Optical Switching and Networking 11 (2014) 189–201

Contents lists available at ScienceDirect

Optical Switching and Networking

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

Network coding-based protection ☆

Ahmed E. Kamal *, Mirzad Mohandespour

Department of Electrical and Computer Engineering, Iowa State University, Ames, IA 50011, United States

ARTICLE INFO

Available online 6 July 2013

Keywords:
Network survivability
Protection
Network coding

ABSTRACT

This paper serves as a tutorial lecture on the use of network coding to provide resource efficient and agile proactive protection. Network coding, which was introduced in Ahlswede et al. (2000) [1], allows intermediate network nodes to form linear combinations of packets received on different input links. The use of network coding results in capacity enhancement. This capacity enhancement is used to provide protection channels which are used to carry combinations of redundant data, and are solved by the receivers in order to recover data lost due to network failures.

The paper starts by addressing network coding-based protection of bidirectional unicast connections, and explains the use of p-Cycles to carry linear combinations of the redundant data units. The paper also discusses an earlier protection strategy which is based on diversity coding, in which the linear combinations are formed at special nodes, including sources, and is used to protect unidirectional connections. A generalized network coding-based protection which uses a tree to carry the linear combinations will be presented. Protection of multicast connections using network coding is also explained.

1. Introduction

Network backbones are implemented using optical fibers which provide large amounts of bandwidth. However, the downside of this is that the failure of a single fiber, which is not uncommon, can affect large numbers of users and connections. It is therefore important that if any part of the network fails, the network will continue to operate. This concept of withstanding failures is usually referred to as *network survivability* or *network resilience*.

The area of optical network survivability has been a very active area of research, and many techniques for optical network survivability have been introduced. These techniques can be classified as either *Predesigned Protection* or *Dynamic Restoration* techniques [2]. Predesigned protection is a proactive protection technique, in which bandwidth is reserved in advance so that when a failure takes place, the reserved bandwidth is used to reroute the traffic affected by the failure. These techniques include the 1+1 protection, in which traffic of a lightpath is transmitted on two link disjoint paths, and the receiver selects the stronger of the two signals. They also include 1:1 protection, which is similar to 1+1, except that traffic is not transmitted on the backup path until a failure takes place. The 1:1 technique has been extended to 1:N protection, in which one set of protection circuits is used to protect N paths. A generalization of 1:N is the M:N, where M protection paths are used to protect N working paths. Moreover, the Shared Backup Path Protection (SBPP) [3] is a reactive protection strategy in which protection against failures is provided on an end-to-end basis, i.e., by provisioning a protection path between the two end points of the connection. However, the links in the protection path need not be reserved for the exclusive protection of just one connection, and the protection resources may be

☆ This research was supported in part by grants CNS-0626741 and CNS-0721453 from the National Science Foundation, and a gift from Cisco Systems.

* Corresponding author. Tel.: +1 515 294 3580.
E-mail addresses: aekamal@hotmail.com, kamal@iastate.edu (A.E. Kamal), mirzadm@iastate.edu (M. Mohandespour).

1573-4277/$ - see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.osn.2013.06.006

shared between multiple connections. Two connections with protection paths which overlap must have link disjoint working paths. On the other hand, dynamic restoration, which is a reactive strategy, does not reserve capacity in advance, but when a failure occurs, spare capacity is discovered, and is used to reroute the traffic affected by the failure.

The advantage of protection techniques is that they provide agile recovery from failures. However, they require significant amounts of protection resources, which are at least 100% of primary working resources. On the other hand, restoration techniques are more resource efficient, but are much slower than their protection counterparts.

Many survivability strategies have been developed with the objective of combining the agility advantages of proactive protection, and the resource efficiency of reactive protection, such as 1:N and SBPP. A class of these strategies, which has been introduced recently, is to use the technique of *network coding* [1] to achieve these objectives. Network coding allows intermediate network nodes to perform linear combinations on data units received on different input ports. These combinations are forwarded downstream towards destination nodes, and are then solved to recover original data units. Network coding results in enhancing the network capacity, especially when multicasting is used. Network coding-based protection uses the same concept of network coding to form combinations of redundant data units transmitted inside the network, and these combinations are solved at the receivers, or in some cases by intermediate nodes, in order to recover from data lost due to failures.

Network coding-based protection has a number of advantages. In addition to providing agile proactive protection, failures need not be detected explicitly, and rerouting of the signal is not needed. This results in simplifying both the management and control planes. This strategy can be implemented at a number of layers, including the optical layer and the MPLS layer.

This paper introduces some of the techniques which have been developed in the literature in order to implement network coding-based protection, with emphasis on implementation in optical networks. The next section provides a brief background to network coding, in addition to listing the operational assumptions which will be used in the rest of this paper. Section 3 discusses several techniques which have been introduced for protecting multiple unicast connections. Protection strategies for multicast connections are discussed in Section 4. Section 5 briefly discusses some of the enabling technologies and protocols which can be used to implement network coding-based protection in optical networks. Finally, Section 6 concludes this paper with some summarizing remarks.

2. Background and assumptions

This section provides a brief background to network coding, as well as introduces the operational assumptions.

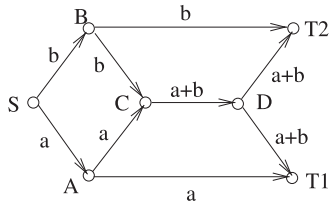

Fig. 1. An example of network coding.

2.1. Background on network coding

Network coding refers to performing linear coding operations on traffic carried by the network at intermediate network nodes. In this case, a node receives information from all, or some of its input links, encodes this information, and sends the information to all, or some of its output links. This approach can result in enhancing the network capacity, hence facilitating the service of sessions which cannot be otherwise accommodated. This is especially true when the service mode is multicasting. An example of the use of network coding is shown in Fig. 1, in which node S transmits to nodes T1 and T2, and each link in the network has a capacity of one data unit per time unit. Data units a and b are delivered to nodes T1 and T2, respectively, using the outer links. At the same time, data units b and a are delivered to T1 and T2 by adding a and b at node C, where the addition is modulo 2. Then, b and a are recovered at T1 and T2 by adding the explicitly received data units (a and b, respectively), to a+b. The network can then achieve a capacity of two data units per time unit, which is the max-flow capacity of this network.

The concept of network coding was first introduced by the fundamental work of Ahlswede et al. [1]. Their main contribution was a theorem which is often referred to as the main theorem of network coding. The theorem simply states that: Given a multigraph $G(V,E)$ and a multicast connection with source s, and a set of k destination nodes $\{d_1, d_2, \ldots, d_k\}$, the multicast rate $r = \min_i(maxflow(s,d_i))$ is achievable under network coding. Here V denotes the set of vertices, E is the set of edges, and the maximum flow from s to each destination d_i is denoted by $maxflow(s,d_i)$. The multicast rate cannot be higher than maximum flow from the source to each destination. Therefore it is upper bounded by smallest maximum flow. The theorem proves that the upper bound is in fact achievable. In the next step Li et al. [4] showed that the multicast rate r can be achieved under linear network coding, i.e., when nodes generate linear functions of their incoming flows. Reference [5] introduced an algebraic characterization of linear coding schemes that results in a network capacity that is the same as the max-flow min-cut bound, when multicast service is used. The authors show that failures can be tolerated through a static network coding scheme under multicasting, provided that the failures do not reduce the network capacity below a target rate.[1] Reference [6] introduced deterministic and randomized algorithms for

[1] Further elaboration on this issue will be presented in Section 4.1 where multicasting protection is addressed.