A Survey of Survivability in Multi-Domain Optical Networks

Hamza Drid[*,a], Bernard Cousin[**,a], Miklos Molnar[**,a,b], Samer Lahoud[**,a]

[a] *Campus universitaire de Beaulieu 35042 Rennes CEDEX, France.*
[b] *INSA of Rennes -IRISA- 35043 Rennes Cedex, France*

Abstract

Network survivability is becoming an important issue and a topical subject in WDM optical mesh networks. Many works have studied network survivability. However, few works have focused on survivability in multi-domain optical networks. This paper reviews the literature on survivability against failures in multi-domain optical networks. The main objective of this study is to evaluate and analyze existing solutions and to compare their performance in terms of different criteria: resource utilization, ratio of rejected connections and recovery time.

Key words: multi-domain, survivability, p-cycle, topology aggregation, optical network

1. Introduction

The development of Wavelength Division Multiplexing (WDM) technologies has increased enormously the transmission capacity of optical networks. However, any failure in the network can result in huge data loss and a lot of traffic being blocked. For this reason, operators must incorporate survivability considerations during the network design process. Survivability means that the network has the ability to maintain an acceptable level of service even after a failure within the network. This requirement becomes more critical as the size and usage of networks increase.

The literature offers a wide range of protection mechanisms against various types of failure [15]-[23]. However these works are generally addressed at single-domain protection, because they assume that each node in the network has complete vision of the physical topology of the entire network. Such an assumption is not realistic in the case of large networks like multi-domain networks. A multi-domain network is a network composed of several single-domain networks, interconnected by inter-domain links. Each single domain can be regarded as an independent network that has its own local rules of operation and management to provide services [4]. Due to scalability constraints and domain management policies, the internal topological details of a domain are usually not shared externally. As a result, no node in a multi-domain network can have complete information on the multi-domain network. For instance, complete information would correspond to the detailed states of wavelength usage on each link of the multi-domain optical network. Thus, the protection of multi-domain networks is more difficult than that of single-domain networks.

Although survivability in multi-domain optical networks is very important, only a few studies have been proposed in the literature. In this paper, we first introduce general concepts and elements related to survivability. We then survey current research on survivability in multi-domain optical networks, discussing their capabilities and performance. Many of these proposals are designed to handle the most frequent failure in optical networks, which is a single link/node failure. Moreover, these works have been proposed for protecting connections at the light-path level. Basically, all these works try to find a trade-off between different concurrent goals: efficient use of backup resources and fast recovery time. To evaluate these works, we have considered different comparison criteria: resource utilization, recovery time and ratio of rejected connection.

The rest of the paper is organized as follows. In Sections 2 and 3, we present some concepts on survivability in WDM networks and elements related to multi-domain optical networks. In Section 4, we describe the main solutions proposed in the literature addressed at survivability in multi-domain networks, we also analyze

[*]Corresponding author
[**]Principal corresponding author
Email addresses: hamza.drid@irisa.fr (Hamza Drid), bernard.ousin@irisa.fr (Bernard Cousin), molnat@irisa.fr (Miklos Molnar), bernard.ousin@irisa.fr (Samer Lahoud)

the advantages and drawbacks of each solution. The numerical results and conclusion are presented in Sections 5 and 6.

2. Survivability in WDM Optical Networks

Networks are subject to a number of component failures, such as links, nodes and wavelength channels . A single network failure may seriously damage end-user applications and interrupt network services. Therefore, it is imperative to incorporate survivability mechanisms in the network to guarantee network services.

Survivability can be provided on different layers of the network [24], such as the IP, MPLS, SONET/SDH, and WDM layers. Although each of the higher layers may have its own recovery mechanism, it is interesting to ensure survivability on the WDM layer since it presents a number of advantages compared to survivability on higher layers, such as fast service recovery, efficient resource utilization and transparency of protocols [21].

Methods for ensuring survivability in WDM networks can be classified into two main classes: restoration [22] and protection [23]. Restoration is a reactive approach in which a backup light-path is searched and established after a failure on the primary light-path occurs. This has the advantage of low overhead in the absence of failures. Protection is a pro-active approach in which the backup light-path is identified and its resources are reserved at the time of establishing the primary light-path itself.

Since failures may cause huge data and revenue loss, protection is considered the favourite mechanism for survivability in WDM networks. This is because it guarantees full recovery whereas restoration may not, if resources are not available, and it has faster recovery time as all backup light-paths are pre-established. However, the stated advantages of protection over restoration come at the expense of a higher consumption of bandwidth resources.

Protection schemes can be classified according to the type of resources protected (link-based versus path-based) [17-18] and according to the type of resources used for protection (dedicated versus shared) [19-20]. In link-based protection, for each link of a primary light-path a backup light-path is identified. Upon the failure of a link, the end nodes of the failed link are immediately switched to the backup light-path. Whereas in path-based protection, one backup light-path is selected to protect all links in the primary light-path. The failure notification message informs the source and destination nodes of each primary path that traverses the failed link/node. Path-based protection is more efficient in capacity utilization compared to link-based protection since only one backup path is required to protect all links in the primary light-path. Recovery time in link-based protection is faster than in path-based protection since the path mechanism requires a longer time to generate a failure notification message.

Dedicated protection sets up two disjoint paths (primary/backup) in the network for each connection demand. The resources for backup paths are dedicated for only one connection. In the shared protection scheme, different backup light-paths can share resources if their primary light-paths do not fail simultaneously [16].

3. Characteristics of Multi-Domain Networks

3.1. Network Model

A multi-domain optical network composed of M connected domains can be represented by a graph $G = (D_i, E)$ for $i = 1, 2, , M$, where D_i and E represent, respectively, the graph of domain number i and the set of inter-domain links (links that connect two border nodes in different domains). The domain i is denoted as $D_i = (GN_i, IN_i, IL_i)$ $(1 \leq i \leq M)$, where GN_i, IN_i and IL_i represent the set of border nodes, the set of interior nodes and the set of intra-domain links in domain i, respectively. An intra-domain link connects nodes of the same domain.

An interior node can view only local network information, it supports only the intra-domain routing in its own domain. A border node can view both the local network information and the global network information of the multi-domain virtual topology and it can perform intra-domain routing in its own domain and inter-domain routing in multi-domain network. We call the nodes through which a primary light-path enters domain D_i Domain Ingress Nodes (DIN_i) and the nodes through which a primary light-path exits domain D_i Domain Egress Nodes (DEN_i).

In this work, without loss of generality, we assume that all links are bi-directional and contain w available wavelengths. Optical connections are established in the network. Each connection demand requires one wavelength on all links traversed by its primary light-path. We also assume that each node in the network has full wavelength conversion capacity, hence wavelength assignment is not the focus of our work. Rather, our aim is to compare multi-domain survivability schemes, so this assumption is made for simpler calculation.

The type of failure considered in this study is a single failure. This means that when a failure occurs, the

affected link or node is repaired before a second failure occurs. This assumption simplifies the management of protection while satisfying the real requirements of network operators.

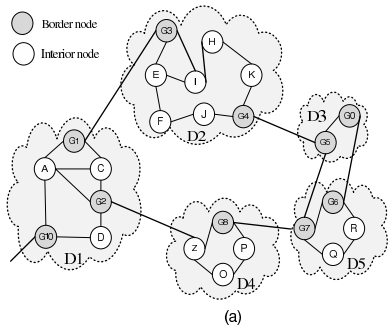

Figure 1: A multi-domain network

In Figure 1, the gray nodes denote border nodes and the white nodes denote interior nodes. Domain D1 has three internal nodes (A, C, D) and three border nodes (G10, G1, G2).

3.2. Topology Aggregation Models

A single domain network is controlled by one authority and generally has a small size. Therefore, each network node of a single domain network can get access to all the information on the single domain network (e.g. physical topology, available resources) and can perform intra-domain routing. Unlike a single domain network, in multi-domain networks, domains generally belong to different operators and the size of the entire network is very large. Consequently, for reasons of confidentiality and scalability, the detailed topology of each domain is not communicated outside the domain.

To make the network scalable in order to be able to compute efficient primary and backup light-paths, various solutions have been proposed. These solutions can be classified into two classes: frequency reduction and quantity reduction. In the first class, the frequency of topology updates is reduced without compromising routing performance. In the second class, the size of information exchanged between domains is reduced while preserving routing performance.

In this paper, we consider quantity reduction only, because it can solve both confidentiality and scalability problems, by hiding and reducing at the same time the physical topology information exchanged between operators. The topology size reduction can be realized using a topology aggregation process. It is a process that allows the representation of the internal topology of each domain in a compact and abstract manner.

There exist several proposed topology aggregation models [10-12]. The models discussed in this work include the Single Node model, the Full Mesh model and the Star model. All these models aim to summarize the topology of the routing domains as accurately as possible.

Single-node aggregation model: this model reduces a routing domain with multiple nodes and links to a single virtual node. The single-node aggregation model offers the greatest reduction of topology because it reduces the size complexity of routing information to O(1). Routing information size represents the number of data broadcast by a domain to its neighbors. In the single node aggregation model, the number of routing data advertised is one. This information represents the best, worst or average values of all the QoS parameters along all the links within the original domain. Figure 2(a) illustrates a single-node virtual topology of the multi-domain network shown in Figure 1.

Full-mesh aggregation model: this model constructs a topology composed only of border nodes, which are connected by virtual links. The complexity of this model is higher than the previous model (O(1/2.BN^2), where BN is the number of border nodes). Figure 2(b) illustrates a full-mesh virtual topology of the multi-domain network shown in Figure 1.

Star aggregation model: this model provides a compromise between the two previous models, in which all border nodes are connected via virtual links to a virtual central node as shown in figure 2(c). The complexity of this model is O(BN).

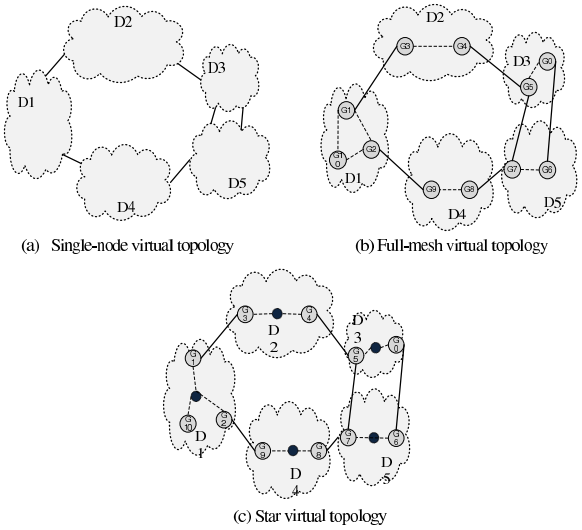

Figure 2: Topology aggregation models

4. State-of-the-Art

This section reviews the various solutions proposed to solve the challenges of survivability in multi-domain optical networks. Moreover, this section analyzes these solutions and shows their advantages and disadvantages.

4.1. RSM: "Reliability in single domain versus multi-domain optical mesh networks"

In reference [1], the authors consider a particular model to represent multi-domain optical networks. In this model, the domains are considered to be connected by two pairs of border nodes, primary and secondary. The primary pair of border nodes acts as the restoration point for links and interior node failures, whereas the secondary border nodes are used to restore against the failure of the primary border nodes. The set composed of the border nodes (primary and secondary) and the inter-domain links connecting two neighboring domains is considered to be a single domain. In this model, the primary light-path is divided into a set of segments, with each segment belonging to one domain. The segment length is limited by the border nodes of the domain and each segment is protected by a backup segment in the same domain.

According to this approach, the protection is done locally, inside each domain, and this can result in faster restoration. However, it consumes considerable resources for protection because many different backup segments are required for protecting one end-to-end primary light-path: one for each traversed domain. In addition, the authors assume the presence of at least two pairs of border nodes connecting two neighboring domains (primary and secondary). However, such an assumption is not always fulfilled in real networks.

4.2. SPSFR: "Subpath protection for scalability and fast recovery in optical WDM mesh networks"

In reference [2], a sub-path protection for multi-domain networks is proposed. It is a particular case of shared path protection. In this solution, after computing the primary light-path in the physical topology of the multi-domain network, each domain protects the segment of the primary light-path which crosses it. To facilitate protection, the authors assume that the domains are connected directly together at border nodes. In other words, inter-domain links don't exist. The backup resources are shared only among backup segments in the same domain. Sub-path protection can even employ different protection schemes in different domains (like Dedicated Protection Schemes) to provide protection based on differentiated quality of service (QoS).

This solution offers acceptable recovery time, however the authors make the strong assumption that domains are connected directly together at border nodes. This assumption is not realistic in the context of multi-domain networks.

4.3. ESPP: "Shared path protection in multi-domain optical mesh networks"

In reference [3], the authors propose Extended Shared Path Protection (ESPP) intended for multi-domain networks. In shared path protection, the spare resources can be shared among different backup light-paths as long as those light-paths do not fail simultaneously [16]. This approach proceeds in two steps: In the first step, the topology of multi-domain networks is aggregated into a single virtual topology on which the primary light-path and backup light-path are calculated. The aggregated virtual topology is composed of virtual domains, which are inter-connected by inter-domain links. The aggregation model used to aggregate the domains is the full-mesh model.

Each virtual link is associated with primary and backup costs. These costs are calculated using primary and backup light-paths existing in the network. In the second step, an intra-domain routing is performed inside each domain in order to map each virtual link of the primary and backup light-paths onto the physical topology.

The advantage of this solution is that it can get a close to optimal primary/backup light-path pair. In other words, it can find a close to optimal disjoint (primary/backup) light-paths between any two nodes in the sense that the total length of these paths is minimized. However, the recovery time is very long. This results from the fact that the backup light-path is routed across the entire network. Moreover, the nodes performing the restoration are the source and destination nodes, and failures have to be notified to all nodes on the primary light-path.

4.4. LSSP: "Local segment-shared protection for multi-domain optical mesh networks"

To improve the recovery time of ESPP and avoid the notification of failures to all nodes on the primary light-path, Local Shared Segment Protection (LSSP) for multi-domain networks is proposed [4].

The main idea of LSSP is that each domain protects the segment of the primary light-path which crosses it.

Consequently, the end-to-end primary light-path is protected. LSSP selects the available path with the minimum number of virtual link hops as the primary light-path on the virtual topology, and then maps each virtual link of the primary light-path onto the intra-domain physical topology. Finally, for each intra-domain primary light-path, a segment-shared backup is computed.

This approach is rather scalable since each network operator protects its domain links independently of other domains. But the authors assume that the inter-domain links are equipped with one dedicated protection link, which is a restrictive assumption.

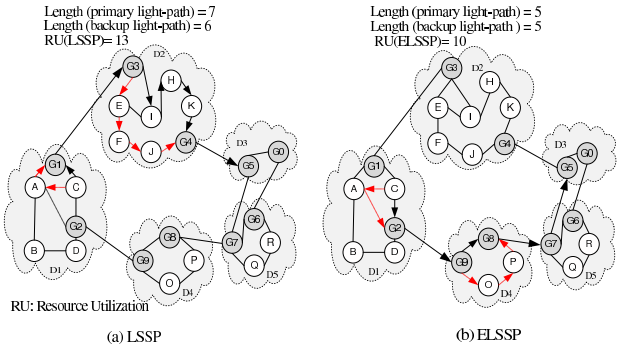

Figure 3: LSSP versus ELSSP

4.5. *ELSSP: "Segment-shared protection for dynamic connections in multi-domain optical mesh networks"*

As we have mentioned previously, the primary light-paths calculated by LSSP correspond to the shortest paths in the virtual topology of multi-domain networks. Note that the cost assigned by LSSP to the virtual links and inter-domain links of the virtual topology is unitary (i.e. one hop count). Such a cost hides all the physical topology of each domain and affects the quality of primary light-path computed on this topology.

To overcome this drawback, the authors of reference [5] propose ELSSP. The main idea of ELSSP is to assign to each virtual link a cost depending on the physical topology and updated according to the current state (available wavelengths on each physical link) of each domain. Therefore, the quality of primary light-paths calculated by ELSSP is improved. Then, each primary light-path is divided and protected in the same way as LSSP.

The following example shows how LSSP and ELSSP compute the primary light-path. Figures 3(a) and 3(b) illustrate LSSP and ELSSP, respectively, where black arrows denote the primary light-path and red arrows denote the shared-segment backup light-path. We can see that LSSP uses 7 (resp. 6) wavelength links for the primary (resp. backup) light-path, whereas ELSSP uses 5 (resp. 5) wavelength links for the primary (resp. backup) light-path. So ELSSP reduces the utilized network resource for the connection request from node C in Domain 1 to node G5 in Domain 3.

We can see in Fig. 3 that ELSSP is more efficient than LSSP in terms of resource utilization. However, the authors considered neither the protection of inter-domain links nor border nodes in their proposal. This makes this solution less attractive and incomplete.

4.6. *LBDDR: "A novel domain-by-domain survivable mechanism in multi-domain wavelength-division-multiplexing optical networks"*

To improve ESPP, LSSP and ELSSP, the authors of reference [6] propose load-balanced domain-by-domain routing (LBDDR) for survivability in multi-domain optical networks. The main idea of LBDDR is that, for each connection request, two disjoint light-paths (primary / backup) are computed without the need of either the virtual topology or the physical topologies of multi-domain networks. This solution uses domain-by-domain routing (DDR) to find the intra-domain primary sub-path and backup sub-path in each single domain to form the efficient inter-domain primary light-path and backup light-path for each connection request.

The DDR solution can be expressed as follows: first, DDR checks whether the source node and destination node are both in the same domain. If this is the case, two link-disjoint light-paths (primary and backup light-paths) from source node to destination node are computed.

In the other case, the source node computes two disjoint light-paths (primary/secondary) from the source node to the nearest border node in the same domain. The selected border node in the neighboring domain is considered as the new source node and it executes the same process applied by the original source node. This process continues until the destination node is reached. The authors assume that the different domains are directly connected by border nodes. In order to reduce the probability of blocking, LBDDR proposes a new load-balanced routing method, which encourages the traffic to be uniformly distributed over the links.

The advantage of this solution is that the domains do not need to exchange topology information amongst themselves in order to achieve routing. The main drawback of this solution is that the light-path calculation is

not well controlled, because the nodes involved in the computation have no idea about the topology on which the primary light-path will be calculated. The second drawback that can be cited is that the authors neither considered the protection of inter-domain links nor the protection of border nodes in their work.

4.7. SSPP: "A shared sub-path protection strategy in multi-domain optical networks"

In reference [7], the authors propose a new solution which improves the recovery time of ESPP and overcomes the drawback of solutions which ignore the protection of border nodes and inter-domain links. It eliminates the notification of failures to all the nodes on the primary light-path. Its main idea is to divide the computed primary light-path into several segments, and then compute for each segment two intra-domain backup segments to protect the intra-domain links, and one inter-domain backup segment to protect the inter-domain link and border nodes.

The primary light-path is computed in the same manner as in the ESPP solution. This light-path is divided into several segments. Each segment begins at border node DIN_i and ends at border node DEN_{i+1}.

The segment is protected as follows: each domain locally protects the part of the segment that crosses it, i.e., D_i protects the $DIN_i - DEN_i$ part and D_{i+1} protects $DIN_{i+1} - DEN_{i+1}$. And then domains D_i and D_{i+1} collaborate and compute a backup light-path from DIN_i to DEN_{i+1} protecting failure on border nodes DIN_{i+1} and DEN_i. This will automatically protect the inter-domain link $DEN_i - DIN_{i+1}$.

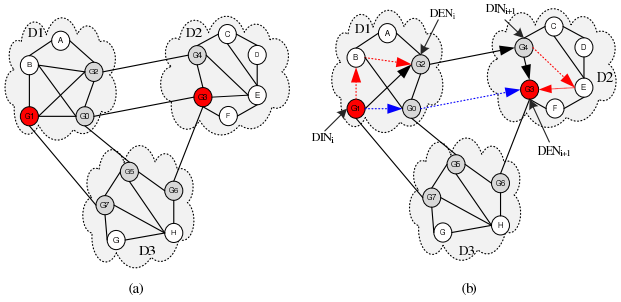

Figure 4: SSPP

Figure 4 show how SSPP works. The primary physical light-path obtained after the first step is G1-G2-G4-G3 where G1 is the source node and G4 is the destination node. The computed primary light-path in our example contains one segment. The DINs along the primary light-path are G1 and G4. The DENs are G2, G3. The intra-domain backup sub-segments of sub-segments G1-G2 and G4-G3 are G1-B-G2 in domain D1 and G4-E-G3 in domain D2. The inter-domain backup sub-segments protect the border nodes G2 and G4 and the inter-domain link G2-G4 is G1-G0-G3.

This solution eliminates the notification of failures to all the nodes on the primary light-path, as a result the recovery time is reduced. The major drawback of this solution is that it still consumes more backup resources than ESPP. In addition, there is no guarantee of finding a backup light-path which protects the border nodes and inter-domain links when the protection is limited between two domains.

4.8. "p-Cycle Protection in Multi-domain Optical Networks"

In reference [8], the authors propose a solution for a multi-domain network protection based on p-cycles [9]. The main goal of this solution is to protect the inter-domain links. This solution proceeds in three steps. In the first step, the set of p-cycles protecting the inter-domain links is computed. This set of p-cycles is computed over a single-node virtual topology (cf. Fig. 5(b)), in which each domain is represented by a single virtual node. The second step consists in determining for each p-cycle calculated in the previous step (e.g. in Fig. 5(b) the set of p-cycles is composed of one p-cycle: D1-D3-D2-D4-D1), the border nodes to which the links of the p-cycle (the on-cycle [1] and straddling links [2]) are connected. In Fig. 5(c) the on-cycle links are G-A, B-K, H-P and M-T, the straddling links are D-Z, D-Y and C-M. The border nodes connected to the on-cycle inter-domain links of a p-cycle are called the on-cycle border nodes (CBN) and those connected to straddling inter-domain links are called straddling border nodes (SBN). In Fig. 5(c), the CBNs are : G, A, B, K, H and P, the SBNs are D, Z, Y, C and M. Moreover, in this step, the end nodes of inter-domain on-cycle and straddling links need to be connected internally to assure continuity of the p-cycle (cf. Fig. 5(c)). The internal links connecting the CBN and SBN nodes are virtual. During the last step, each internal virtual link calculated in the second step is translated into a physical light-path. Note that, in this solution, the calculated p-cycles bypass the intra-domain links without the possibility of protecting them.

However, this approach presents some drawbacks related to the quality of the set of p-cycles protecting the

[1] An on-cycle link is a link which belongs to the p-cycle

[2] A straddling link is a link which does not belong to the p-cycle but whose two end-nodes are on the p-cycle.

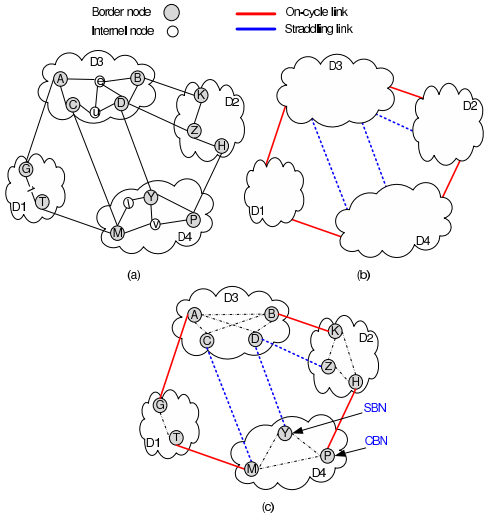

Figure 5: P-cycle in multi-domain networks

inter-domain links. At first, the p-cycles protecting the inter-domain links are computed over a single virtual-node topology. This virtual topology reduces a domain with multiple links and nodes to a single virtual node. Such a representation hides all the topological information describing the domain. Consequently, the real cost of a p-cycle on the physical topology is unknown. The second drawback which we can point out with this solution is due to the fact that the set of p-cycles obtained is designed only to protect the inter-domain links. One of the advantages of a p-cycle is that some of the communications within each domain can be protected by the existing p-cycles, without using additional resources. Those communication links that can be protected freely are those passing through the intra-domain links crossed by the existing p-cycles.

5. Analysis and Simulation Results

5.1. Simulation model

In this section, we present a qualitative and quantitative evaluation in order to compare the performance of the various solutions described. First, we make a quantitative comparison between the solutions which consider a generic model of multi-domain network topology (topology composed of domains interconnected via inter-domain links) and dynamic traffic (ESPP, LSSP, ELSSP and SSPP).

