Recent Progress in Dynamic Routing for Shared Protection in Multi-domain Networks

Dieu-Linh Truong and Brigitte Jaumard, *Senior Member, IEEE*

***Abstract*— A large number of studies on routing for shared protection focus on minimizing the network transport capacity in a static routing framework. A smaller number of studies have been conducted on dynamic routing. Most of them do not meet the scalability requirements of multi-domain networks. This paper reviews the recent works in dynamic routing for shared protection in multi-domain networks, and proposes a quantitative comparison amongst the most efficient approaches. Some of the remaining challenges are discussed at the end of the paper.**

I. Introduction

Over the last years, many studies have been made on network survivability. Restoration and protection are two main techniques for recovering the network connections from equipment failures or cable cuts. The restoration works in a reactive manner. When a working path fails following a link or node failure, a backup path is searched for replacing the failed working path. The protection works in a pro-active manner. A backup path is searched and reserved for the working path before a failure occurs, generally at the same time as the working path routing. Protection guarantees full recovery whereas the restoration may not if resources are not available at the failure time.

Classical topological protection models are link, segment, path and ring-based protections (Fig. 1). In link protection, each link of the working path is individually protected. In path protection, the end-to-end working path is protected by an end-to-end backup path. In segment protection, each working path is divided into segments and each one is protected by a backup segment. A variant of this protection model is the overlapping segment protection where working segments overlap each other (see, e.g., [9]). In ring-based protection, rings are established in the network with backup capacity and protect the segments that are on-ring or straddling a ring. A well-known instance of the ring-based protection is the p-cycle protection scheme.

Protection is usually studied under a single failure assumption because of its practical meaning. Although many researches focus on link failure only, we consider both link and node failures in this paper. A key characteristic of protection is then that a working entity and its backup elements must be link/node disjoint in order to ensure that at least one of them survives upon a single link/node failure. Link and segment protections leave the segment end nodes unprotected because they are the common points between the working path and backup segments. Path and overlapping segment protection protect all nodes (except for the source and the destination nodes) because each of them is an intermediate node of the path or of at least one segment.

These protection techniques can be deployed in dedicated or in sharing mode. In dedicated mode, resources along a backup path/segment are uniquely reserved for the protection of one working path/segment. In sharing mode, backup paths (or segments) of different working paths (or segments) can share resources and thus spare some backup capacity. Shared protection, whether it is considered for paths, segments or overlapping segments leads respectively to Shared Path Protection (SPP), Shared Segment Protection (SSP) or Overlapping Segment Shared Protection (OSSP).

The routing objective of shared protection is typically minimizing the overall working and backup capacity. While it is easy to identify the working capacity, the resource sharing possibility adds a greater complexity to the estimation of the required backup bandwidth. The reason is that, for a given pair of working and backup paths/segments, the amount of required backup bandwidth varies from one backup link to another, depending on the amount of accumulated sharable backup bandwidth on the link. This sharable bandwidth depends on the routes of the established working and backup paths/segments in the network. Given a request for bandwidth d and the accumulated backup bandwidth $B_{\ell'}$ on link ℓ', the following formula computes the additional backup bandwidth $b^{\ell}_{\ell'}$ needed on link ℓ' for protecting link ℓ when the former is used in a backup path/segment and the latter is used in the corresponding working path/segment (see, e.g., [4] for details):

$$b^{\ell}_{\ell'} = \max\{0, B^{\ell}_{\ell'} + d - B_{\ell'}\}, \tag{1}$$

where $B^{\ell}_{\ell'}$ is the part of $B_{\ell'}$ that cannot be shared for protecting ℓ. It is indeed the backup bandwidth of the requests whose working paths go through ℓ and backup paths go through ℓ'.

Routing for shared protection goes into two major directions: static routing and dynamic routing. In the former, working and backup capacities in the network are set according to a static demand matrix with requested bandwidths either described per connection, per source-destination or per link. Most studies evaluate the amount of backup capacity that is needed, assuming an exact demand matrix, others compute the backup capacity for a working capacity that is bounded by a given working capacity envelope. In any case, with the given demand matrix or the working envelope profile, the complex computation of (1) is not an issue. It is however not the case for dynamic routing.

