Evaluating the Efficiency of Shortcut Span Protection

Sarah Ruepp, Lars Dittmann, Michael Berger
DTU Fotonik
Technical University of Denmark
Ørsteds plads, B 343, 2800 Kgs. Lyngby
Denmark
{srru,ladit,msbe}@fotonik.dtu.dk

Thomas Stidsen
DTU Management
Technical University of Denmark
Produktions torvet, B 426, 2800 Kgs. Lyngby
Denmark
thst@man.dtu.dk

Abstract: This paper presents a comparison of various recovery methods in terms of capacity efficiency with the underlying aim of reducing control plane load. In particular, a method where recovery requests are bundled towards the destination (Shortcut Span Protection) is evaluated can compared against traditional recovery methods. The optimization model is presented and our simulation results show that Shortcut Span Protection uses more capacity than the unbundled related methods, but this is compensated by easier control and management of the recovery actions.

Key–Words: Resilience, Linear Programming, Simulation, Networking, Control Plane

1 Introduction

Network resilience has been a widely studied topic both in industry and in academia. A large amount of resilience mechanisms have been defined for linear, ring, mesh and hybrid topologies, covering both static protection and dynamic restoration [1–5]. There are two main directions of research within the network survivability area. The first one deals with capacity minimization, where mathematical models are applied to provide resilience to the network with the least amount of additional capacity (i.e. restoration overbuild). The other research direction focusses on how recovery mechanisms can be practically implemented in communication networks, so that they are efficient without overburdening the control and management plane. While most research is conducted in either one of these fields, it is important to be aware of that there exists a trade-off between high capacity efficiency and simplicity of the control. This is due to the fact that the high granularity of recovery requests desired for capacity minimization means that a large number of smaller connections must be recovered in case of a failure. A new type of mesh protection which takes this trade-off into account, so-called Shortcut Span Protection (SSP) was presented in [6, 7].

Traffic engineering deals with the issue of planning the utilization of existing networks and the expansion of existing networks. To facilitate good traffic engineering, optimization methods are often utilized, e.g. [8–10]. In [8] the expansion of a multiservice IP network is considered. Using Linear Programming and Mixed Integer Programming, the design of a network, regarding the necessary size of the links, is considered. It is concluded that Mathematical Programming (i.e. both LP and MIP) are valuable tools when dealing with traffic engineering. While Mathematical Programming is a strong tool it is often not possible to use it due to either the size of the optimization problem or the complexity of the planning problem. In Traffic Engineering it is often necessary to deal with several issues at the same time, i.e. both minimizing costs and at the same time minimizing the delay. In [10] and in [9] multi-objective optimization problems are handled using evolutionary algorithms. In [10] routing of GMPLS paths is considered. A four dimensional objective is applied, minimizing both the maximal delay, the average delay, the cost and the maximal flow on a path. Given a four-dimensional objective function, Mathematical Programming is not an option. The four-dimensional objective function is minimized using an evolutionary algorithm, the result being a number of possible routing plans, each of these being pareto-optimal. In [9] a similar routing problem, now regarding lightpaths, is optimized such that the number of necessary wavelengths is minimized, and at the same time the maximum attenuation and the total delay is also minimized. In [9] it is demonstrated how the complex routing probem can be optimized as in [10] using an evolutionary algorithm.

In this paper, we evaluate SPP by simulation to compare the capacity requirements to well known protection methods.

The remainder of this paper is organized as follows. Section 2 presents background information on optical networking. Network topologies are detailed in 3 and control plane mechanisms for optical networks are shown in section 4. Section 5 presents the evaluated recovery methods. The mathematical model is detailed in section 6. In section 7, the simulation study is presented. Section 8 shows the simulation results and section 9 concludes the paper.

2 Optical networking

Optical networks have been developed as the solution to accommodate the high bandwidth demands of our information society. Traditionally, optical networks have been controlled in a centralized structure with manual interaction. This approach is however inefficient with a dynamic traffic pattern, which creates the need for distributed and highly flexible control mechanisms, where the network can be self-controlling by automatically setting up, tearing down and recovering connections when required. According to the ITU an optical network can be modelled as a *transport* plane (i.e. data plane), a *control* plane and a *management* plane [11], shown in figure 1. The transport plane refers to the logic and hardware responsible for the physical transfer of data. The control plane covers the infrastructure and distributed intelligence that controls the establishment and recovery of connections in the network. The management plane encompasses systems, interfaces and protocols used to manage the network and its services [12].

