2004

Survivable Traffic Grooming with Differentiated End-to-End Availability Guarantees in WDM Mesh Networks

Wang Yao
University of Nebraska - Lincoln, wyao@cse.unl.edu

Byrav Ramamurthy
University of Nebraska - Lincoln, bramamurthy2@unl.edu

The 13th IEEE Workshop on Local and Metropolitan Area Networks, 2004. LANMAN 2004.
DOI: 10.1109/LANMAN.2004.1338407

Survivable Traffic Grooming with Differentiated End-to-End Availability Guarantees in WDM Mesh Networks

Wang Yao and Byrav Ramamurthy
Department of Computer Science and Engineering,
University of Nebraska-Lincoln, Lincoln NE 68588 USA
Email: {wyao,byrav}@cse.unl.edu

***Abstract*— Traffic grooming is critical in WDM optical metropolitan area networks (MANs), where low-rate connections are packed onto high-rate wavelength paths (lightpaths). Various applications in the MAN demand different levels of reliability. Therefore, it is necessary to provision connections with differentiated reliability guarantees in the MAN. In this paper, we first present an analytical model to calculate the availability of connections using different protection schemes in WDM optical MANs with general mesh topologies. Then we propose and simulate two grooming algorithms which can provision availability guaranteed connections based on per-connection requirements.**

***Index Terms*—Survivability, traffic grooming, availability, path protection, WDM.**

I. Introduction

Traffic grooming is an essential functionality to provision sub-wavelength connections in wavelength division multiplexed (WDM) optical metropolitan area networks (MANs). In a WDM optical MAN with general mesh topology and grooming capability, low-rate connections are carried over the virtual topology, which consists of high-rate lightpaths established over the physical topology. The physical topology is composed of optical cross-connects (OXCs) or add/drop multiplexers (ADMs) connected by optical fibers.

Reliability is critical for optical networks because a single failure may affect a large volume of traffic. While network service providers (NSPs) may choose any scheme to provide reliable services, what really matters for customers is the reliability of the end-to-end connections. The reliability requirement is usually decided by the customer application and defined in the service level agreement (SLA) between the NSP and the customer. As different applications in a MAN demand services of different characteristics, their reliability requirements also vary. On the other hand, the goal of the NSP is to maximize the revenue subject to the SLAs and resource constraints.

Path protection is often used for connections with high reliability requirement. Path protection can be provided at different granularities with different schemes. Two typical protection schemes are 1+1 dedicated protection and 1:N shared protection. In WDM mesh grooming networks, the protection schemes can be applied either at lightpath (wavelength) granularity or connection (sub-wavelength) granularity.

While most previous work addressed traffic grooming [1][2] and protection [8]-[12] problems separately, [3] and [4] considered them jointly. The work in [3] proposed two grooming policies, namely mixed primary-backup grooming policy (MGP) and segregated primary-backup grooming policy (SGP). The work in [4] compared protection schemes at different granularities in the WDM grooming networks: protection at lightpath (PAL) and protection at connection (PAC). However, neither of them addressed the problem of how to provision connections meeting the specific reliability requirements defined in the SLAs. The work in [5] proposed a framework to provision availability guaranteed lightpaths. The use of availability to measure reliability in the optical networks was introduced in [6].

In this paper, we first present a model to calculate the connection availability in WDM mesh grooming networks using different protection schemes. Then we propose two survivable grooming algorithms based on the model to provision connections with differentiated availability requirements.

II. Availability Model

A general equation to calculate the availability of a component (e.g. fiber link) is (1):

$$A = MTTF/(MTTF + MTTR), \tag{1}$$

where A is the availability, MTTF is the mean time to failure and MTTR is the mean time to repair the component.

A. Availability of an Unprotected Connection

For an unprotected connection C_u as shown in Fig. 1, its availability is the product of all the availabilities of the lightpaths it traverses, which in turn is the product of all the availabilities of the fiber links each lightpath uses.

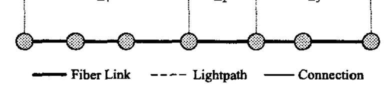


Fig. 1. Unprotected connection.

B. Availability of a Protected Connection

A combination of four protection schemes is shown in Fig. 2. For dedicated path protection scheme, each primary path has an allocated backup path. For shared path protection scheme, each primary path may share resources in the backup path with other link-disjoint primary paths. For Shared-PAL scheme, we define the set of primary lightpaths sharing some resources in the backup lightpath with primary lightpath L_p as shared backup resource lightpath group (SBRLG) of L_p. In Fig. 2 (b), SBRLG(L_{pi}) = $\{L_{pi}^1, L_{pi}^2, ..., L_{pi}^{ni}\}$. For Shared-PAC scheme, we define the set of primary connections sharing some resources in the backup connection with primary connection C_p as shared backup resource connection group (SBRCG) of C_p. In Fig. 2 (d), SBRCG(C_p) = $\{C_p^1, C_p^2, ..., L_p^n\}$.

