Evaluation of Blocking Constraints for Survivable WDM Optical Networks

Satkunarajah Suthaharan, Fathima Sharfana A, and Shagitha Thiruvanantharajah
Department of Physical Science,
Vavuniya Campus of the University of Jaffna.

***Abstract*—The advantage of a huge amount of data transmission in form of multimedia broadband services can be benefited using a technique called wavelength division multiplexing (WDM) technology. In WDM, the huge amount of bandwidth can be divided on a fiber in several non-overlapping wavelength channels simultaneously. In case of failure in optical networks, vast amount of data will be lost due to some reasons such as fiber-cut. Protection is one of the survivability methods to overcome such failures. We consider dedicated protection in this paper in which primary paths and their associated backup paths are configured at the time of connections establishment. We suppose that a failure on a primary path, the traffic is rerouted through backup path without any configuration as the backup paths are pre configured, therefore, dedicated protection provides the benefit of short recovery time. In this paper, we investigate the performance caused by various constraints in terms of blocking probability for dedicated protection in WDM networks. To evaluate the constraints for blocking probability we deploy various algorithms. In this paper, we carry out the investigation with detailed simulation experiments on different data rates in a standard NSFNET network topology. Findings of our investigation are as follows. (1) Blocking caused by the lack of backup paths is comparatively higher. (2) In certain algorithm, blocking caused by the lack of primary path is higher and considerable. (3) Two algorithms show the same pattern in all the constraints of blocking. (4) Blocking caused by the lack of primary resources and the lack of backup resources are negligible when using all the algorithms.**

***Keywords*—optical networks; dedicated protection; blocking constraints, lightpath assignment.**

I. Introduction

Optical networking technology gives the efficient solution to the huge bandwidth requirement in order to use multimedia broadband services and distributed applications. This benefit can be realized when using wavelength division multiplexing (WDM) technology [1]. WDM divides the huge transmission bandwidth available on a fiber into several non-overlapping wavelength channels and admits the optical transmission of data through optical fiber. It provides bidirectional communication over optical fiber medium in the order of gigabits and terabits per second [2]. WDM can be further realized with electromagnetic spectrum. Electrical signals are carried in the form of light pulses through optical fiber to carry information. Electrical signals are converted into optical signals using injection laser diode (ILD) at the sender side, and a photo diode is used to convert the light into electrical signals at the receiver side. It is mostly used in the optical fiber network to transmit data in several channels of a single strand fiber. Particularly in C-band, the bandwidth each of which 50 GHz of a fiber can be divided into 88 channels to support a combined bit rate in the range of 4.4 Tbps using WDM technology [3].

Since the failure in the backbone network is the most common occurrence, securing high capacity data is an essential task in optical network. Failures may lead to performance degradation, loss of huge amount of data, and blocking of services in the network [4][5]. Survivability is a mechanism which is proposed to secure optical network and to provide continuous services in the presence of network failures. Survivability can be performed by provisioning both primary path and backup path in a network. Primary path is used to transmit traffic and the backup path is used to reroute the traffic in case of failure. Protection and restoration are the two schemes in survivability approach which provide less amount of data loss particularly in mesh topology [6][7]. In protection scheme, pre assigned backup paths are established at the time of admitting connection request. The primary and backup paths follow the link disjoint constraints in which all the links in a primary path are not selected for setting up backup path. Dedicated protection is an approach where the backup resources are reserved dedicatedly. A network topology with eight nodes and ten links are shown in Fig. 1 to illustrate the dedicated protection. Solid arrows denote the pre configured primary path (P) and backup path (B). Backup paths B1 and B2 are configured at their appropriate nodes during the time of admitting primary paths P1 and P2 respectively. Suppose that, a link failure on primary path P1, backup traffic will be rerouted through backup path B1without any node configuration as B1 is pre configured. Since the network nodes are preconfigured at the time of connection establishment in dedicated protection, this approach has less recovery time to reroute the traffic through backup path in case of component or link failure. This is the advantage over the traditional shared protection method. However, the resources cannot be shared in dedicated protection method which is achieved in shared protection.

A new connection request can be admitted by considering several constraints in dedicated protection. Initially, a primary path must be identified from a source to a destination to route a primary traffic. Secondly, sufficient resources (wavelengths) must be selected in each link of the primary path. Thirdly, a backup path must be identified from the same source and the same destination in order to reroute the backup traffic

978-1-5386-1676-5/17/$31.00 © 2017 IEEE