Photon Netw Commun
DOI 10.1007/s11107-011-0323-1

Application-aware protection in DWDM optical networks

Hamza Drid · Nasir Ghani · Bernard Cousin

Received: 27 April 2011 / Accepted: 21 June 2011
© Springer Science+Business Media, LLC 2011

Abstract Fast recovery time and reduced resource utilization are the two main criteria for determining the quality of survivability mechanism. Now, it is well known that link-based protection and path-based protection provide, respectively, a short recovery time and reduced use of resources. To benefit from the both of these saliencies, we propose in this paper to use these mechanisms simultaneously. Indeed, demands mandating shorter recovery time will be protected using link-based protection. Meanwhile, other demands (e.g., no-critical) will be protected using path-based protection. Simulation results show that the proposed solution achieves a good trade-off between resource utilization and recovery time.

Keywords Protection · Survivability · Link-based protection · Path-based protection · Optical network

1 Introduction

Survivability means that the network has the ability to maintain acceptable levels of service even after an occurrence of failures within the network. Now, given the ever-increasing speed of modern optical *dense wavelength division multiplexing* (DWDM) backbones, failure events lasting few seconds may cause massive losses, i.e., both in terms of data volumes and ensuing revenue declines. Therefore, it is crucial to develop rapid survivability mechanisms that work to minimize the level of damage. Furthermore, given that the number of wavelengths channels may be limited in most DWDM networks (and new fiber build-outs are timely and costly), related survivability mechanisms should also minimize their overall resources usages. As a result, these two criteria—fast recovery and resource minimization—form the key objectives for ascertaining the quality of survivability mechanisms in this effort.

Now, most optical network survivability schemes can generally be classified into one of two key categories, protection [1] or restoration [2]. Namely, restoration is a reactive approach in which a backup light path connection is searched and established *after* a failure on the primary light path occurs. Meanwhile, protection is a pro-active approach in which the backup light path is *pre-reserved*, i.e., at the same time with the working light path setup. Hence, these mechanisms can guarantees full recovery whereas restoration schemes cannot. Overall, since failures may result in large losses, protection schemes are generally favored in optical DWDM networks.

To date, various protection mechanisms have been studied for DWDM networks, including link-based [3] and path-based protection [4]. Namely, link-based protection provides a backup for each link of a primary light path (cf. Fig. 1). Hence, upon failure of a link, the end nodes of the failed link activate the backup path and reroute the traffic around the failed link.

Meanwhile, in path-based protection, only one backup light path is computed to protect all links in the primary light path (cf. Fig. 2). Hence, when a link fails here, notification messages are sent to the source and destination nodes

H. Drid (✉) · B. Cousin
University of Rennes I-IRISA, Campus universitaire de Beaulieu,
35042 Rennes, France
e-mail: hdrid@irisa.fr

B. Cousin
e-mail: bcousin@irisa.fr

N. Ghani
ECE Department, University of New Mexico,
Albuquerque, NM 87111, USA
e-mail: nghani@ece.unm.edu

Published online: 08 July 2011

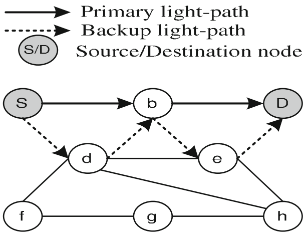

Fig. 1 Link-based protection

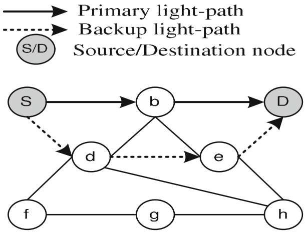

Fig. 2 Path-based protection

in order to activate and reroute the traffic on the backup light path, i.e., switchovers.

From the above, it is noted that path-based protection is usually more efficient in terms of capacity utilization, as compared with the link-based protection, i.e., since only one backup light path is required to protect all links in the primary light path. Indeed, many studies have already shown this result [5]. In addition, path-based approach can also protect all nodes in the primary light path, except the source and destination nodes. In contrast, link-based protection is generally more resource intensive and only provides "localized" protection. However, at the same time, this approach gives much faster recovery times, i.e., since only the two end-point nodes of the failed link are involved in the recovery switchover.

In order to leverage the saliencies of both link- and path-based protection mechanisms, in this effort we propose to use them simultaneously. Specifically, the exact choice of protection mechanism will be made according to the user application demand requirements. Namely, demands requiring very fast recovery times will be provisioned with link-based protection, whereas other demands will be protected using path-based strategies. Overall, this "joint" solution tries to achieve an acceptable trade-off between two competing objectives, i.e., minimizing backup resource efficiencies and minimizing recovery timescales.

Overall, this paper is organized as follows: First, Sects. 2 and 3 present our motivations and the description of our heuristic scheme, respectively. Next, Sect. 4 studies the performance of the scheme using network simulation. Finally, conclusions and directions for future work are presented in Sect. 5.

2 Motivation

In this section, we describe the key motivation of our approach. Specifically, the requirement needs of some of today's applications are analyzed, and then the main guidelines of our heuristic are introduced to meet those requirements.

Over the past years, the variety and number of high-bandwidth network applications has grown significantly. For some applications, a failure in network connectivity can disrupt a mission-critical transaction, which in turn can even be catastrophic, e.g., remote instrument operation, tele-medicine/surgery, etc. In general, these applications are classified here as "real-time" applications and are characterized by hard real-time requirements, e.g., guaranteed bandwidth, very low delay, minimal loss. Meanwhile, there are also various other applications that can tolerate a certain amount of time delay, as long as loss behaviors do not occur, e.g., such as e-mail, chat applications, remote backup/storage, etc. Furthermore, application demands can also be classified based upon their nature, e.g., critical and no-critical. Here, the former types require very short recovery times, whereas the latter types can generally suffice with somewhat more latent recovery.

Using these above classifications, we now propose a novel heuristic-based solution for protecting critical demands using link protection. As a result, the associated recovery times here will be significantly reduced here. Meanwhile, demands with less stringent requirements will be protected using path protection, thereby providing an improved level of resource efficiency in the network.

3 Heuristic scheme

The proposed "application-aware" protection scheme is now presented here.

3.1 Network model

Consider the requisite notation first. The DWDM optical network is modeled as an undirected graph $G = (V, E)$, in which each *optical cross-connect* (OXC) node $v \in V$ represents an optical switch and each edge $e \in E$ represents a network link. Here, all links are assumed to be bi-directional and also contain W available wavelengths. Furthermore, is assumed that each user demand requires one optical light path connection across the network, albeit this can readily be generalized to handle multiple wavelengths as well. Finally, it is also assumed that each OXC node has full wavelength conversion capability, thereby precluding the further consideration of wavelength selection in this current effort. Now, before presenting the details of the heuristic scheme, some additional variables are also introduced as follows:

C_i: Cost of link j; it depends of physical length, installation cost, etc.

Cr_j: Current cost of link j given as follows:

$$Cr_j = \begin{cases} \frac{W-F_j}{W} + C_i & \text{if } F_j > 0 \\ \infty & \text{otherwise} \end{cases}$$

F_j: Number of available wavelengths on link j

B_j: Number of backup wavelengths on link j

D_n: Demand number n

Using the above, the proposed scheme implements the following set of steps:

- **Step 1**: Loop and wait for demand arrival. If a demand D_n arrives, go to ***Step 2***.
- **Step 2**: Adjust the link-cost according to Eq. 1 and compute the shortest-route from the source node s to destination node d as the working path WP_n. If WP_n can be found successfully, go to ***Step 3***; otherwise, block demand, restore the network state, and go back to ***Step 1***.
- **Step 3**: if D_n is a critical request go to ***Step 4***; otherwise go to ***Step 5***.
- **Step 4**: Compute the shortest-path from the source node s to destination node d as the backup path BP_n. WP_n, and BP_n should be disjoint. If BP_n can be found successfully, accept this demand, update the network state in $G = (V, E)$, and go back to ***Step 1***; otherwise, block this demand, restore the network state, and go back to ***Step 1***.
- **Step 5**: For each link of working path WP_n, compute a shortest-path as the backup path BP_n,i. If all backup paths BP_n,i are found successfully, accept this demand, update the network state in $G = (V, E)$, and go back to ***Step 1***; otherwise, block this demand, restore the network state, and go back to ***Step 1***.

