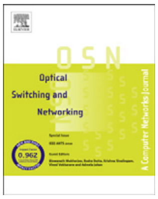
Optical Switching and Networking 10 (2013) 119–131

Contents lists available at SciVerse ScienceDirect

Optical Switching and Networking

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



Inter group shared protection (I-GSP) for survivable WDM mesh networks

Anwar Haque [a], Pin-Han Ho [a,*], Hamed M.K. Alazemi [b,1]

[a] *Department of Electrical and Computer Engineering, University of Waterloo, Ontario, Canada N2L3G1*
[b] *Department of Computer Engineering, Kuwait University, PO 5969, Safat 13060, Kuwait*

ARTICLE INFO

Article history:
Received 14 February 2011
Received in revised form
16 April 2012
Accepted 26 June 2012
Available online 19 August 2012

Keywords:
Integer linear programming (ILP)
Optical network
Shared path protection
Shared risk link group
Wavelength routing
Wavelength division multiplexing (WDM)

ABSTRACT

This paper focuses on the survivable routing problem in WDM mesh networks where the objective is to minimize the total number of wavelengths used for establishing working and protection paths in the WDM networks. The past studies for survivable routing suffers from the scalability problem when the number of nodes/links or connection requests grows in the network. In this paper, a novel path-based shared protection framework, namely inter group shared protection (I-GSP), is proposed where the traffic matrix can be divided into multiple protection groups (PGs) based on specific grouping policy. Optimization is performed on these PGs such that sharing of protection wavelengths is considered not only inside a PG, but between the PGs. Simulation results show that I-GSP based integer linear programming model, namely, ILP-II solves the networks in a reasonable amount of time for which a regular integer linear programming formulation, namely, ILP-I becomes computationally intractable. For most of the cases the gap between the optimal solution and the ILP-II stays within 6%. The proposed ILP-II model yields a scalable solution for the capacity planning in the survivable optical networks based on the proposed I-GSP protection architecture.

1. Introduction

The rapid growth and recent advances in photonic communication technology have opened the door for long haul wavelength division multiplexing (WDM) [1] based optical networks, which carry data traffic in a rate of Terabit per second to become the prime technology in transport networks. Any unexpected disruption to such an ultra-high speed network may have disadvantages that result in a huge loss to its end-users and the carrier itself. Thus, survivability has been well recognized as one of the most important objectives in the design of WDM mesh networks such that any unexpected interruption to the working traffic can be restored in a short time to guarantee service continuity and data integrity. For this purpose, the effort of pre-planning spare capacity (i.e., protection paths) for the corresponding working capacity (i.e., working paths) has been well recognized as one of the most effective approaches. With pre-planned spare capacity, the working paths affected by the failure can be switched over to the protection paths for maintaining service continuity. This task is known as survivable routing where the traffic demand is known in advance.

Developing an effective scheme that can be both capacity-efficient and computation-efficient has long been a challenge. The past studies for survivable design took approaches of optimization for allocating the working and protection paths. One drawback of such approaches is that as the number of nodes/links or connection requests grow, the problem quickly becomes

---

[*] Corresponding author.
E-mail address: pinhan@bbcr.uwaterloo.ca (P.-H. Ho).

[1] This work is realized in collaboration with Dr. Hamed Alazemi during his sabbatical at the University of Quebec, INRS, Montreal, Canada.

1573-4277/$ - see front matter © 2012 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.osn.2012.06.002

computationally intractable, even in moderate-sized networks. To overcome the scalability problem, one of the most commonly adopted ideas is to divide the traffic demands into different protection groups (PGs).