In dynamic routing, each request or bundle of requests is considered as it comes in without any global knowledge about the traffic matrix. A number of solutions have been proposed for dynamic routing with protection. Most of them

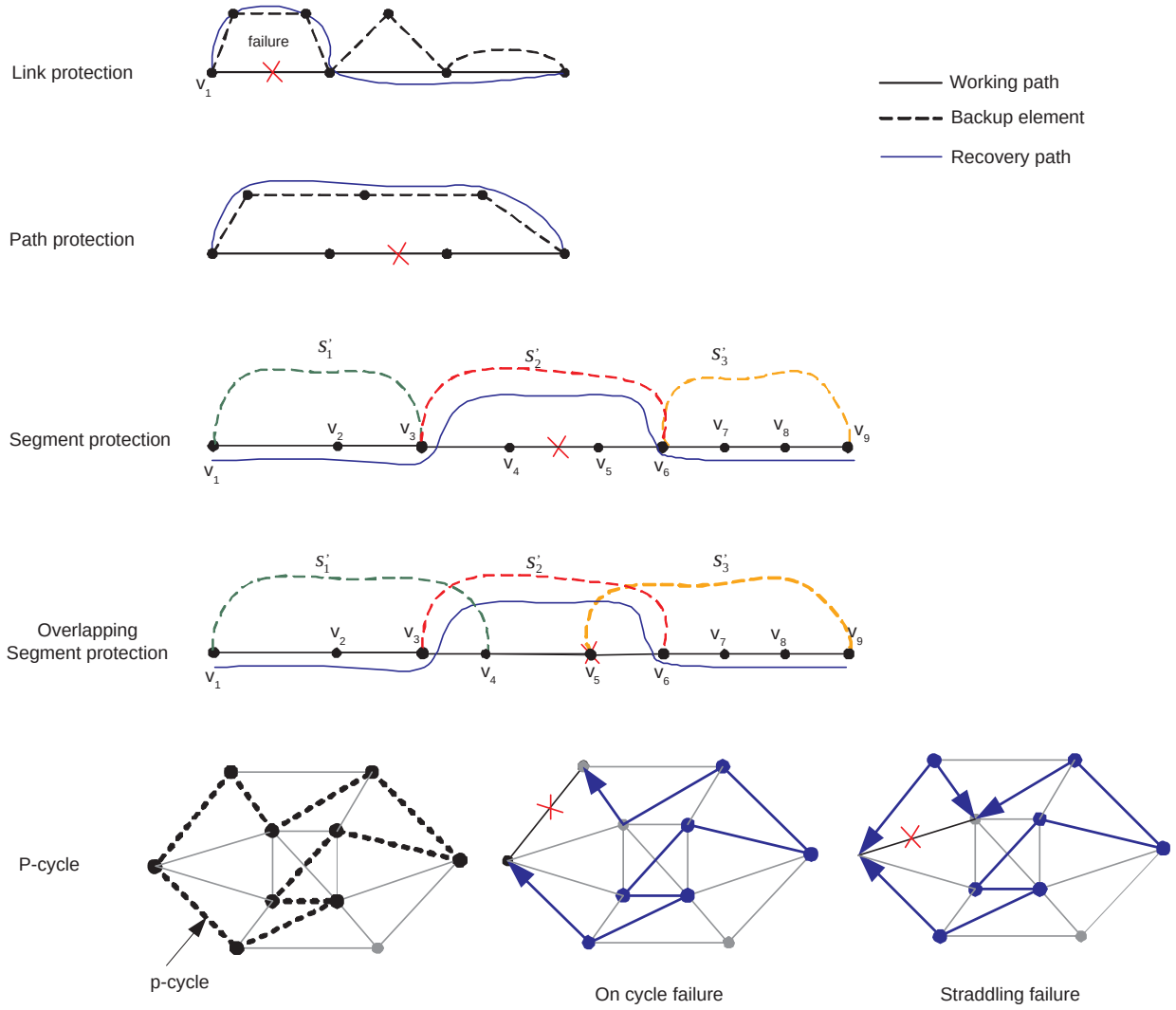


Fig. 1. Classical protection models

perform a sequential routing where the working path is routed first and then the backup path, see [4] for a review that includes, e.g., Iterative Two-Step-Approach (ITSA), Distributed Partial Information Management (DPIM), Active Path First - Potential Backup Cost (APF-PBC), Short Leap Shared Protection (SLSP), Optimal Protection Domain Allocation (OPDA), Cascaded Diverse Routing (CDR) and Protection using Multiple Segments (PROMISE). The other solutions propose joint routings of working and backup paths such as Share with Complete Information (SCI) or the optimal OSSP solution [5]. Whether with a sequential or a joint scheme, proposed solutions use (1) or its variants for computing the backup cost of the incoming request. The up to date bandwidth allocation history on each network link is required for such a computation whenever a request is routed. Such complete and global information can only be freshly available in single-domain networks, therefore the listed solutions are implicitly limited to single-domain networks and are not suitable for multi-domain networks.

A multi-domain network is composed of multiple domains (see Fig. 2). Its important characteristic is the lack of complete and global information which results from the restricted information exchange between domains due to scalability and domain privacy requirements. This explains why most available solutions are not applicable in multi-domain networks.

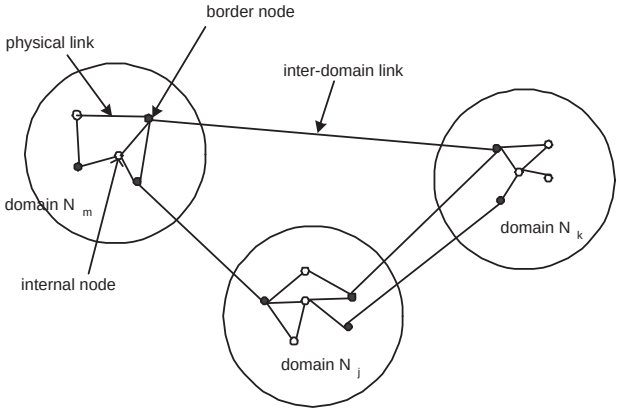


Fig. 2. Multi-domain networks

Multiple intra-domain protections	Akyamac *et al.* [1]	Segment protection. No detailed routing algorithm is given. End-to-end restoration is used when a border node fails.
	Sub-path protection [8]	Segment protection. Static routing. Network does not have any inter-domain link.
	LSSP [3]	Segment protection. Inter-domain links are assumed to be dedicatedly protected by another protection scheme.
HiTA	Multi-domain p-cycles [2]	p-cycles are used in the inter-domain level. Static routing.
	Multi-domain SPP with WPF/JDP [11]	Path protection. Bandwidth cost approximations.
	RaM [9]	OSSP. Bandwidth cost approximations.
	MaR [10]	OSSP. Introduction of potential intra-paths for a non full mesh TA. Exact bandwidth costs.
Others	Huang *et al.* [6]	Proposed for MPLS networks. Detailed routing model is not available.
	Multi-segment protection [7]	Segment protection. Routing is designed only for a multi-domain network with a particular structure.

TABLE I
CLASSIFICATION OF MULTI-DOMAIN PROTECTION SOLUTIONS

Few studies explicitly focused on multi-domain networks.

This paper describes the recent progress in dynamic routing for shared protection in multi-domain networks. The static routing, dedicated protection or the protection in single-domain networks are out of the scope of this paper.

Researches in survivable routing for multi-domain networks proceeds in two major directions: the Multiple intra-domain protections and the Hierarchical routing with Topology Aggregation (HiTA). Table I presents a classification of the proposed solutions that will be reviewed in the next sections.

II. Multiple intra-domain protections

In the Multiple intra-domain protection approaches, a segment-based protection model is often used where a segment spans over a domain. The segment inside each domain is individually protected by using a single-domain protection solution. This approach is quite scalable when the number of domains increases. The question arises as how to protect the border nodes and inter-domain links that are not protected by any domain. This last issue is handled differently in each work. We briefly described them below.

In [8], a sub-path protection is proposed for large networks but not for multi-domain networks. For the protection purpose, the network is divided into domains directly attached to each other and thus inter-domain links do not exist. An independent single-domain protection can be used in each domain. The solution cannot be used for generic multi-domain networks due to the absence of inter-domain links.

In [1], in order to protect inter-domain links, the authors define artificial domains that contains the inter-domain links between any two neighboring domains. A working path is cut into concatenated segments at domain borders, each one belongs to a real or artificial domain and is protected by a backup segment in the same domain. All links including the inter-domain links are protected. However, the border nodes are not protected because they are segment end nodes. When a border node fails, an alternate end-to-end path is searched for replacing the affected working path in a restoration fashion.

A different line of thought corresponds to the Local Segment Shared Protection (LSSP) [3] that addresses the multiple failure issue. Each working segment within a domain is protected by a backup segment in the same domain. The authors assume that each inter-domain link is physically equipped with one dedicated protection link so that LSSP is not responsible for inter-domain link protection.

Although the inter-domain link protection is usually either forgotten or handled by a separate technique in Multiple intra-domain protections, it offers a protection model that is highly scalable since the protections are limited to domain networks and thus no extra routing information needs to be exchanged among domains for backup path/segment routing.

III. Hierarchical routing with Topology Aggregation

A. Overview

In order to deal with the restricted information exchange requirements in multi-domain networks, one can reduce the frequency of information exchanges resulting from out of date routing information if the frequency is below the information change rate. Routing algorithms must be specifically designed to tolerate the out of date information. A second strategy consists of keeping the routing information up to date but with a reduced amount. Most of the existing solutions in Hierarchical routing with Topology aggregation uses the second strategy.

