Computer Communications 32 (2009) 1677–1684

Contents lists available at ScienceDirect

Computer Communications

journal homepage: www.elsevier.com/locate/comcom

Priority-aware optical shared protection: An offline evaluation study

Wissam Fawaz *, Timothy Sawah, Chadi Abou-Rjeily

Lebanese American University (LAU), Byblos, Lebanon

ARTICLE INFO

Article history:
Received 5 July 2008
Received in revised form 14 May 2009
Accepted 19 June 2009
Available online 27 June 2009

Keywords:
Optical networks
Protection
Quality of service provisioning
Integer linear programing
Heuristics

ABSTRACT

The availability of an optical connection is considered to be a critical service differentiator in WDM optical networks. In this regard, the design of a protection scheme that improves the availability of high priority optical connections and makes efficient use of optical resources is a major challenge faced by optical network operators. In a previous study, we proposed the so-called priority-aware shared protection survivability scheme as a potential solution to this design issue.

In this paper, we complement our previous study. More specifically, we develop an offline study whose main purpose is to assess the efficiency of the priority-aware shared protection scheme. Through this study, we show that the priority-aware shared protection strategy as opposed to existing protection strategies is able to achieve the best tradeoff between optical resource usage and optical connections' availability satisfaction.

1. Introduction

The Wavelength-Division Multiplexing (WDM) technology increases the transmission capacity of fiber links by several orders magnitude. It divides the tremendous bandwidth of a fiber into many non-overlapping wavelengths (WDM channels) which can be operated at the peak electronic speed of several gigabits per second [1]. In wavelength-routed WDM networks, an optical cross-connect (OXC) can switch the optical signal on a WDM channel from an input port to an output port; thus an optical connection (lightpath) may be established from a source node to destination node along a path that may span multiple fiber links. As WDM keeps on evolving, fibers are witnessing a huge increase regarding their carriage capacity, which has already reached the order of terabits per second and will continue to grow for years to come. Therefore, the failure of a network component (e.g., a fiber link, an optical cross-connect, an amplifier, a transceiver, etc.) can weigh heavily on optical carrier operators due to the consequent huge loss in data and revenue. Indeed, a single outage can disrupt millions of users and result in millions of dollars of lost to users and operators of the optical network. The Gartner research group attributes for instance up to 500 million dollars in business losses due to optical network failures by the year 2004 [2]. Providing resilience against failures is thus an important requirement for WDM optical networks. Building on this, *network survivability* together with its impact on network design becomes a critical concern for optical operators. In this regard, we believe that *protection*, a proactive procedure, is a key strategy to ensure optical network *survivability*.

In the so-called *dedicated-path protection* scheme (also called 1:1 protection), one path, referred to as the primary path, is used to carry traffic during normal operation, while one extra backup path is pre-reserved and activated to recover the connection under failure condition. Spare resources can be exclusively allocated for one primary connection (as in the dedicated protection case) or can be shared among different connections (shared protection) as long as any two of these connections are link-disjoint, e.g., do not belong to the same Shared Risk Link Group (SRLG). The latter case refers to the so-called *classical shared-path protection* where *N* primary connections share a single protection path (also referred to as 1:*N* protection). Another protection scheme that was discussed in the literature is the so-called mixed shared-path protection [3,4] that allows a primary connection and one or more backup paths to share the same wavelength channel. We bring the reader's attention to the fact that the mixed shared-path protection scheme will not be considered in this study and will be the subject of a future paper.

To date, the majority of the work concerning shared protection considered the primary connections as equally important when contending for the use of the shared backup resources. In other words, when several connections fail successively, the first failed connection is recovered by the backup path irrespective of the *availability* requirements of the remaining failed connections. Hence, these latter connections are penalized and remain in an unrecovered state until either their primary paths

* Corresponding author. Tel.: +961 3 63 93 64.
E-mail addresses: wissam.fawaz@lau.edu.lb (W. Fawaz), timothy.sawah@lau.edu.lb (T. Sawah), chadi.abourjeily@lau.edu.lb (C. Abou-Rjeily).

0140-3664/$ - see front matter © 2009 Elsevier B.V. All rights reserved.
doi:10.1016/j.comcom.2009.06.010

are repaired or until backup resources are released. From a service perspective, classical shared protection does not provide an optimal survivability scheme as it does not take into account the different QoS requirements of the primary connections during the recovery procedure. To cope with such a limitation, we envisaged in [5] to introduce a relative priority among the primary connections sharing backup resources. As such, we proposed a novel scheme that we referred to as the *priority-aware shared protection* survivability scheme. In the proposed protection scheme, the availability requirement of an optical connection is used as a priority indicator. In fact, it is assumed that by means of an Optical Service Level Agreement (O-SLA) [6] the optical connection would subscribe to an optical service with a certain required availability level. The higher the required availability is, the higher the priority of the optical connection would be. Building on this observation, the priority-aware shared protection scheme operates as follows. If a low priority connection fails first its recovery would be possible. However, once a high priority connection is failed, it will use the backup resources, resulting in the preemption of the previously recovered lower priority connection.