The solutions which have a particular network such as RSM, SPSFR and LBDDR are not considered in this comparison. In LBDDR and also in SPSFR, the authors assume that the domains are connected directly together at border nodes (i.e. inter-domain links do not exist). This is not the case in the remaining solutions: ESPP, ELSSP, SSPP and LSSP, which consider the existence of inter-domain links. As a result, a comparison is not possible because inter-domain links change the cost of the primary and protection paths. Concerning RSM, it is valid only for a particular kind of network. Moreover the routing algorithm is not described. Afterwards, we present a qualitative comparison between all the solutions presented.

The simulation experiments are performed on the network topology represented in Figure 6 and taken from reference [14]. The topology is composed of a simplified version of the European research network GEANT2 interconnected to research and education networks (RENs) participating in the MUPBED project. Between two different domains, the node-pair is interconnected by a bi-directional fiber link. Each fiber link is assumed to have 32 wavelengths and each network node is assumed to have full wavelength conversion capacity.

The traffic model used in our simulations is the incremental traffic model [25], in which connection requests (for a random source and destination) enter the network sequentially. Once a connection request is satisfied, the light-path setup stays in the network and it is never released. Incremental traffic is simpler than dynamic traffic but allows for testing of online algorithms. This assumption is reasonable in current backbone optical networks where traffic is less flexible and connections remain for a long time. Each demand requests for one unit of capacity (i.e., one wavelength). We suppose also that there are no waiting queues in the network nodes, i.e., if the connection is blocked (there are no available resources), the network discards it directly.

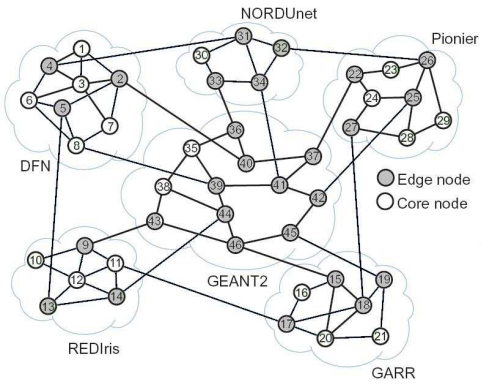

Figure 6: Test topology

5.2. Performance metrics

Several metrics are used to evaluate the effectiveness of the various proposed solutions. These metrics are considered to measure the capacity efficiency and recovery time of the proposed solutions. They include resource utilization, ratio of rejected connection and average primary backup light-path length.

Resource Utilization (RU): This constitutes a major evaluation criterion for WDM network design [22]. It gives an insight into the quality of protection. The RU can be defined as the sum of the total backup and primary wavelength resources. Low RU is more efficient than high RU due to the fact that high RU requires a large capacity to establish and protect the connection against failures.

RU = Σ Primary capacity + Spare capacity

Ratio of rejected connection (RRC): This metric measures the ratio of connections that are rejected because of the lack of wavelength on the links. It is the probability that a request entering the network will be rejected. It corresponds to the ratio between the number of connection requests that are rejected to the total number of connection requests. Formally, RRC is computed as follows:

RRC = Σ rejected connection requests / Σ connection requests

Recovery time: The recovery time is an important measure for the quality of any survivability scheme. It refers to the time between the occurrence of a network failure and the time at which the affected traffic is rerouted through the backup light-path. It includes both the notification and configuration times. The notification time is the time required to notify the failure to the nodes concerned in the primary light-path. The configuration time is the time required to configure the nodes on the backup light-path. Smaller primary and backup light-paths lead to faster recovery time. Clearly, the recovery time depends on the primary and backup light-path lengths. Short light-path length leads to a fast recovery time.

Generally speaking, the recovery time for one connection is indicated by the mean number of hops in the primary/segment-primary light-path and its backup light-path. In our simulation, the recovery time is defined as the ratio of the sum of all recovery times to the total number of primary/segment-primary light-paths. The recovery time can be expressed as following:

$$Recovery\ \ time = \frac{\sum length((P+B)/2)}{nbr\_of\_primary/segments\ \ light\_paths}$$

Where P is the primary/segment-primary light-path and B is the backup light-path which protects it.

5.3. Analysis

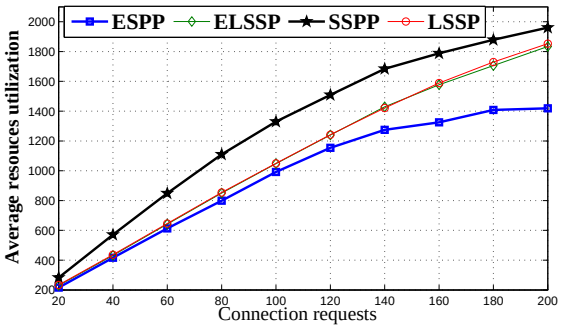

Figure 7: Resource utilization

In Figure 7, the evolution of the average resource utilization as a function of the number of connection requests in the network is displayed. We can see that the average resource consumption of ESPP is better than the other solutions. The reason for this is that LSSP, ELSSP and SSPP assign multiple local segment-backup light-paths in each single domain while ESPP assigns only one backup light-path across multi-domains so that ESPP consumes fewer backup resources than the other solutions.