While the Multiple intra-domain protection approach considers the survivable routing in each domain individually, HiTAconsiders it on the whole multi-domain network. In order to deal with the scalability requirement, the multi-domain network is aggregated by a Topology Aggregation (TA) scheme in order to become a simpler network in terms of topology and routing information so that it can be considered as a single-domain network. In such simple network, called aggregated network or inter-domain network, classical protection models such as link, path, segment, OSSP or p-cycles with a single-domain routing can be used. In general, the routing in the aggregated network can sketch out rough routes for working and backup paths/segments. Detailed routings are performed later individually inside each domain in order to refine the rough paths/segments.

HiTA is generally less scalable than Multiple intra-domain protections because some aggregated routing information is needed to be exchanged in the inter-domain scope for refreshing the aggregated network.

B. Topology Aggregation

The TA technique is an important element in each HiTA routing scheme. It includes the topology aggregation and the information aggregation.

1) Aggregation of topology: There are two main aggregation techniques for the topology: mesh aggregation and star aggregation (see Fig. 3a). In mesh aggregation, a domain is transformed into a graph composed of selected border nodes and some virtual links between those nodes. A virtual link represents the set of physical intra-domain paths (or intra-path for short) between its two border nodes. The mesh aggregation technique that creates a virtual link between each pair of border nodes is called full-mesh TA.

In a star aggregation, a virtual node is introduced for each domain. The domain is transformed into a graph composed of some selected border nodes, the virtual node and virtual links connecting the virtual node and the selected border nodes.

Full-mesh TA is more flexible than star TA as the routes between different pairs of border nodes are modeled by independent virtual links while in star aggregation, those routes, once set, all contain the virtual node. However, the full-mesh TA is less scalable than a star TA since the size of the aggregated network increases quadratically in the former case and linearly in the latter case with respect to the original domain size.

2) Aggregation of information - challenges: In the aggregation of topology, some physical links of the original network are eliminated resulting in the loss of routing information associated with those links. Link-states of virtual links are introduced for replacing the lost information. The challenges are: i) how to define those link-states so that they reflect faithfully the routing capacity as well as the original connectivity inside a domain, and then ii) how to use those link-states for estimating the working and backup costs of a request at the aggregation level.

Each routing solution answers these questions in a different way. Link-states usually include free capacity, backup capacity, sharable/non-sharable backup capacity and disjointness between intra-paths of virtual links. Simple and efficient techniques such as Widest shortest path, Shortest widest path, etc., can be used for the aggregation of free capacity. However, it is much more difficult to aggregate the sharable/non-sharable backup capacity or the disjointness due to their high dependency on working and backup path allocation history.

C. Existing solutions in HiTA *class*

1) Multi-domain p-cycles: The main idea of Multi-domain p-cycles [2] is to aggregate the network by using a mesh TA to become an inter-domain network, then using some pre-defined p-cycles for the protection of inter-domain link uniquely. As for intra-domain links, three protection strategies can be applied: no protection, p-cycles, dedicated segment protection. Multi-domain p-cycles corresponds to a network design problem with a static routing.

2) Multi-domain SPP: The work in [11] propose to use shared path protection for multi-domain networks and two routing algorithms for setting the shared protection. The routing follows the HiTA principle.

The network is first aggregated by a full-mesh TA with a tailored information aggregation. A set of link-states for each virtual link containing the residual capacity, allocated backup capacity etc., as well as the formulas to deduce them from the link-states of physical links are proposed. When a request comes in, it is first passed to the inter-domain routing. The problem consists in finding, at the aggregation network level, a pair of disjoint working and backup paths that minimizes the total working and backup costs. Although the exact backup cost can be deduced from (1), it depends on physical link-states that are inaccessible information at the aggregated network level. The authors proposes then formulas to compute approximately the working and backup costs as function of link-states of virtual links. Consequently, the inter-domain routing is feasible at the aggregated network level. Two routing algorithm are proposed: Working Path First (WPF) where the working path is identified first then the backup path, and Joint Directive Path (JDP) where the working and backup path are considered together. After the inter-domain routing, an intra-domain routing is performed inside each domain in order to map each virtual link of the working and backup paths to the least cost intra-path among those represented by the virtual link.

The work [11] is a pioneering one in proposing in detail the link-states for virtual links as well as a way to compute approximately the bandwidth cost of a request at the aggregated network level. This allows a reasonable inter-domain routing.

3) RaM *multi-domain OSSP:* In [9], a series of OSSP routing solutions are proposed that will be referred to as RaM (Route and Map). They use a similar TA and routing steps that are proposed for the Multi-domain SSP in [11]. The differences with the Multi-domain SSP are that the inter-domain step is a single-domain OSSP routing and some link-states of virtual links are defined specifically for OSSP.

The study in [9] is one of the first that offers a short recovery by introducing both working and backup segment length constraints. In comparison with Multi-domain SPP, the working and backup segment lengths are significantly reduced (see Section V-C).