This paper presents a complementary study to the proposal we brought up in [5] and that has been later on refined in both [7,8]. The authors in [7] made a number of assumptions that aimed at facilitating the study of our priority-aware shared protection scheme. They proposed to accomplish this by treating the case of backup sharing among primary connections having the same failure rates. This study differs from the one presented in [7] in that it considers backup sharing in its most general form and thus no assumptions are made with respect to the way backup sharing is being deployed in the optical network. It is important to note that in [8] we presented an online study of the priority-aware shared protection scheme, where we evaluated the performance of the proposed scheme in a dynamic network environment. In our main objective behind this paper is to assess the efficiency of the priority-aware shared protection scheme in comparison to the existing protection schemes. We envision to achieve this purpose by evaluating the cost in terms of resources (i.e., number of wavelengths needed for instance) resulting from the deployment of both the priority-aware scheme and the classical existing schemes. As a distinguishing feature from the work presented in [8], this cost assessment is carried out considering a static optical traffic scenario, i.e., an offline scenario. This *offline study* compares the performances of the protection schemes in question in terms of the *resources needed (wavelengths)* in the network, and of the resulting connections' *Availability Satisfaction Rate (ASR).* In fact, the performance of each protection strategy is studied via a static optimization [9] approach which can be summarized as follows: given a static traffic matrix with predefined availability requirements, and given a protection strategy deployed in the WDM network, find the optimum values of a set of network variables that minimizes a given cost function, under a set of constraints. It is clear that the constraints will greatly vary from one protection strategy to another. Retaining a certain harmony with the existing literature pertaining to WDM network offline studies [10–13], the cost function to be optimized is the number of wavelengths necessary to route the static traffic in the network. However, our work is one of the few studies to take into consideration an additional cost, that is, the availability satisfaction rate of the provisioned clients.

The paper is structured as follows: in Section 2, we evaluate the availability of an optical connection under different protection strategies. In Section 3, we introduce the offline study to gauge the benefits behind the priority-aware shared protection scheme. Finally, Section 4 concludes the paper.

2. Combinatorial analysis of availability in WDM mesh networks

Throughout the offline study, there will be a need to compute the availability of a connection under different protection strategies, namely the unprotected case, dedicated and classical shared protection, and the proposed priority-aware protection scheme. This computation is based on the combinatorial analysis approach presented in the following subsections.

We assume that:

- a system is either available (functional) or unavailable (excerpting failure);
- different network components fail independently in the network;
- for any component, the *up* times (or mean value Mean Time To Failure, MTTF) and the repair times (or mean value Mean Time To Repair, MTTR) are independent memoryless processes with known mean values (as presented in [14]).

The availability of a system is the fraction of time the system is up during the entire service time. If a connection t is carried by a single path, its availability (denoted by A_t) is equal to the path availability. The path holding t fails when at least one of the components along the path is defective. According to [15] the contribution of cable-cut rate to the overall path failure is predominant compared to that of other components. If the connection t is dedicated or shared protected, A_t is determined by both its primary and backup paths.

2.1. Methodology for assessing network-component availability

A network component's availability can be estimated based on its failure characteristics. Upon the failure of a component, it is repaired and restored to be "as good as new". This procedure is known as an alternating renewal process. Consequently, the availability of a network component j (denoted as a_j) can be calculated as follows [16]:

$$a_j = \frac{MTTF}{MTTF + MTTR} \tag{1}$$

In particular, the *MTTF* of a fiber link is distance related and can be derived according to measured fiber-cut statistics as those presented in [14].

2.2. Availability of an unprotected connection

When a connection t is not protected, it is available only when all the network components along its route i are available. If K_i denotes the set of components used by path i, the availability of connection t, A_t, can be computed as

$$A_t = \prod_{j \in K_i} a_j \tag{2}$$

2.3. Availability of a dedicated-path protected connection

In dedicated-path protection, a connection t is carried by one primary path p and protected by one backup path b which is link disjoint with p.

When primary path p fails, its traffic is switched to backup path b as long as b is available; otherwise, the connection becomes unavailable until the failed component is replaced or restored [17,18]. As a result, t is up only when p is up or b is up when p fails. A_t can thus be computed as follows: