. 2006.

[6]. J. Zhang,K. Zhu, and B.Mukherjee, "Backup reprovisioning to remedy the effect of multiple link failures in WDM mesh networks," IEEE J. Sel. Areas Commun., vol. 24, no. 8, pt. Supplement, pp. 57–67, Aug. 2006.

[7]. S. Ramamurthy, L. Sahasrabuddhe, and B. Mukherjee, "Survivable WDMmesh networks," J. Lightw. Technol., vol. 21, no. 4, pp. 870–883, Apr. 2003.