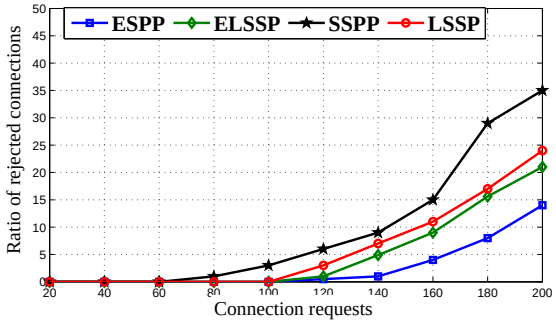

Figure 8: Ratio of rejected connections

With regard to the second metric, figure 8 shows the evolution of RRC as a function of the number of connection requests in the network.

This figure shows clearly that the RRC values of the ESPP solution are lower and better than the other solutions. In fact, it is clear that the mechanism which consumes more bandwidth has a higher blocking probability. Visibly, the positive difference between the RRC values of ELSSP and LSSP is also totally due to the quality of the primary light-paths in ELSSP.

Since the recovery time is an important performance for the quality of any survivability scheme, we also eval-

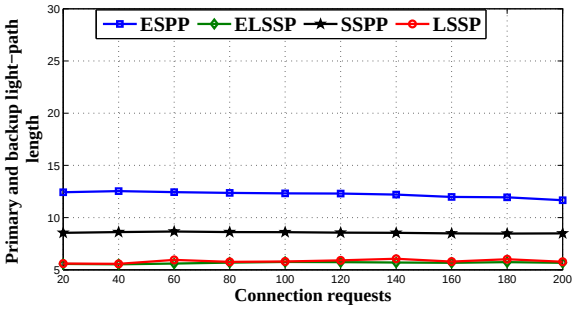

Figure 9: Recovery time

uate the solutions described in terms of recovery time. In our simulation the recovery time is expressed as the average length of primary and backup light-paths. A short length means faster recovery time. Figure 9 depicts the evolution of primary and backup light-path length as a function of the number of connection requests in the network.

Although, ESPP is more efficient in capacity utilization than the other solutions, the length of primary and backup light-paths in ESPP is very long. This difference is due to the fact that, in ESPP, the backup light-paths are computed over the entire multi-domain network topology because the source and destination nodes of each individual primary light-path are responsible for switching the traffic onto a backup light-path. Consequently, the recovery time of ESPP is very long. In the case of LSSP, ELSSP and SSPP, each domain protects the segment of the primary light-path that crosses it. As a result, the lengths of the backup light-paths and their primary segment light-paths are reduced.

Figure 10 presents a qualitative comparison of the different approaches for survivability in multi-domain optical networks.

As regards protection coverage, only the ESPP and SSPP approaches can protect any type of failure in the network. However, ESPP has a very long recovery time because the nodes that are responsible for switching the traffic onto a backup light-path are the source and destination nodes of each individual primary light-path. Also, although SSPP can protect all types of failure, it consumes a lot of resources. To facilitate protection, most of the solutions presented have made very restrictive assumptions. For example, the presence of two pairs of border nodes connecting two neighboring domains (RSM), or assuming that the inter-domain links are equipped with one dedicated protection link as in LSSP, ELSSP and LBDDR. None of these assumptions are valid for multi-domain optical networks. Concerning p-cycles, an important property of p-cycles is that the cycles are fully pre-configured with pre-planned spare capacity and, when a link fails, only the two end nodes of the failed link need to perform the recovery actions, and no switching actions are required at any intermediate nodes of the cycles. This property greatly improves p-cycles recovery time.

6. Conclusion

In this paper, we have addressed survivability in multi-domain optical networks. The main objective of this study is to survey and analyze the various existing solutions proposed for survivability in multi-domain optical networks. Among the solutions presented, a few (SPSFR, LBDDR) assume that the domains are connected directly together at border nodes. Some (LSSP, ELSSP) do not consider the protection of inter-domain links or border nodes in their proposal. According to this study, we can see that despite the various solutions proposed, there is no solution that satisfies all the constraints imposed by multi-domain optical networks.

It appears that survivability in multi-domain optical networks is an active area of research and it would be interesting to propose a solution which combines the advantages of several solutions. For instance, combining the ESPP solution which has good resource utilization with p-cycles which have fast recovery times.

Finally, we consider that these solutions represent a first step in providing solutions to a challenging problem: survivability in multi-domain optical networks.

References

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

[2] 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, 2004, pp. 1859-1875.

[3] D. Truon and B. Thiongane, *Dynamic routing for shared path protection in multi-domain optical mesh networks*, Journal of Optical Networking, 2006, pp. 58-74.

[4] L. Guo, *LSSP: A novel local segment-shared protection for multi-domain optical mesh networks*, Computer Communications, 2007, pp. 1794-1801.

