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. Restoration works in a reactive manner. When a working path fails following a link or node failure, a backup path is searched for to replace the failed working path. Protection works in a proactive manner. A backup path is searched for and reserved for the working path before a failure occurs, generally at the same time as working path routing. Protection guarantees full recovery, whereas restoration may not if resources are not available at the time of failure.

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 a backup path. In segment protection each working path is divided into segments, and each segment is protected by a backup segment. A variant of this protection model is overlapping segment protection, where working segments overlap each other [1]. 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 ring-based protection is the $p$-cycle protection scheme.

Protection is usually studied under a single failure assumption because of its practical meaning. Although much research focuses on link failure only, we consider both link and node failures in this article. A key characteristic of protection is 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 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 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 to shared path protection (SPP), shared segment protection (SSP), or overlapping segment shared protection (OSSP), respectively.

The routing objective of shared protection is typically to minimize the overall working and backup capacity. While it is easy to identify the working capacity, the resource sharing possibility adds 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.
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 \( B' \) on link \( l' \), the following formula computes the additional backup bandwidth \( b_l \) 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., [2] for details):

\[
b_l = \max\{0, B'_{l'} + d - B_{l'}\},
\]

where \( B'_{l'} \) is the part of \( B' \) 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 through \( l' \).

Routing for shared protection goes in 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 described either per connection, per source-destination, or per link. Most studies evaluate the amount of backup capacity needed, assuming an exact demand matrix; others compute the backup capacity for a working capacity bounded by a given working capacity envelope. In any case, with the given demand matrix or working envelope profile, the complex computation of Eq. 1 is not an issue. This 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 perform sequential routing where the working path is routed first and then the backup path; see [2] for a review that includes the 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 [3]. Whether with a sequential or joint scheme, proposed solutions use Eq. 1 or its variants to compute the backup cost of the incoming request. 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 multidomain networks.

A multidomain network is composed of multiple domains. 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 article describes the recent progress in...
dynamic routing for shared protection in multidomain networks. Static routing, dedicated protection, and protection in single-domain networks are out of the scope of this article.

Research on survivable routing for multidomain networks proceeds in two major directions: multiple intradomain protection and hierarchical routing with topology aggregation (HiTA). Table 1 presents a classification of the proposed solutions that are reviewed in the next sections.

**MULTIPLE INTRADOMAIN PROTECTION**

In multiple intradomain 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 using a single-domain protection solution. This approach is quite scalable when the number of domains increases. The question arises of how to protect the border nodes and interdomain links that are not protected by any domain. This last issue is handled differently in each work. We briefly describe them below.

In [5] subpath protection is proposed for large networks but not for multidomain networks. For protection purposes, the network is divided into domains directly attached to each other; thus, interdomain links do not exist. Independent single-domain protection can be used in each domain. The solution cannot be used for generic multidomain networks due to the absence of interdomain links.

In [4], in order to protect interdomain links, the authors define artificial domains that contain the interdomain links between any two neighboring domains. A working path is cut into concatenated segments at domain borders, each belonging to a real or an artificial domain and protected by a backup segment in the same domain. All links including the interdomain links are protected. However, 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 to replace the affected working path in a restoration fashion.

A different line of thought corresponds to local SSP (LSSP) [6], which 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 interdomain link is physically equipped with one dedicated protection link, so LSSP is not responsible for interdomain link protection.

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

<table>
<thead>
<tr>
<th>Multiple intradomain protection</th>
<th>Akyamac et al. [4]</th>
<th>Segment protection. No detailed routing algorithm is given. End-to-end restoration is used when a border node fails.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>LSSP [6]</td>
<td>Segment protection. Interdomain links are assumed to be dedicatedly protected by another protection scheme.</td>
</tr>
<tr>
<td>HiTA</td>
<td>Multidomain p-cycles [7]</td>
<td>p-cycles are used at the interdomain level. Static routing.</td>
</tr>
<tr>
<td>Others</td>
<td>Huang et al. [10]</td>
<td>Proposed for MPLS networks. A detailed routing model is not available.</td>
</tr>
</tbody>
</table>

**Table 1. Classification of multi-domain protection solutions.**
Hierarchical Routing with Topology Aggregation

Overview

In order to deal with the restricted information-exchange requirements in multidomain 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 out-of-date information. A second strategy consists of keeping the routing information up to date but in a reduced amount. Most of the existing solutions in HiTA use the second strategy.

While the multiple intradomain protection approach considers survivable routing in each domain individually, HiTA considers it on the whole multidomain network. In order to deal with the scalability requirement, the multidomain 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 a simple network, called an aggregated or interdomain network, classical protection models such as link, path, segment, OSSP, or p-cycles with 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 intradomain protection because some aggregated routing information needs to be exchanged in the interdomain scope to refresh the aggregated network.

Topology Aggregation

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

Aggregation of Topology — There are two main aggregation techniques for the topology: mesh and star aggregation (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 intradomain paths (or intrapaths 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, full-mesh TA is less scalable than 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.

Figure 3. Topology aggregation in each domain and in multidomain networks: a) TA techniques; b) original multidomain network; c) aggregated network in full-mesh TA; d) aggregated network using PiPs.
Each PiP corresponds to one intrapath.

**Aggregation of Information: Challenges** — In the aggregation of topology some physical links of the original network are eliminated, resulting in loss of routing information associated with those links. Link states of virtual links are introduced to replace the lost information. The challenges are:

- How to define those link states so that they faithfully reflect the routing capacity as well as the original connectivity inside a domain
- 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 intrapaths of virtual links. Simple and efficient techniques such as widest shortest path or shortest widest path can be used for the aggregation of free capacity. However, it is much more difficult to aggregate the sharable/non-sharable backup capacity or disjointness due to their high dependence on working and backup path allocation history.

**EXISTING SOLUTIONS IN HitA CLASS**

**Multidomain p-cycles** — The main idea of multidomain p-cycles [7] is to aggregate the network by using mesh TA to become an interdomain network, then using some predefined p-cycles for the protection of interdomain links uniquely. As for intradomain links, three protection strategies can be applied: no protection, p-cycles, and dedicated segment protection. Multidomain p-cycles correspond to a network design problem with static routing.

**Multidomain SPP** — The work in [8] proposes to use shared path protection for multidomain 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, and so on, as well as the formulas to deduce them from the link states if physical links are proposed. When a request comes in, it is first passed to interdomain 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 derived from Eq. 1, it depends on physical link states that are inaccessible at the aggregated network level. The authors then propose formulas to approximately compute the bandwidth of a request at the aggregated network level.

**RoM Multidomain OSSP** — In [1] a series of OSSP routing solutions are proposed referred to as RoM (Route and Map). They use similar TA and routing steps as those proposed for multidomain SSP in [8]. The differences from multidomain SSP are that the interdomain step is single-domain OSSP routing, and some link states of virtual links are defined specifically for OSSP.

The study in [1] is one of the first to offer short recovery by introducing both working and backup segment length constraints. In comparison to multidomain SPP, the working and backup segment lengths are significantly reduced.

**MaR Multidomain OSSP** — The study in [9] 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 intrapaths to carry out the traffic crossing the domain and call them potential intrapaths (PiPs). Those PiPs are abstracted as a single virtual edge, and the domain is aggregated as a simple graph made of those virtual edges (Fig. 3d). 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 help reduce the blocking probability of OSSP routing and encourage backup bandwidth sharing between backup segments. The criteria are:

- Minimizing working capacity
- Minimizing backup capacity
- Maximizing the possibility of finding pairwise disjoint PiPs that carry working traffic
- Maximizing the possibility that a pair of virtual links have disjoint PiPs

Each PiP is considered a single edge in terms of not only topology, but also backup bandwidth sharing. Two backup segments can share bandwidth if they share an entire PiP.

Unlike most HitA solutions, MaR performs unique interdomain routing in the aggregated network. All single-domain OSSP routing solutions can be used for interdomain routing. Intradomain routing is unnecessary since each PiP corresponds to one intrapath.

Each PiP performs unique interdomain routing in the aggregated network. All single-domain OSSP routing solutions can be used for interdomain routing. Intradomain routing is unnecessary since each PiP corresponds to one intrapath.
better optimization of bandwidth consumption than RαM, which uses two separate routing steps. Although the preselection of PiPs reduces a priori the intrapath choices for building working and backup segments, the well defined pre-selection criteria help orient bandwidth saving and high bandwidth sharing solutions.

**OTHER SOLUTIONS**

We discuss here solutions that are difficult to classify within the multiple intradomain protection or HiTA framework.

In [10] an OSSP routing scheme is proposed, originally for multiprotocol label switching (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 interdomain links attached to the domain. No backup bandwidth sharing possibility is taken into account during the routing.

In [11] another OSSP routing scheme is proposed for a special type of multidomain network. Indeed, domains are assumed to connect to a backbone region 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 to which it belongs. The combined view of the border nodes of the source and destination domains gives the complete view of the multidomain network. These nodes can thus perform 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 or destination domain.

**QUANTITATIVE COMPARISON**

In this section we perform a quantitative comparison of the dynamic routing solutions for shared protection. Solutions without detailed routing algorithms such as [4, 10], static routing solutions like multilongin p-cycles [7] and subpath protection [5], and solutions for particular networks such as [11] are excluded from the comparison.

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

Comparisons are performed on LARGE-8 [1], a multidomain network with eight domains generated using the multidomain topology generator GT-TM.

Comparisons are made using the backup overhead, that is, the 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.

**BANDWIDTH SAVING**

In [6] the authors quantitatively compare PATH [8] and LSSP on different small-size multidomain topologies. Although the protection of interdomain links is not taken into account in LSSP, LSSP still consumes about 15–30 percent more backup resources 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, RαM, and MoR under incremental traffic. In Fig. 4a we compare their performance with that of a single-domain optimal OSSP [3], denoted Opt, on a small multidomain network of 28 nodes in order to highlight the trade-off between routing quality and scalability. For Opt, the multidomain network is considered as a single-domain one without domain borders. NoShare denotes dedicated segment protection. We observe that, in general, RαM backup overhead is close to Opt. MoR backup overhead is mostly equal to the backup overhead of Opt when the working segment length threshold increases, revealing that MoR saves as much backup bandwidth as Opt.

Figure 4b shows backup overhead for the NoShare, RαM, MoR, and PATH schemes in LARGE-8 with incremental traffic. Obviously, RαM, MoR, and Opt, as shared protection solutions, save much more backup bandwidth than NoShare. Slightly counterintuitively, segment-based protection uses more backup resources than path-based protection; MoR outperforms PATH, which, in addition, is not much better than RαM. 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.

**BLOCKING PROBABILITY**

Figure 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 behind the other schemes, MoR is as good as PATH, and these latter ones offer the lowest blocking probability.

**PATH/SEGMENT LENGTHS AND RECOVERY TIMES**

Lastly, Fig. 4d depicts the comparative results with respect to the segment and path lengths for RαM; unlimited RαM (i.e., RαM when segments are not length constrained), MoR, and PATH in LARGE-8. The working segment length threshold is set to five 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 than the backup paths of PATH. Since recovery time is proportional to working and backup path/segment length, segment protection offers faster recovery than path protection.
CONCLUSIONS

The comparative analysis of the previous section showed that segment and path protection models are competitive in multidomain networks. With a reasonable segment length threshold, segment protection offers 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 $M\alpha_R$ routing, can be very close to or even outperform path-based protection.

Although the multiple intradomain protection techniques are more scalable than HiTA, they may encounter difficulties in covering the interdomain region (i.e., border nodes and interdomain links). The most commonly proposed solution is to add a separate protection scheme for these last elements, leading to nonhomogeneous protection over the network. This implies extra management effort and signaling overhead.

CHALLENGES OF PROTECTION IN MULTIDOMAIN NETWORKS

SCALABILITY VS. ROUTING QUALITY

The first challenge in the routing operation for shared protection in multidomain networks is to find the best possible trade-off between scalability and routing quality. Multiple intradomain protection takes advantage of the complete information inside each domain but lacks a global view of the networks; therefore, it often ends with a locally optimal solution that may be far from a globally optimal one. On the contrary, HiTA-like algorithms address the scalability requirement but lose some accuracy due to the use of aggregated information. Better aggregation, if possible, should be considered for reducing lost information and preserving scalability. The nonfull-mesh TA with PiPs of $M\alpha_R$ is a very promising solution.

Figure 4. Performance of SPP and OSSP solutions in multidomain networks: 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.
WAVELENGTH CONTINUITY PROBLEM

While the reviewed routing solutions can be widely used for synchronous optical network (SONET) mesh multidomain networks where opto-electronic-optical OEO conversion is performed at every node, they are not necessarily the best solutions for all-optical wavelength-division multiplexing (WDM) multidomain networks due to the wavelength continuity constraint of the latter ones.

If no wavelength conversion is allowed, the wavelength continuity constraint forces a WDM connection to use a unique wavelength along all its links. It may be difficult to satisfy when connections use many links from multiple domains. Moreover, taking this constraint into account in the routing problem may jeopardize the scalability requirement since it concerns all domains through which the connections may go and adds one more set of variables (for wavelength assignment) to the mathematical models. This may explain why until now there has been no work tackling shared protection in multidomain networks with the wavelength continuity constraint. One should not forget the signal attenuation, often dealt with in another step of network design, which might be accentuated with the wavelength continuity constraint. It then raises the question of 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 multidomain networks except for MoR.

OTHER ISSUES

The design of dynamic and survivable routing in multidomain networks requires extensions of the control plane. The survivable routing information (i.e., the inputs of 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 nonsurvivable multidomain routing.

The existing interdomain routing protocol (e.g., Border Gateway Protocol) needs to be extended by adding new messaging and/or working scenarios in order to be able to carry survivable routing information.

Finally, although segment shared protection can bring various advantages to multidomain networks, its implementation in optical networks in general remains an issue. The segment end nodes must be able to cope with a 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


BIOGRAPHIES

DIEU-LIH TRUONG (linhtd@it-hut.edu.vn) received her Ph.D. from the Department of Computer Science and Operations Research, Université de Montréal, Canada in 2007. She is currently a professor with the Department of Information Technology, Hanoi University of Technology, Vietnam. Her interests include multidomain networks and survivability.

BRIGITTE JAUMARD (bjaumard@cisse.concordia.ca) holds a Concordia University Research Chair on the Optimization of Communication Networks in CIiSE, Concordia University. She is an active researcher in combinatorial optimization, with a focus on applications in telecommunications.