AN IMPROVED DISTRIBUTED ROUTING PROTOCOL FOR MULTI-DOMAIN OPTICAL NETWORKS USING TOPOLOGY AGGREGATION

Giridhar S Sharma
Dept of Computer Science
Oklahoma State University
Stillwater, OK

Michel Toulouse
Dept of Computer Science
Oklahoma State University
Stillwater, OK

Dieu-Linh Truong
Hanoi University of Science and Technologies
Hanoi, Vietnam

***Abstract*— Multi-domain networks consist of several domains connected together by inter-domain physical links. Routing and failure protection in such networks are complex issues that have only started to receive attention. One source of difficulties lies in the lack of shared information among domains, such as network topologies, bandwidth, and size of the network. This kind of information can only be estimated across the different domains. Truong and Jaumard [1] propose a two-step routing and protection approach where in the first step a topology aggregation and cost estimation is obtained to model the inter-domain network followed by a detailed intra-domain routing step. Different approximation techniques are used to estimate costs and residual bandwidths in the aggregated model of the multi-domain network. But protection and routing interact in a complex manner, which renders difficult these estimations. In this paper, we propose a technique that aims at improving the cost estimation in the aggregated topology.**

***Keywords*— Multi-domain network, protection, routing**.

I. INTRODUCTION

A multi-domain network is an interconnection of several single-domain networks. Communication requests made in one domain can reach destinations in other domains through inter-domain links which connect two border nodes that belong to different single-domain networks. Border nodes have information about the inter-domain connectivity through aggregated information exchanges using protocols such as Border Gateway Protocol (BGP). The detailed information such as topology and bandwidth allocation is available only inside the respective domains. Therefore, no node is fully aware of complete information of other domains.

Different routing and protection protocols have been proposed in the literature for multi-domain optical networks. In [1], Truong and Jaumard propose a protocol based on topology aggregation and shared segments. A topology aggregation is a graph G = (N, V) that stands as a coarse representation of a multi-domain network. In this graph, N represents the set of border nodes and V represents two different types of links connecting border nodes: 1- inter-domain links; 2- virtual links which exist between each pair of border nodes belonging to a same single-domain. Virtual links abstract physical paths between border nodes in a single-domain. Routing (working paths) and protection (backup paths) are initially computed using the aggregated topology of the multi-domain network. In order for routing algorithms to work, cost and residual bandwidth estimates need to be provided for the virtual links. Further, working paths in multi-domain networks tend to be very long, which cost more in bandwidth for protection and for the recovery time from a failure. The paper in [1] seeks to address these issues using shared segments in which working and backup paths are decomposed into segments and where backup segments can share bandwidth to protect working paths. But shared segments render more difficult to get good estimate of the virtual link costs. In this work, we introduce an approach to compute the real cost for some of the virtual links, which we call "real virtual links".

The rest of the paper is organized as follows: section 2 is an introduction to protection protocols in multi-domain networks; particularly those associated to shared segment protection. In section 3, a detail of our proposed heuristic is provided. Section 4 and 5 provide the implementation and the conclusion respectively.

II. SHARED PROTECTION

Protection and restoration are two classes of strategies that address network failures. Protection protocols tend to have a faster recovery time because these protocols reserve at routing time bandwidth on

backup paths to re-route the working traffic from a failed component.

Shared protection is a mechanism to protect against single link or node failure in working paths by sharing bandwidth among backup paths. Shared Segment Protection (SSP) has been proposed to achieve faster recovery in multi-domain networks (see [2] and [3]). Instead of protecting the end-end working path, each working path is divided into segments and these segments are protected individually by other backup segments. It is called shared segment because it still shares the backup bandwidth with other backup segments. However, this approach suffers from one drawback, wherein segment end nodes are not protected. The node failure will affect both working and backup segments. To overcome this drawback, in Overlapping Shared Segment Protection (OSSP) segments overlap each other, protecting both links and nodes. Different working paths in OSSP share the backup bandwidth on same backup link. However, there is one condition where backup path among the nodes cannot be shared, which is called the segment sharing condition. If two working segment are sharing a node or a link, then they cannot share the backup bandwidth. There has to be a separate backup bandwidth which should be reserved on the backup segment.

Fig 2. illustrates the segment sharing condition. As it can be observed in Fig 2 (a), the segments v1→v2 and v3→v4 can share backup bandwidth since both do not belong to the same shared risk group and thus backup bandwidth will be max{d1,d2}. Whereas in (b) there has to be additional bandwidth reserved since the segments share the node v7 and hence they belong to same shared risk group. Thus the total backup bandwidth required would be d1+d2.