[5] X. Zhang, D. Liao, S. Wang and H. Yu, *On segment shared protection for dynamic connections in multi-domain optical mesh networks*, International Journal of Electronics and Communications, 2009, pp. 1-6.

[6] L. Guo et al., *A novel domain-by-domain survivable mechanism in multi-domain wavelength division-multiplexing optical networks*, International Journal of Optical Fiber Technology, 2009, pp. 192-196

Criteria / Solutions	Protection coverage				Ressource utilisation	Recovery time	Assomptions
	Interior nodes	Border nodes	Interior Links	Inter-domain Links			
RSM [1]	Yes	Yes	Yes	Yes	Bad	Medium	Bad
SPSFR [2]	Yes	Yes	Yes	No	Medium	Medium	Bad
ESPP [3]	Yes	Yes	Yes	Yes	Good	Bad	Good
LSSP [4]	Yes	No	Yes	No	Medium	Medium	Bad
ELSSP [5]	Yes	No	Yes	No	Medium	Medium	Bad
LBDDR [6]	Yes	No	Yes	No	Medium	Medium	Bad
SSPP [7]	Yes	Yes	Yes	Yes	Bad	Medium	Good
p-Cycles [8]	No	No	No	Yes	Bad	Good	Good

Figure 10: Qualitative comparison

[7] X. Xie, W. Sun, W. Hu and J. Wang, *A shared sub-path protection strategy in multi-domain optical networks*, Proc. Optical Fiber Communication and Optoelectronics Conference, 2007.

[8] J. Szigeti, R. Romeral, T. Cinkler and D. Larrabeiti, *p-Cycle Protection in Multi-Domain Optical Networks*, Photonic Network Communications, 2009, pp. 35-47.

[9] W. D. Grover and D. Stamatelakis, *Cycle Oriented Distributed Preconfiguration: Ring-like Speed with Mesh-like Capacity for Self-planning Network Restoration*, Proc. IEEE International Conference on Communications, 1998, pp. 537-543.

[10] B. Awaebuch and Y. Shavitt, *Topology aggregation for directed graphs*, Presented at IEEE Symposium on Computers and Communications, 1998.

[11] W. Lee, *Minimum equivalent subspanner algorithms for topology aggregation in ATM networks*, Presented at 2nd International Conference on ATM, 1999.

[12] K. R. Bhutani, A. Battou and B. Khan, *Two Approaches for Aggregation of Peer Group Topology in Hierarchical PNNI Networks*, International Journal of Intelligent Automation and Soft Computing, 2000.

[13] G. Maier, C. Busca and A. Pattavina, *Multi-Domain Routing Techniques with Topology Aggregation in ASON Networks*, ONDM2008, Spain. 2008.

[14] E. D. Manley, H. S. Hamza and J. S. Deogun, *On the Bandwidth Efficiency of Pre-Crossconnected Trails*, IEEE International Conference on Communications, UK, June 2007.

[15] Q. Zheng and G. Mohan, *Multi-layer protection in IP-over-WDM networks with and with no backup lightpath sharing*, Computer Networks Journal, 2006, pp. 301-316.

[16] D. Zhou, S. Subramaniam, *Survivability in optical networks*, IEEE Network, 2000, pp.16-23.

[17] H. Zang, C. Ou and B. Mukherjee, *Path-protection routing and wavelength assignment (RWA) in WDM mesh networks under duct-layer constraints*, IEEE/ACM Transactions on Networking, 2003, pp. 248-258.

[18] P. Ho, J. Tapolcai and T. Cinkler, *Segment shared protection in mesh communications networks with bandwidth guaranteed tunnels*, IEEE/ACM Transactions on Networking, 2004, pp.1105-1118.

[19] P. Ho and H. Mouftah, *Shared protection in WDM mesh networks*, IEEE Communications Magazine, 2004, pp. 70-76.

[20] C. V. Saradhi and C. S. R Murthy, *Dynamic establishment of differentiated survivable lightpaths in WDM mesh networks*, Computer Communications, 2004, pp. 273-294.

[21] H. Drid, , B. Cousin, S. Lahoud and M. Molnór, Multi-criteria p-cycle network design, IEEE Conference on Local Computer Networks, Montreal, Canada, Oct 2008, pp. 361-366.

[22] S. Ramamurthy and B. Mukherjee, *Survivable WDM mesh networks- Part I: Protection*, Proc. IEEE INFOCOM, Mar. 1999, pp. 744-751.

[23] S. Ramamurthy and B. Mukherjee, *Survivable WDM mesh networks- Part II: Restoration*, Proc. IEEE Integrated Circuits Conf., June 1999, pp. 2023-2030.

[24] N. Ghani et al., *Control plane design in multi-domain/multi-layer optical networks*, in Proc. IEEE Communications Magazine, 2008, pp. 78-87.

[25] D. Eric et al., *Deogun On The Bandwidth Efficiency of Pre-Crossconnected Trails*. Proc. of IEEE International Conference on Communications, 2007, pp. 2294-2299.