Optical Switching and Networking 9 (2012) 81–96

Contents lists available at SciVerse ScienceDirect

Optical Switching and Networking

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

A novel Topology Aggregation approach for shared protection in multi-domain networks

Dieu-Linh Truong [a,*], Brigitte Jaumard [b]

[a] Department of Data Communications and Computer Networks, School of Information and Communication Technology, Hanoi University of Technology, Hanoi, Viet Nam

[b] Computer Science and Software Engineering, Concordia University, Montréal, QC, Canada, H3G 1M8

ARTICLE INFO

Article history:
Received 16 January 2010
Received in revised form 18 June 2011
Accepted 30 August 2011
Available online 9 September 2011

Keywords:
Topology Aggregation
Multi-domain networks
Protection

ABSTRACT

Routing for shared protection in multi-domain networks is more difficult than that in single-domain networks because of the scalability requirements. We propose a novel approach for shared protection routing in multi-domain networks where the key feature is a special Topology Aggregation. In this Topology Aggregation, only some potential intra-domain paths (intra-paths for short) are selected for carrying working and backup traffic between domain border nodes. The abstraction of each intra-path to a virtual edge makes the original multi-domain network to become an aggregated network. On the aggregated network, a single-domain routing algorithm for shared protection can be applied for obtaining the complete routing solutions. The experiments show that the proposed approach is scalable. Moreover it is close to the optimal solution in single-domain networks and outperforms the previously proposed scalable solutions in multi-domain networks.

1. Introduction

Many studies have been published for connection protection against failures. Some of them propose protection models such as link, path, segment or p-cycle, the others concentrate on the problem of allocating working and backup resources. When dedicated protection is employed, the resource allocation task is simply finding diverse paths for working and backup connections and can be solved by different diverse path routing algorithms such as those in [1,2].

For the bandwidth saving purpose, shared protection has been proposed for link, path and segment protection [3] or even Overlapping Segment Protection [4], a segment protection model where working segments can overlap each other. In addition to the basic idea of link, segment, overlapping segment and path protection, shared protection for these models allows sharing bandwidth amongst backup elements. Backup elements can be backup link, segment or path, commonly referred to hereafter as "backup segments". Working elements are working link, segment or path and are similarly called "working segments".

In order to guarantee 100% recovery of any single link or node failure, two backup paths/segments are allowed sharing bandwidth if and only if their working segments are link and node-disjoint. This condition is called *sharing condition*, see Fig. 1 for an illustration. In case (a), the working segment from v_1 to v_2, with requested bandwidth d_1, and the working segment from v_5 to v_6, with requested bandwidth d_2, are link and node-disjoint. Their backup segments can share bandwidth over the common link (v_4, v_3) and the needed backup bandwidth on this link is $\max\{d_1, d_2\}$ in order to be able to protect both working paths. In case (b), the two working segments share node v_7, their backup segments cannot share backup bandwidth. The needed backup bandwidth on link (v_4, v_3) is $d_1 + d_2$,

[*] Corresponding author.
E-mail addresses: linhtd@soict.hut.edu.vn (D.-L. Truong), bjaumard@cse.concordia.ca (B. Jaumard).

1573-4277/$ – see front matter © 2011 Elsevier B.V. All rights reserved.
doi:10.1016/j.osn.2011.08.001

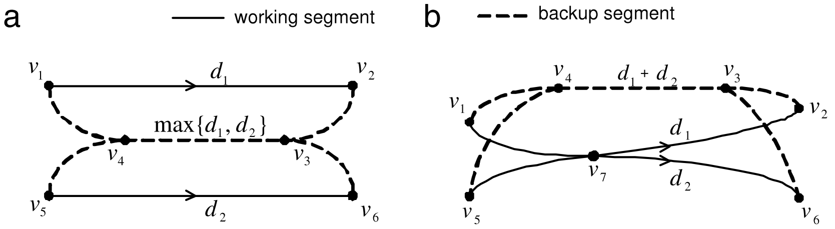

Fig. 1. Examples of cases where two backup segments can share backup bandwidth (a) and cannot (b).

which is greater than in case (a). Hence, the amount of backup bandwidth to be reserved for a backup segment depends on the working segment to be protected as well as on the existing working and backup segments. This dependency makes the routing problem for shared protection complex.