4 Performance valuation

The performance of the proposed "application-aware" heuristic algorithm is now analyzed using discrete event simulation. Specifically, the key evaluation metrics used here include resource utilization, recovery time, and the ratio of rejected demands. In particular, simulation experiments are carried out using two widely used network topologies (US network [6] and NSF network [7]) shown in Fig. 3. In each of these networks, it is assumed that each fiber link has $W = 32$ wavelengths and all OXC nodes support full wavelength conversion.

Meanwhile, the demand traffic model used in our simulations is the incremental traffic model of [8], in which connection requests (for a random source and destination) enter the network sequentially. Once a connection request is satisfied, it is assumed that its light path remains indefinitely in the network, i.e., it is never released. Indeed, this is quite representative of traffic on most real-world optical backbones, and moreover, is somewhat simpler than other dynamic traffic profiles used for testing "on-line" provisioning heuristic algorithms. As stated earlier, it is also assumed that each demand requests one wavelength unit of capacity. Finally, there are no waiting queues for network requests, i.e., subsequent re-tries of failed demands are not allowed and such requests are simply rejected.

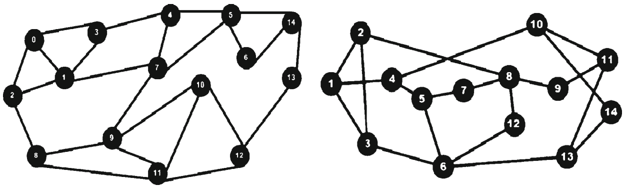

Fig. 3 Test networks

To evaluate our solution, three different scenarios are considered. Namely, in the first scenario, *path-based protection* (PBP) is implemented, in which one backup light path is computed to protect all links in the primary light path. Meanwhile, in the second scenario, *link-based protection* (LBP) is used, where a backup light path is computed for each link in a primary light path. At last in the third scenario, the simultaneous path- and link-based protection schemes are implemented, as per differing demand requirements. Here, we distinguish between two kinds of demands, critical and no-critical. Specifically, these demands are randomly generated using a uniform distribution, i.e., with 50% selection of each demand type.

Finally, the key performance metrics used include *resource utilization* (RU) [9] and recovery time [10]. The former gives insights into the quality of protection and is defined as the sum of the total backup and primary wavelength resources used. Hence, low RU is more efficient than high RU due to the fact that high RU requires a large capacity to establish and protect the connection against failures.

The average RU values as a function of number of requests (load) is plotted in Figs. 4 and 5. Here, it is clear that PBP protection is better than the LBP protection. The reason for this is that link-based protection assigns for each link of primary light path a backup light path while path-based protection use only one backup light path to protect all links in the primary light path. Meanwhile, the proposed joint scheme achieves a trade-off between the two, as expected.

The corresponding recovery times for these schemes are also analyzed here. Now, this value typically depends upon the length of the primary and backup light paths [10], i.e., shorter light path lengths lead to a faster recovery times. Hence, in our simulations, the recovery time is gauged as the average length of primary and backup light paths. The

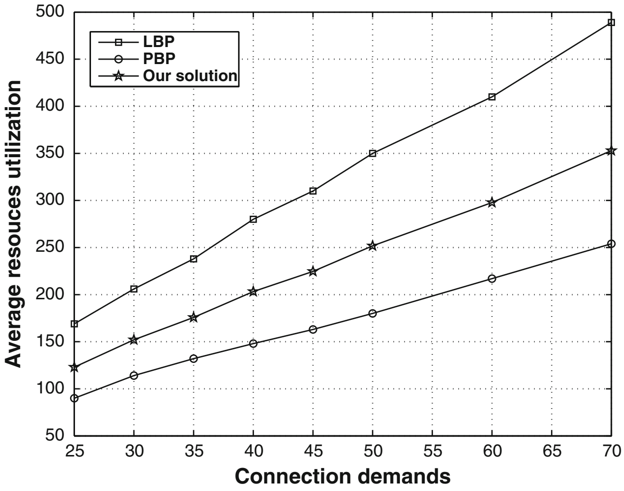

Fig. 4 RU (NSF network)