4) MaR *multi-domain OSSP:* The study in [10] presents the so-called MaR (Map and Route) routing approach for OSSP with a quite innovative TA solution regarding the topology as well as the information aggregation aspects.

The idea is as follows. In order to simplify the routing operations in each domain, we use only some intra-paths to carry out the traffic crossing the domain and call them Potential Intra-Paths (PiPs). Those PiPs are abstracted as a single virtual edge and the domain is aggregated as a simple graph made of those virtual edges (see Fig.3 (d)). The detailed information about the physical links taken by each PiP is not advertised outside the domain, thus the domain privacy is preserved and the scalability is fulfilled.

In each domain, the PiP selection is subject to four criteria that helps to reduce the blocking probability of the OSSP routing and encourage the backup bandwidth sharing between backup segments. The criteria are: *i)* minimizing working capacity, *ii)* minimizing backup capacity, *iii)* maximizing the possibility of finding pairwise disjoint PiPs that carry working traffic, *iv)* maximizing the possibility that a pair of virtual links have disjoint PiPs. Each PiP is not only considered as a single edge in terms of topology but also in terms of backup

bandwidth sharing. Two backup segments can share bandwidth if they share an entire PiP.

Unlike most HiTA solutions, MaR performs a unique inter-domain routing in the aggregated network. All single-domain OSSP routing solutions can be used for the inter-domain routing. The intra-domain routing is unnecessary since each PiP corresponds to one intra-path. Again, working and backup segment are restricted in length resulting in a fast recovery.

TA with PiPs brings numerous advantages to MaR. Firstly, the one-to-one correspondence between a virtual edge and a unique intra-path allows identifying exactly the working and backup costs of a request at the aggregated network level and results in a precise routing. Secondly, the single step routing in MaR leads to a better optimization of the bandwidth consumption in comparison with RaM, which uses two separate routing steps. Although the pre-selection of PiPs reduces a priori the intra-path choices for building working and backup segments, the well defined pre-selection criteria help to orient to bandwidth saving and high bandwidth sharing solutions.

IV. Other solutions

We discuss here the solutions that are difficult to classify within the Multiple intra-domain protections or HiTA framework.

In [6], an OSSP routing scheme is proposed originally for MPLS networks but still valid for optical networks. The working path is divided into segments with end nodes at domain borders. Each segment is protected by resources coming from a single-domain and the inter-domain links attached to the domain. No backup bandwidth sharing possibility is taken into account during the routing.

In [7], another OSSP routing scheme is proposed for a special type of multi-domain networks. Indeed, domains are assumed to connect to a backbone region in a star structure through border nodes. Domains do not connect directly to each other. Therefore, a connection starts at the source domain, goes through the backbone region and gets to the destination domain. A border node has a complete view of the backbone and of the domain it belongs to. The combined view of the border nodes of the source domain and the destination domain gives the complete view of the multi-domain network. These nodes can thus perform the routing with complete information without TA. This network model is not realistic as in practice, domains can interconnect directly. A connection may involve several transit domains whose view is not accessible by the border nodes of the source nor the destination domain.

V. Quantitative comparison

In this section, we perform a quantitative comparison amongst the dynamic routing solutions for shared protection. The solutions without detailed routing algorithms such as [1] and [6], the static routing solutions like multi-domain p-cycles [2] and sub-path protection [8], the solutions for particular networks such as [7] are excluded from the comparison.

We therefore compare WPF/JDP, RaM, MaR and LSSP. Results obtained with WPF are denoted by PATH in order to distinguish them from the other ones which are segment-based approaches. JDP is ignored as its results are very similar to those with WPF.

Comparisons are performed on LARGE-8 (see [9]), a multi-domain network with 8 domains generated by using the multi-domain topology generator GT-ITM.

Comparisons are made using the *Backup overhead*, i.e., ratio between the overall working and backup capacity of the network and the smallest working capacity of the network minus 1. This measures the backup bandwidth redundancy of a protection scheme. A protection scheme is bandwidth saving if its backup overhead is small.

A. Bandwidth saving

In [3], the authors compare quantitatively PATH [11] and LSSP on different small size multi-domain topologies. Although the protection of inter-domain links is not taken into account in LSSP, LSSP still consumes about 15%-30% more backup ressource than PATH. LSSP is claimed to provide faster recovery than PATH because working and backup segments are shorter than working/backup paths.

We made additional comparisons for PATH, RaM and MaR under incremental traffic. In Fig. 4a, we compare their performance with that of a single-domain optimal OSSP [5], denoted by Opt, on a small multi-domain network of 28 nodes in order to highlight the trade off between the routing quality and the scalability. For Opt, the multi-domain network is considered as a single-domain one without domain borders. NoShare denotes a dedicated segment protection. We observe that, in general, RaM backup overhead is closed to Opt. MaR backup overhead is mostly equal to the backup overhead of Opt when the working segment length threshold increases revealing that MaR saves as much backup bandwidth as Opt.