Shared protection under static traffic has received a lot of interest. Several efficient solutions have been proposed, especially the well-known *p*-cycle initially introduced in [5] and further developed for segment protection in [6,7]. However, network traffic today changes dynamically; static traffic is no longer an appropriate assumption except for planning. For this reason, we focus only on dynamic traffic.

For a given new incoming request, the dynamic routing problem for shared protection consists of establishing a working path and associated backup segments for it, while minimising the bandwidth they use. This routing should be done without any forecast on upcoming requests. Some optimal solutions for shared protection in single-domain networks has been proposed, for example the SCI model in [8] or the model in [4]. Several heuristics with smaller computational effort have also been proposed such as the works in [9], PDBWA and PIBWA in [10], SLSP-O in [11], CDR in [12], PROMISE in [13] or recursive shared segment protection in [14]. These works limit themselves to single-domain networks because they need detailed information on bandwidth allocation on each network link for their complex bandwidth cost computations.

Shared protection for multi-domain networks is much more complex than that for single-domain networks due to the network characteristics and size. A multi-domain network is made of the interconnection of several single-domain networks [15], see an illustration in Fig. 2(a). In order to satisfy the *scalability requirements*, only the aggregated routing information can be exchanged amongst domains [16] by an Exterior Gateway Protocol such as BGP. Consequently, a given node is neither aware of the global multi-domain network topology nor of the detailed bandwidth allocation on each network link, although the complete routing information can still be available within each domain thanks to more frequent routing information updates performed by an Interior Gateway Protocol. This characteristic makes the current shared protection routings for single-domain networks inapplicable for multi-domain networks.

Some works address the routing problem in multi-domain networks but very few solutions have been proposed for protection in multi-domain networks. These solutions have been analysed and evaluated in [17,18]. Some of them, e.g. [19–21], do not take care of inter-domain link protection and turn the multi-domain protection into multiple intra-domain protection. The others tackle the scalability issue by using a traditional Topology Aggregation approach such as nodal, full mesh or star model for aggregating each domain. The works in [22,23] proposed to use *p*-cycle protection at both intra-domain level and inter-domain level. Again multi-domain protection using *p*-cycle is a protection scheme for static or relatively stable traffic. Even in the stable traffic context, multi-domain *p*-cycle protection requires very high resource redundancy for protecting 100% links against failure. The works in [24,25] proposed full mesh aggregations. Let us denote a domain $N_m = (V_m, L_m)$, where V_m and L_m are the sets of nodes and links. In those works, the domain is aggregated to become graph $G_m = (V_m^{\text{BORDER}}, V_m^{\text{2BORDER}})$ composed of a border node set V_m^{BORDER} and a virtual link set V_m^{2BORDER} (see Fig. 2(b)). A virtual link connects two border nodes of a domain and represents the set of domain internal paths running between these border nodes. Such a path is called an intra-path. The multi-domain network becomes a so-called inter-domain network. Each virtual link is then associated with approximative working and backup costs. Single-domain routing algorithms for shared protection are used in this inter-domain network for finding the working and backup segments which are paths of virtual and inter-domain links. Virtual links are then mapped back to intra-paths in order to get the full end-to-end paths. In this paper, this approach is referred to as "Route-and-Map" and denoted by R*a*M.

Although R*a*M offers good routing results and scalability, we found that the approximation made in working and backup cost computation leads the inter-domain routing to a solution that is different to the real one obtained after intra-domain routing. In this paper, we propose to eliminate the approximation in R*a*M. The idea is that: between each pair of border nodes, only some best intra-paths are used for carrying traffic. These intra-paths are then exposed as links at inter-domain level. The routing will be performed only in this inter-domain level. This approach can be seen as if we perform the mapping of intra-paths to virtual links first then routing. It is the so-called "Map-and-Route" or M*a*R for short. The advantage of this approach is that working and backup costs of intra-paths (i.e. links of inter-domain network) can be computed exactly and the routing is performed only once on the inter-domain network.

This paper is organised as follows. The next section provides general ideas of the proposed approach. Section 3 states the mapping sub-problem in each domain, its