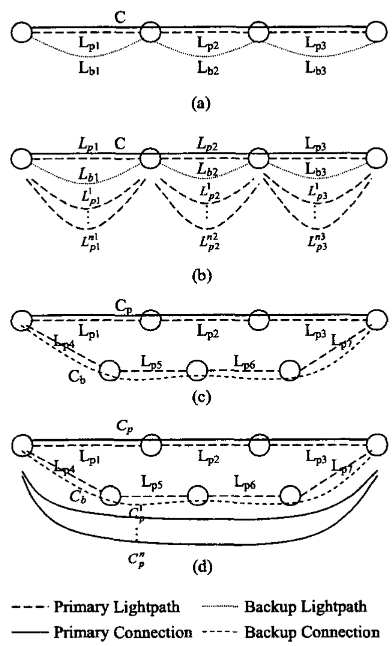


Fig. 2. Protection Schemes: (a) Dedicated-PAL, (b) Shared-PAL, (c) Dedicated-PAC, (d) Shared-PAC.

Let A_c^l be the availability of a connection with PAL. Equations (2) and (3) can be used for dedicated-PAL, and (2) and (4) can be used for shared-PAL.

$$A_c^l = \prod_{l_i \in L_c} A_l^i , \tag{2}$$

$$A_l^i = 1 - (1 - A_p^i)(1 - A_b^i) , \tag{3}$$

$$A_l^i = A_p^i + (1 - A_p^i) \times A_b^i \times \sum_{j=0}^{n_i} \frac{1}{j+1} P_f^j , \tag{4}$$

where A_p^i is the availability of a primary lightpath l_p^i used by the connection C, A_b^i is the availability of the backup lightpath l_b^i of the primary lightpath l_p^i, A_l^i is the joint probability of primary lightpath l_p^i and backup lightpath l_b^i, L_c is the set of lightpaths a connections C uses, P_f^j is the probability of exactly j lightpaths in SBRLG(l_p^i) are unavailable. We assume the j lightpaths fail independently and have the same failure probability. Therefore, when j lightpaths in SBRLG(l_p^i) are unavailable, the probability of l_p^i being the first one to fail is 1/(j+1).

Let A_c^d be the availability of a connection with dedicated-PAC protection scheme and A_c^s be the availability of a connection with shared-PAC protection scheme. They can be calculated by (5) and (6) respectively.

$$A_c^d = 1 - (1 - A_c^p)(1 - A_c^b) , \tag{5}$$

$$A_c^s = A_c^p + (1 - A_c^p) \times A_c^b \times \sum_{i=0}^{n} \frac{1}{i+1} P_f^i , \tag{6}$$

where A_c^p is the availability of the primary connection C_p, A_c^b is the availability of the backup connection C_b, P_f^i is the probability of exactly i connections in SBRCG(C_p) are unavailable.

III. Survivable Grooming Algorithms

Based on the availability model, the grooming algorithm without considering protection can be used to provision dynamically arriving connection requests with differentiated availability requirements. For higher availability requirements, two survivable grooming algorithms corresponding to the PAL and PAC schemes respectively are proposed. Both of the two algorithms can be applied with either dedicated or shared protection schemes. All the three algorithms presented in this section are based on a link bundled auxiliary graph (LBAG) model [7]. Using the LBAG model, the algorithms can calculate the shortest path currently available in the network for a connection request. Note that the LBAG model is adaptive in that it considers the current network state information in the calculation.

A. Grooming with No Protection (GNP) algorithm

Calculate the shortest path as the candidate path using the LBAG model. Calculate the availability of the candidate path. If it meets the availability requirement, then satisfy the request using the path; otherwise, block the request.

B. Grooming with Protection at Lightpath level (GPL) algorithm

Calculate the shortest path as the candidate path using the LBAG model. If the candidate path does not contain new lightpath, calculate the availability of the candidate path. If it meets the availability requirement, then satisfy the request using the path; otherwise, block the request. If the candidate path contains new lightpaths, then use the LBAG model to calculate the shortest link-disjoint paths in the physical topology to serve as the backup paths of these new lightpaths. Calculate availability of the new lightpaths. Then calculate the availability of the candidate path. If it meets the availability requirement, then satisfy the request using the path; otherwise, block the request.