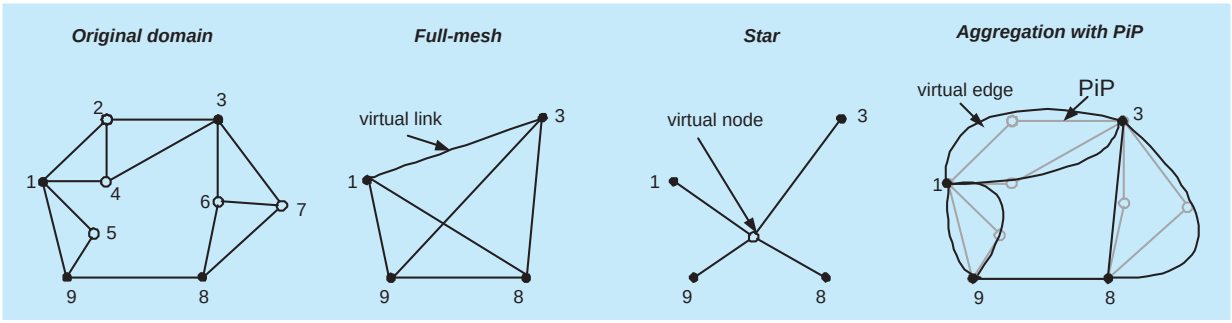
Fig. 4b shows backup overhead for the NoShare, RaM, MaR and PATH schemes in LARGE-8 with incremental traffic. Obviously, RaM, MaR, Opt, as shared protection solutions, save much more backup bandwidth than NoShare. In a little against intuitive way, segment-based protection uses more backup resources than path-based protection, MaR outperforms PATH which, in addition, is not much better than RaM. In conclusion, a good routing strategy can favor a segment-based protection scheme against a path-based protection one as it will be better in terms of backup bandwidth savings.

B. Blocking probability

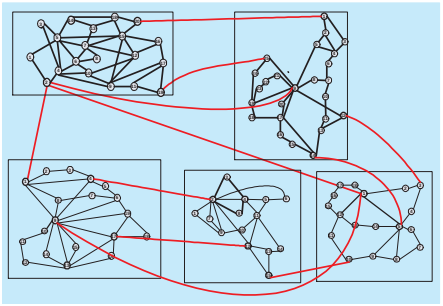
Fig. 4c shows a comparison with respect to the blocking probabilities on LARGE-8 under dynamic traffic. Similar conclusions as for the backup overhead are obtained: NoShare is left far from the other schemes, MaR is as good as PATH and these latter ones offer the lowest blocking probability.

C. Path/segment lengths and recovery times

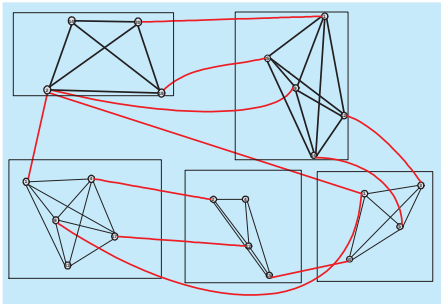
Last, Fig. 4d depicts the comparative results with respect to the segment and path lengths for RaM; unlimited RaM, i.e., RaM when segments are not length constrained, MaR and PATH in LARGE-8. The working segment length threshold



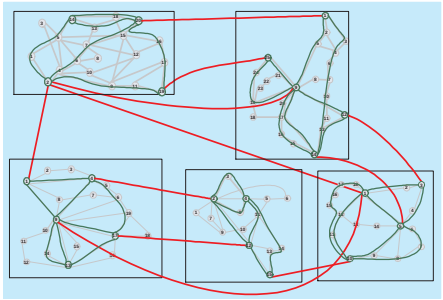
(a) TA techniques



(b) Original multi-domain network



(c) Aggregated network in Full-mesh TA



(d) Aggregated network using PiPs

Fig. 3. Topology Aggregation in each domain and in the multi-domain networks.

is set to 5 links. The working segments of segment-based protections have never been observed longer than the working paths of PATH. With a reasonable segment length threshold, segment protection can offer shorter backup segments in comparison with backup paths of PATH. Since the recovery times is proportional to the working and backup path/segment length, segment protection offers a faster recovery over path protection.

VI. Conclusions

The comparative analysis of the previous section showed that segment and path protection models are competitive in multi-domain networks. With a reasonable segment length threshold, segment protection offers a faster recovery than path protection, which is an asset in large networks. Regarding blocking probability and backup resource savings, segment-based protection, in particular with a MaR routing, can be very close or even outperforms path-based protection.