In this paper, a path-based shared protection framework is proposed, namely inter-group shared protection (I-GSP) that divides the total traffic demand (i.e., traffic matrix) into multiple PGs and optimization is conducted on each of the PG where sharing of protection resources between the PGs is considered. Based on the I-GSP framework, this paper introduces an Integer Linear Programming (ILP) model, namely ILP-II which optimizes the task of resource allocation in each PG where sharing of protection resources between the PGs is allowed. The working paths in each PG are mutually link-disjointedly routed. To compare the capacity efficiency of ILP-II, ILP-I is introduced which also formulates path-based shared protection but optimization is conducted on the total traffic matrix. It is clear that ILP-I will produce the optimal solution since the optimization is performed on the total traffic matrix, but will become computationally intractable when the network size and traffic demand grow [4,6,7,16,17,38]. Results from ILP-I will be compared with ILP-II to evaluate the gap between the optimal and ILP-II solution. A dedicated protection scheme is also implemented; namely, ILP-III that is similar to the ILP-I except that no sharing of spare resources is allowed. Results from ILP-III will be used to compare the capacity efficiency between "sharing" and "no-sharing" scenarios. The performance and the computation complexity of each model will be investigated.

The rest of the paper is organized as follows. Section 2 provides an overview of the recently reported survivable routing schemes. Section 3 formulates the problem. Section 4 introduces the proposed ILP-I and ILP-II models. Section 5 shows the experiment results, and Section 6 concludes the paper.

2. Background work

A brief review is provided in this section on the recently reported survivable routing schemes. With survivable routing, two types of protection schemes are defined – dedicated and shared protection, according to whether or not resource sharing (i.e., wavelength sharing) is allowed between different protection lightpaths.

The concept of SRLG serves as the key role in the development of shared protection schemes. SRLG is defined as a group of network elements (i.e., links, nodes, physical devices, software/protocol identities, or a combination thereof) subject to the same risk of single failure [4]. In practical cases, an SRLG may contain multiple seemingly unrelated and arbitrarily selected links/nodes. The fact that two paths do not take any common SRLG is referred to as the SRLG-disjointedness, which is the major effort of achieving 100% restorability under a single failure scenario if one of the paths is taken as the working path and the other is taken as the protection path. It has been observed that the resource sharing between different protection paths can substantially reduce the ratio of redundancy required to achieve 100% restorability [5].

Dedicated protection (i.e., 1+1 or 1:1) provides a very fast service restoration at the expense of high ratio of redundancy (i.e., the ratio of capacity taken by protection and working paths in the network) usually reaches 100% or more. To implement dedicated protection in mesh WDM networks, the physical routes for the working and protection paths must be determined. The two paths are SRLG-disjoint such that no any single failure will affect both paths at the same moment.

For shared protection, the spare capacity (i.e., wavelengths) taken by protection paths can possibly be shared by some other protection paths. The SRLG disjointedness must exist not only between the working-protection path-pair, but also among the working paths for which the corresponding protection paths share the same wavelength. It is clear that the implementation of shared protection imposes one more disjointedness requirement than that for the dedicated protection. This clearly shows that the development of shared protection schemes is generally more complicated.

From the implementation point of view, the survivable routing schemes can be divided into two categories: link-oriented and path-oriented [2–4]. The former restores the working capacity when it is subjected to any unexpected interruption. In particular, the restoration is done by switching to and merging back from the corresponding spare capacity at the two ends of the link. The path-oriented, however, addresses spare capacity for each working path and investigates the link-disjointedness constraint in the networks.

In mesh networks, link-oriented schemes have been well recognized as feasible approaches with high restoration speed but low capacity efficiency [18,19]. The fast restoration from a failure is due to the fact that the deployment of spare capacity along each link is dedicated to the working capacity along a specific physical span, which may yield a smaller length of protection cycles. In terms of WDM networks with multi-service environments, the link-oriented approach nonetheless falls short in service differentiation and manipulation of distribution for the spare capacity. Note that each lightpath in the optical domain is taken as a discrete bandwidth unit with a specific service level agreement. In the event that the wavelength continuity constraint (e.g., the case without wavelength conversion or with partial/sparse wavelength conversion) is considered, most of the reported link-oriented approaches can barely be applied, except being provided with some extent of modifications. However, these modifications may largely increase the computation complexity by jointly considering the working capacity on multiple wavelength planes and the lightpaths with different class of services along each link [4]. Some of the major link-oriented protection schemes include Minimum node-cover [19,21], ring-cover [22–24], and P-cycle [25–27].

With the path-oriented approach, the spare capacity is allocated along a protection path that is link-disjoint with the working path. The path-oriented approach creates a better platform for achieving service differentiation and traffic engineering for both working and protection paths. In mesh networks, path protection is more feasible than