C. Grooming with Protection at Connection level (GPC) algorithm

Step 1. Calculate the shortest path which meets the availability requirement using the LBAG model. If successful, then satisfy the connection request using a single primary path without protection path; otherwise, go to step 2.

Step 2. Calculate the shortest path and its shortest link-disjoint path as the primary path and backup path respectively. Calculate the overall availability of the path pair. If this path pair meets the availability requirement, then satisfy the connection request using the path pair; otherwise, block the request.

IV. NUMERICAL RESULTS AND ANALYSIS

We simulate the grooming algorithms on the EUPAN network in Fig. 3 with the following assumptions. The arrival of connection requests is a Poisson process with rate λ. The connection requests are uniformly distributed among all node pairs. The connection service time is distributed exponentially with mean $1/\mu$. The connection bandwidth requirement is distributed uniformly between 1 and 4 and the bandwidth capacity of a lightpath is 16. (The bandwidth capacity is normalized based on the smallest grooming granularity in the network. For example, if one wavelength supports an OC-48 channel, and the smallest grooming granularity is OC-3, then the normalized capacity is 48/3=16.) The availability requirements of the connection requests are uniformly distributed among four classes: 90%, 99%, 99.9% and 99.99%. Each node has 32 transceivers and each fiber link supports 16 wavelengths. We simulate 100000 connection requests for each scenario. In addition, full wavelength conversion capability is assumed.

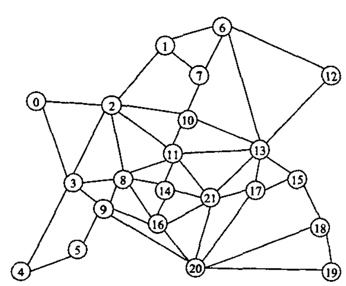


Fig. 3. The EUPAN network used in the simulation.

Fig. 4 compares the performance of the three grooming algorithms in terms of weighted blocking probability, which refers to the percentage of traffic blocked due to resource constraints or not being able to meet availability requirements. As shown, GNP has a fairly constant blocking percentage which is roughly equal to the percentage of traffic that cannot meet availability requirements using a single connection path. As traffic loads increases, the blocking probability of GPL increases because of resource constraints. GPC performs best among the three.

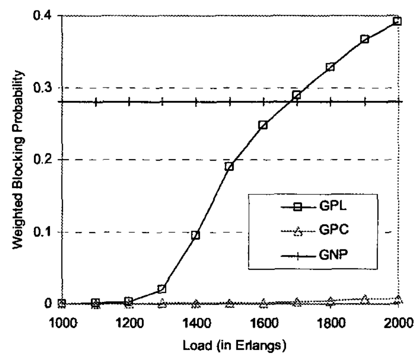
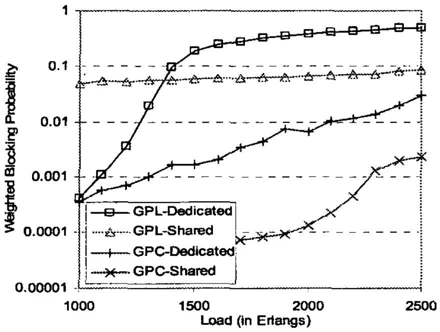


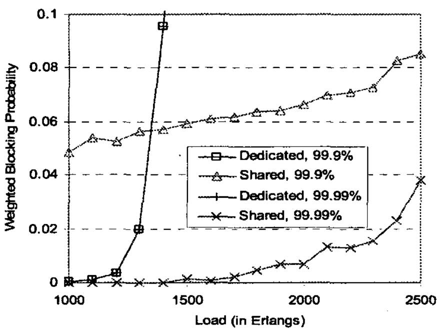
Fig. 4. Performance of the three grooming algorithms. Dedicated protection scheme is used with GPL and GPC. Fiber link availability is 99.9%.

Fig. 5 (a) compares the performance of the GPL and GPC grooming algorithms. As can be seen, GPC generally outperforms GPL, irrespective of whether dedicated or shared protection schemes are used. This may be because GPC tries to satisfy a connection using a single unprotected path if it, by itself, can meet the availability requirement. As a certain percentage of traffic can be satisfied by an unprotected path, the resources are used more efficiently.