Although the Multiple intra-domain protection techniques are more scalable than HiTA, they may encounter difficulties in covering the inter-domain region, i.e., border nodes and inter-domain links. The most commonly proposed solution is to add a separate protection scheme for these last elements, leading to a non-homogeneous protection over the network. This implies extra management effort and signaling overhead.

VII. Challenges of the protection in multi-domain networks

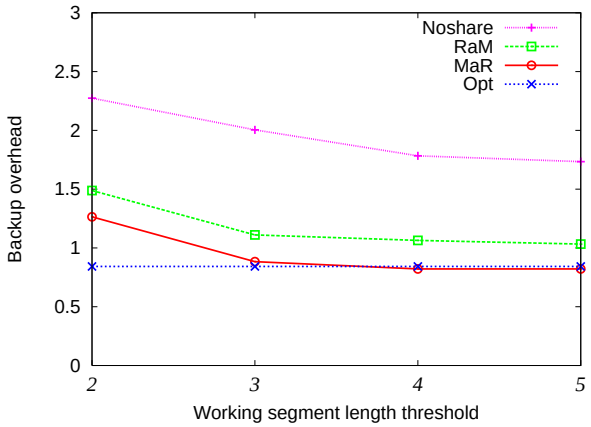
A. Scalability versus the routing quality

The first challenge in the routing operation for shared protection in multi-domain networks is to find the best possible trade off between the scalability and the routing quality. The Multiple intra-domain protection takes advantage of the complete information inside each domain but lacks a global view of the networks, therefore it often ends with a local optimal solution that may be far from a global optimal one. On the contrary, the HiTA-like algorithms addresses the scalability requirement but looses some accuracy due to the use of the aggregated information. Better aggregation, if possible, should be considered for reducing the lost information and preserving the scalability. The non full-mesh TA with PiPs of MaR is a very promising solution.

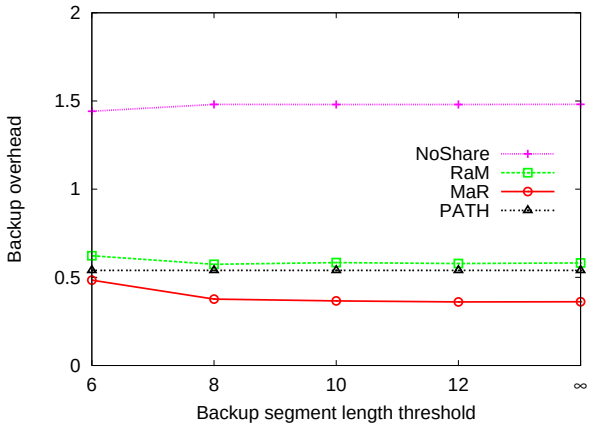
B. Wavelength continuity problem

While the reviewed routing solutions can be widely used for SONET mesh multi-domain networks where OEO conversion are performed at every node, they are not necessarily the best solutions for all optical WDM multi-domain networks due to the wavelength continuity constraint of the latter ones.

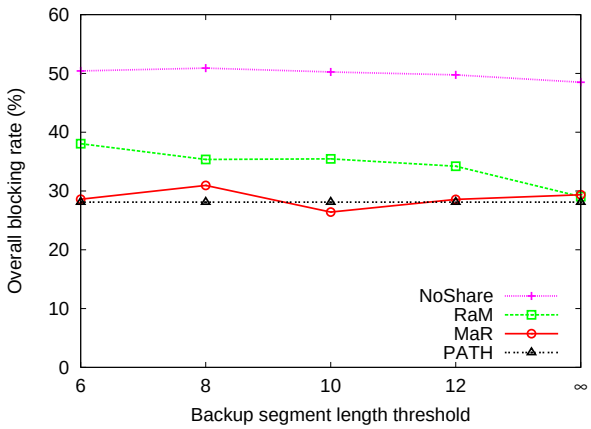
If no wavelength conversion is allowed, the wavelength continuity constraint forces that a WDM connection must use an unique wavelength along all its links. It may be difficult to be satisfied when connections use many links from multiple domains. Moreover, taking this constraint into



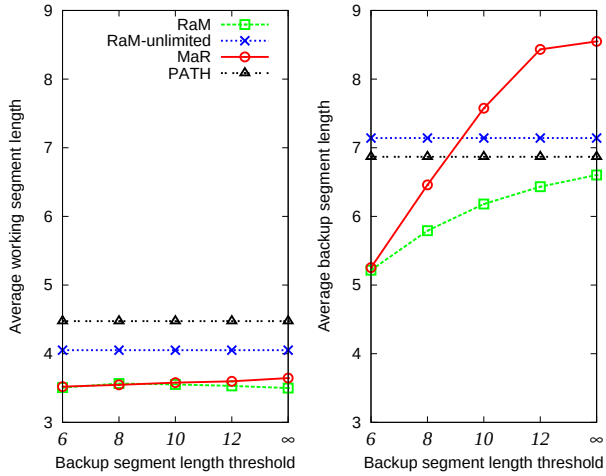
(a) Backup overhead in comparison with single-domain OSSP solutions.