III. PROPOSED SOLUTION

Routing is based mainly on costs calculated from the global information available border nodes. The global information is exchanged among the border nodes through protocols such as BGP. However, this information exchange is not that frequent because, through protocols such as BGP. However, this information exchange is not that frequent because,

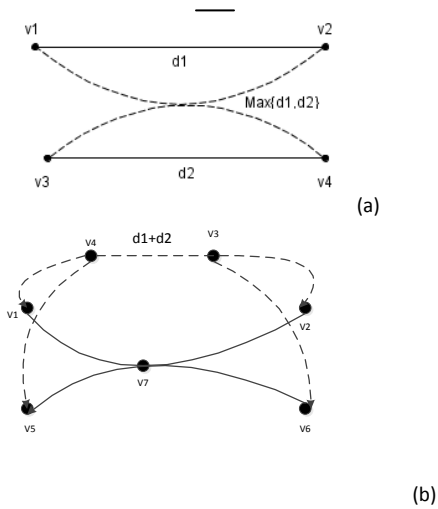

Fig 2 (a) Sharable bandwidth (b) Non-sharable bandwidth

the information is quite large and it creates traffic congestion in the inter-domain links. Hence the calculated cost of a route by a domain in other domain is either outdated or the path may no longer available for routing due to capacity limit on the physical path. In [1], the virtual route is computed in the first step and if there are no intra-domain edges found in second step, the algorithm blocks. However, a solution has been proposed in the same paper, wherein the second iteration similar to inter-domain step is performed to remove blocking virtual edges and then proceeding to the second step, intra-domain routing. Thus the blocking is removed at the cost of this extra iteration. However in the best case, if there was no blocking then, still the cost computed at the first step may be inaccurate.

Let's illustrate the inaccuracy in cost estimation in [1]. For example in Fig 3(a), assume node 7 in D2 is the source of a request and node 1 in D1 is the destination. It might be that the current shortest path to reach 1 from 7 is 7→5→2→1. Until there is an information exchange among border nodes, node 7 may not have this updated information. According to the outdated information at node 7, it might route the request through 7→5→2→4→1 which is an inaccurate shortest path.

To overcome this difficulty, we propose a solution which is based in part on each domain computing a path for the same communication request. Initially, the source of a request informs some border nodes from the different domains of the request destination. Then each domain computes in parallel with the

others a route for the request. The computation in each domain uses the network topology of its domain and the representation of the other domains provided by the aggregated topology. Each route as a routing segment computes with accurate information, the information associated to this segment is mapped to a virtual link for this domain, yielding an accurate cost for this link, which we then called real virtual link. Once this step is completed, some of the virtual links of the aggregated multi-domain topology have accurate cost. Then a working path and a backup path is computed in the aggregated multi-domain network for the same request. Finally the intra-domain routing is computed for the inter-domain links of the multi-domain route computed in the aggregated network. Fig 3(b) shows the real virtual edges by domain 1 colored red. For the above instance assuming node 7 as the source and node 1 as the destination, the solution according to D1 would be as shown in Fig 3(b). Similarly D2 and D3 come up with their solution. These solutions can be compared and combined to get a better approximation. Therefore the calculations and routings are performed in each domain separately and thus leading to more accurate solution than computing the whole cost of the route by a single domain.

IV. SIMULATION

Simulation involves the implementing of a protocol in [1] using the real virtual edge concept. The simulation is coded in C++ using Boost Graph Library (BGL). BGL provides data structures for generating, interfaces for graph manipulation and some basic graph algorithms.

V. CONCLUSIONS

In this paper we are extending the work of paper [1] to improve the cost estimation. The basic heuristics proposed in [1] remain same. However our idea here should improve the cost estimation by computing real virtual edges in each domain to get more accurate cost. It should also improve the cost estimation of the virtual links that have been real virtual links in recent communication requests. This should ultimately contribute to minimize the overall communication cost expresses in terms of the bandwidth used by the working and backup paths.

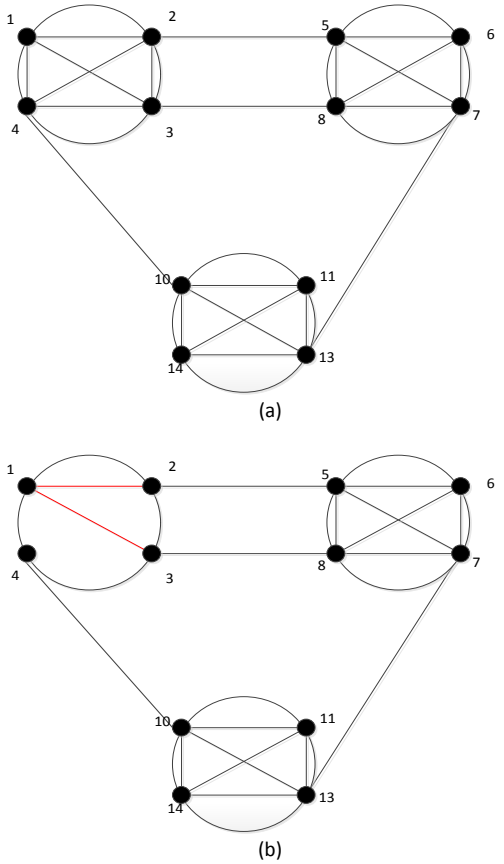

Fig 3. (a) topologically aggregated graph. (b) Real virtual edge in domain 1.

REFERENCES

[1] Truong DL, Joumard B. Using Topology Aggregation for Efficient Shared Segment Protection Solutions in Multi-Domain Networks. IEEE journal on selected areas in communications 2007; vol.25, NO. 9:1-12

[2] Truong DL, Thingoane B. Dynamic routing for shared path protection in multidomain optical mesh networks. Journal of optical Networking 2006; vol.5, No.1:58-74

[3] Truong DL, Joumard B. Recent Progress in Dynamic Routing for Shared Protection in Multidomain Networks. IEEE communications Magazine 2008; 112-119.