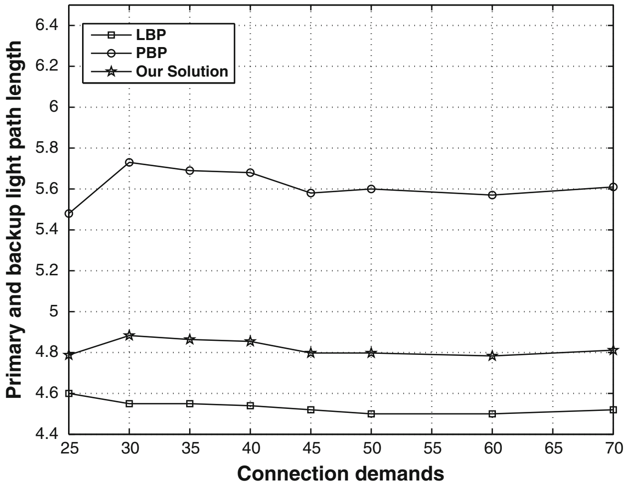

Fig. 6 RT (NSF network)

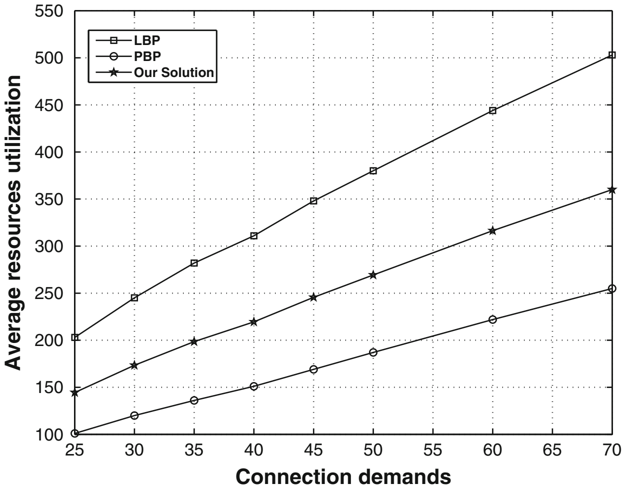

Fig. 5 RU (ARPANET network)

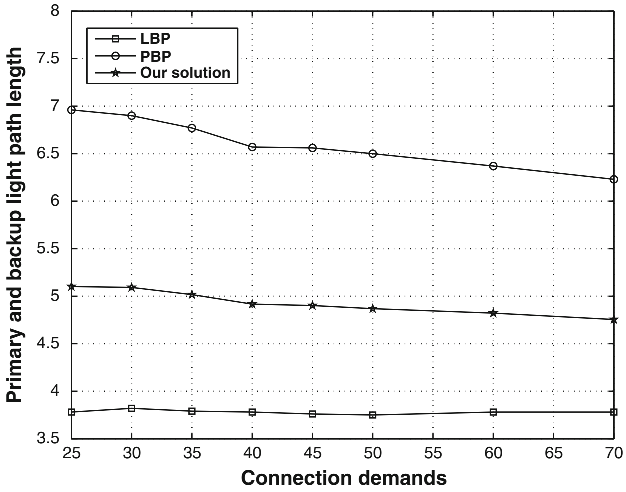

Fig. 7 RT (ARPANET network)

overall results here are again shown for varying connection demands in Figs. 6 and 7. As expected, link-based protection is faster because only the two end nodes of the failed link need to perform restoration. Furthermore, simulations show that the proposed joint solution achieves an acceptable trade-off between two competing objectives, i.e., minimizing backup resource and minimizing recovery timescales. This trade-off is due to the exploitation of link and path protection advantages.

5 Conclusion

This paper studies survivability in WDM optical networks and focuses on two key objectives of resource minimization and recovery times. The relative merits of path- and link-based protection are discussed, and then, a joint scheme is developed to incorporate both. Namely, we propose to protect critical demands using link-based protection and thereby reduce recovery times. At the same time, we propose to protect less stringent demands with path-based protection, thereby reducing resource utilizations.

Overall, our results show that the joint solution achieves a good trade-off between two competing goals: efficient use of backup resources and short recovery time. This study is very encouraging, and we intend to continue our research using other kind of networks such as multi-domain optical networks.