(b) Backup overhead in LARGE-8.



(c) Blocking probability in LARGE-8.



(d) Segment length in LARGE-8.

Fig. 4. Performance of SPP and OSSP solutions in multi-domain networks

account in the routing problem may jeopardize the scalability requirement since it concerns all domains that the connections may go through, and adds one more set of variables (for the wavelength assignment) to the mathematical models. This may explain why, up to now, there has been no work that tackles the shared protection in multi-domain networks with the wavelength continuity constraint. One should not forget the signal attenuation, often dealt with in another step of the network design, and which might be accentuated with the wavelength continuity constraint. It then raises the question when and where to compensate the signal. While these questions and those related to wavelength conversions (including the same questions of when and where) have already been discussed in single-domain networks, there is no study in multi-domain networks except for the MaR one.

C. Other issues

The design of a dynamic and survivable routing in multi-domain networks requires extensions for the control plane. The survivable routing information, i.e., the inputs of the routing algorithms, needs to be exchanged over multiple domains. It varies depending on the routing algorithm. It can be limited to the working and backup allocated capacities or detailed with the backup allocation history on a specific link. This information does not exist in non-survivable multi-domain routing. The existing inter-domain routing protocol, e.g., BGP, needs to be extended by adding new message and/or new working scenarios in order to be able to carry survivable routing information.

Finally, although segment shared protection can bring various advantages to multi-domain networks, its implementation in optical networks in general remains an issue. The segment end nodes must be able to cope with failure notification signal forwarded from intermediate nodes in order to detect a failure and then trigger the recovery process. Such a requirement entails extra equipment costs at intermediate nodes.

REFERENCES

[1] A. Akyamac, S. Sengupta, J.-F. Labourdette, S. Chaudhuri, and S. French, ”Reliability in Single domain vs. Multi domain Optical Mesh Networks,” in Proc. National Fiber Optic Engineers Conference, Dallas, Texas, Sept. 2002.

[2] A. Farkas, J. Szigeti, and T. Cinkler, ”P-cycle Based Protection Schemes for Multi-Domain Networks,” in Proc. International Workshop on Design of Reliable Communication Networks, Italy, Oct. 2005, pp. 223-230.
[3] L. Guo, ”LSSP: A novel local segment-shared protection for multidomain optical mesh networks,” Computer Communications, vol. 30, no. 8, pp. 1794-1801, June 2007
[4] P.-H. Ho, ”State-of-the-art Progress In Developing Survivable Routing Schemes,” IEEE Communications Surveys, vol. 6, no. 4, pp. 2-16, 2004.
[5] P.-H. Ho, J. Tapolcai, and T. Cinkler, ”Segment shared protection in mesh communications networks with bandwidth guaranteed tunnels,” IEEE/ACM Transactions on Networking, vol. 12, no. 6, pp. 1105-1118, Dec. 2004.
[6] C. Huang and D. Messier, ”A Fast and Scalable Inter-Domain MPLS Protection Mechanism,” Journal of Communications and Networks, vol. 6, no. 1, pp. 60-67, Mar. 2004.
[7] T. Miyamura, T. Kurimoto, M. Aoku, and A. Misawa, ”An Interarea SRLG-disjoint Routing Algorithm for Multi-segment Protection in GMPLS Networks,” in Proc. ICBN, Kobe, Japan, Apr. 2004.
[8] C. Ou, H. Zang, N. K. Singhal, K. Zhu, L. H. Sahasrabuddhe, R. A. Mc Donald, and B. Mukherjee, ”Subpath protection for scalability and fast recovery in optical WDM mesh networks,” Journal on Selected Areas in Communications, vol. 22, no. 9, pp. 1859-1875, Nov. 2004.
[9] D. L. Truong and B. Jaumard, ”Using Topology Aggregation for Efficient Segment Shared Protection Solutions in Multi-domain networks,” IEEE Journal of Selected Areas in Communication, vol. 25, no. 9, pp. 96-107, Dec. 2007.
[10] D. L. Truong and B. Jaumard, ”A Map-and-Route Approach for Segment Shared Protection in Multi-domain Networks,” in Proc. High Performance Switching and Routing, Shanghai, China, May 2008.
[11] D. L. Truong and B. Thiongane, ”Dynamic routing for Shared Path Protection in Multidomain optical mesh networks,” OSA Journal of Optical Networking, vol. 5, no. 1, pp. 58-74, Jan. 2006.