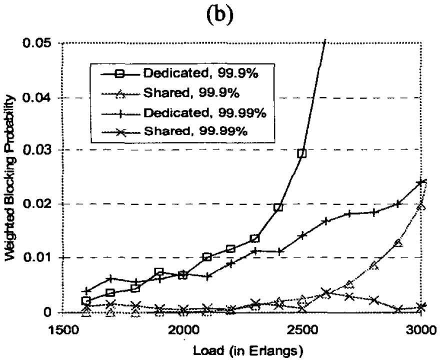
Figs. 5 (b) and (c) compare the performance of the dedicated and shared protection schemes for GPL and GPC respectively. Two values, 99.9% and 99.99%, are used for the link availability. As shown, shared protection scheme is more resource-efficient than dedicated protection scheme, because the grooming algorithms generally have lower blocking probability when shared protection scheme is used. On the other hand, connections with dedicated protection scheme enjoy higher availability than connections using shared protection scheme. As shown in Fig. 5 (b), when the availability of the fiber link increases from 99.9% to 99.99%, the curves of dedicated protection scheme are the same, while the blocking probability drops significantly for shared protection scheme. This implies that the fiber availability at 99.9% is enough to meet the availability requirements of all the requests when GPL-dedicated is used. The requests are blocked due to inadequate resources instead of not being able to meet the availability requirement.



(a)



(b)



(c)

Fig. 5. Performance of the grooming algorithms with different protection schemes: (a) GPL vs. GPC when the fiber link availability is 99.9%, (b) Dedicated vs. Shared using GPL, (c) Dedicated vs. Shared using GPC.

V. CONCLUSIONS

From the availability model, it is obvious that applying protection at either lightpath level or connection level can increase the availability of a connection. Our simulations demonstrate that shared protection is more resource-efficient than dedicated protection and dedicated protection generates higher availability than shared protection. Therefore, dedicated protection is needed for connections with extremely high availability requirements, while shared protection may be preferred for most of the connections.

Our simulations also show that GPC can provision connections in a more flexible way than GPL in the sense that GPC can choose to use a single path for a connection when the single path suffices for the availability requirement. On the other hand, GPL provides protection at a coarser granularity than GPC. It has to protect every lightpath because it has no idea of which connections will use the lightpath.

ACKNOWLEDGMENT

This work was supported in part by the U. S. National Science Foundation grants (ANI-0074121 and EPS-0091900) and the UNL Program of Excellence PRISM Priority initiative.

REFERENCES

[1] K. Zhu, B. Mukherjee, "On-Line Approaches for Provisioning Connections of Different Bandwidth Granularities in WDM Mesh Networks," *OFC 2002*, pp.549-551, 2002.

[2] H. Zhu, H. Zang, K. Zhu, B. Mukherjee, "Dynamic Traffic Grooming in WDM Mesh Networks Using a Novel Graph Model," *Globecom 2002*, 2002.

[3] S. Thiagarajan, A. Somani, "Traffic Grooming for Survivable WDM Mesh Networks," *Optical Network Magazine*, May/June 2002.

[4] C. Qu, K. Zhu, B. Mukherjee, "Survivable Traffic Grooming in WDM Mesh Networks," *OFC 2003*, vol. 2, pp. 624-625, 2003.

[5] J. Zhang, K. Zhu, B. Mukherjee, "Service Provisioning to Provide Per-Connection-based Availability Guarantee in WDM Mesh Networks," *OFC 2003*, vol. 2, pp.622-623, 2003.

[6] M. Clouqueur, W. D. Grover, "Availability Analysis of Span-restorable Mesh Netoworks," *IEEE Journal on Selected Areas in Communications*, vol. 20, no. 4, May 2002.

[7] W. Yao, B. Ramamurthy, "Constrained Dynamic Traffic Grooming in Optical WDM Mesh Networks with Link Bundled Auxiliary Graph Model," *to appear in HPSR 2004*.

[8] S. Ramamurthy and B. Mukherjee, "Survivable WDM Mesh Networks—Part I: Protection," in *Proc. IEEE INFOCOM*, pp. 744-751, Mar. 1999.

[9] Y. Xiong, D. Xu, C. Qiao, "Achieving Fast and Bandwidth-Efficient Shared-Path Protection," *Journal of Lightwave Technology*, vol. 21, no. 2, Feb, 2003.

[10] O. Gerstel, R. Ramaswami, "Optical Layer Survivability—An Implementation Perspective," *IEEE Journal on Selected Areas in Communications*, vol. 18, no. 10, Oct. 2000.

[11] G. Ellinas, E. Bouillet, R. Ramamurthy, J. Labourdette, S. Chaudhuri, K. Bala, "Routing and Restoration Architectures in Mesh Optical Networks," *Optical Networks Magazine*, Jan./Feb. 2003.

[12] G. Li, B. Doverspike, C. Kalmanek, "Fiber Span Failure Protection in Mesh Optical Networks," in *Proc. of SPIE OptiComm 2001*, Denver, CO, Aug. 2001.