References

[1] Ramamurthy, S., Mukherjee, B.: Survivable WDM mesh networks- part I: protection. In: Proceedings of IEEE INFOCOM 744–751, March (1999)

[2] Ramamurthy, S., Mukherjee, B.: Survivable WDM mesh networks- part II: restoration. In: Proceedings of IEEE Integrated Circuits Conference 2023–2030, June (1999)

[3] Ho, P., Tapolcai, J., Cinkler, T.: Segment shared protection in mesh communications networks with bandwidth guaranteed tunnels. IEEE/ACM Trans. Netw. **12**(6), 1105–1118 (2004)

[4] Zang, H., Ou, C., Mukherjee, B.: Path-protection routing and wavelength assignment (RWA) in WDM mesh networks under duct-layer constraints. IEEE/ACM Trans. Netw. **11**(2), 248–258 (2003)

[5] Guido, M., et al.: Optical network survivability: protection techniques in the WDM layer. Photonic Netw. Commun. 251–269 (2002)

[6] Zhang, X., Liao, D., Wang, S., Yu, H.: On segment shared protection for dynamic connections in multi-domain optical mesh networks. Int. J. Electron. Commun. **64**(4), 366–371 (2010)

[7] Zhang, F., Zhong, W.: Performance evaluation of optical multicast protection approaches for combined node and link failure recovery. J. Lightwave Technol. **27**(18), 4017–4025 (2009)

[8] Eric, D., et al.: Deogun on the bandwidth efficiency of pre-cross-connected trails. In: Proceedings of IEEE International Conference on Communication 2294–2299 (2007)

[9] Drid, H., Cousin, B., Lahoud, S., Molnór, M.: Multi-criteria p-cycle network design. In: Proceedings of IEEE Conference on Local Computer Networks. Montreal, Canada, pp. 361–366, Oct. (2008)

[10] Drid, H., Cousin, B., Lahoud, S., Molnór, M.: A survey of survivability in multi-domain optical networks. Comput. Commun. **33**(8), 1005–1012 (2010)

Author Biographies

Hamza Drid received his Engineer Degree in Computer Science in 2004 from the University of Batna (Algeria), and a master degree from the university of Nancy 1 (France) in 2006. In 2010, He received the Ph.D. degree in Computer Science from University of Rennes 1 (France). His main research topics and interests include survivability in WDM optical networks, MPLS, resource optimization and routing in multi-domain optical networks. Since 2011, he is working on elastic optical networks at France Telecom. He has been involved in many research programs at the national and the European level.

Nasir Ghani is currently an Associate Professor in ECE at the University of New Mexico. His research interests include cyber-infrastructure networks, cloud-computing, survivability, applications, and telehealth. He has published over 140 refereed journal and conference papers, and several book chapters, and has co-authored various standardization drafts. Overall, his research has been funded by some key government agencies and some industrial sponsors. In particular, he received the NSF CAREER award in 2005 to support his work in multi-domain network design. Prior to joining academia, he spent over eight years in industry and held key technical positions at several large companies (Nokia, Motorola, IBM) as well as some startups (Sorrento Networks, Array Systems Computing). He is actively involved in a range of service roles and has served as a symposium co-chair for IEEE GLOBECOM, IEEE ICC, and IEEE ICCCN. He has also chaired the IEEE ComSoc Technical Committee on High Speed Networks (TCHSN) and established the High-Speed Networking Workshop for IEEE INFOCOM. He has been an Associate Editor for IEEE Communications Letters and has served as a guest editor for IEEE Network, IEEE Communications Magazine, and Cluster Computing. He received his Bachelor's degree from the University of Waterloo, his Master's degree from McMaster University, and his Ph.D. degree from the University of Waterloo, Canada.

Bernard Cousin is a Professor of Computer Science at the University of Rennes 1, France. Bernard Cousin received in 1987 his Ph.D. degree in computer science from the University of Paris 6. He is, currently, member of IRISA (a CNRS-University-INSA joint research laboratory in computing science located at Rennes). More specifically, he is at the head of a research group on networking. He is the co-author of a network technology book: "IPV6" (Fourth edition, O'Reilly, 2006) and has co-authored a few IETF drafts in the areas of Explicit Multicasting and Secure DNS. His research interests include all-optical networks, dependable networking, high speed networks, traffic engineering, multicast routing, network QoS management, network security and multimedia distributed applications.