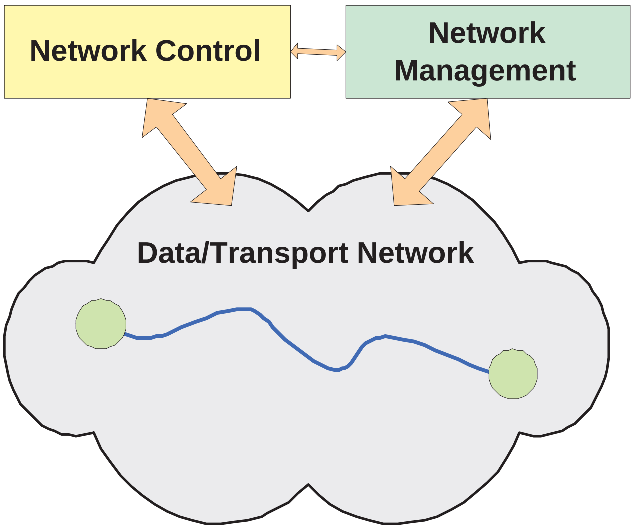

Figure 1: Data, control and management plane.

During the past years, significant development of both the control plane and data plane has occurred. GMPLS [13], ASON [14], and the UNI [15]/NNI [16] specifications are emerging as promising candidates to dynamically control optical networks. Considerable development has also occurred within the data plane. ROADM and OXC, having true optical cores allowing rearrangeability between ports [17] and possibly change of wavelength, have recently been accepted as viable solutions by industry. These components represent a new generation of optical network elements seeking to gradually realize the all-optical network vision hitherto mostly considered in academia. The interaction of the control and data plane is discussed in this paper with the main focus of increasing network survivability.

3 Network Topologies

The structure in which the cables and nodes within an optical network are interconnected is referred to as a network topology. The most common topologies [18] are illustrated in figure 2 and described below:

- Linear/point-to-point: the simplest topology to provide connectivity between two nodes. Currently point-to-point is still the most used topology for the application of WDM networks. This simple topology is the building block of more advanced topologies.
- Ring: an efficient way of interconnecting a group of nodes, because it reduces the fiber usage compared to point-to-point.
- Mesh: can be seen as a combination of the ring and the point-to-point topologies. The greatest advantage of the mesh topology is its flexibility, both when provisioning and protecting connections. Core networks are moving from ring to mesh topologies, because a mesh network is cheaper in terms of fibers, network cards, switches, etc., than if advanced services and protection should be provided in simpler topologies [19].

4 Network Control Plane

4.1 Control Plane Functions

The control plane is responsible for the following functions [12], which are illustrated in figure 3:

- Neighbor discovery: allows a network element to automatically discover its neighbors.
- Routing: covers (a) automatic topology and resource discovery (i.e., propagation of connectivity and resource information); and (b) path computation (i.e., identifying a suitable path using available topology and resource information).

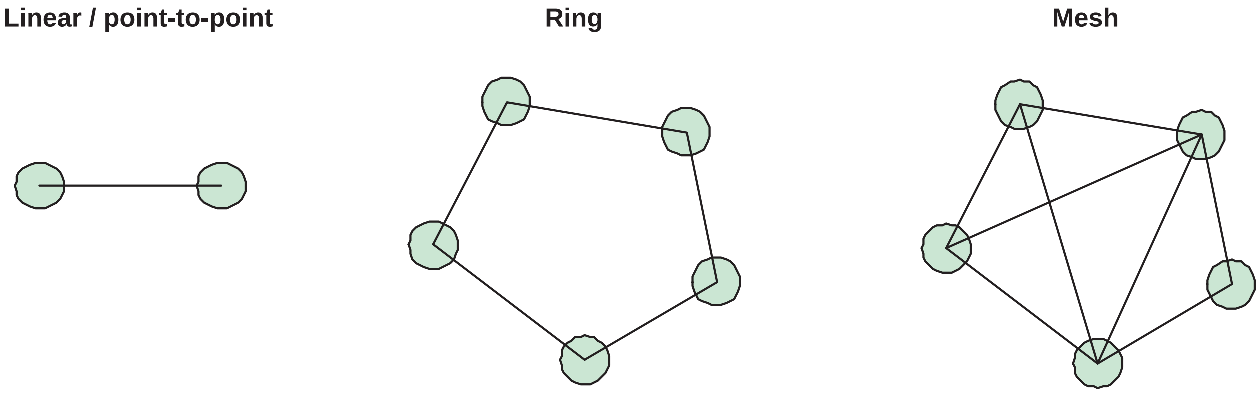

Figure 2: Linear/point-to-point, ring and mesh topology.

- Signaling: specifies the communication between control entities used to establish and maintain connections.
- Local resource management: takes care of bookkeeping and advertising of locally available resources.

All of these control plane functionalities must be operational to automatically provision and recover a connection.

It is advantageous to separate the control plane from the data plane to prevent that failures in one plane will not affect the other. The control plane and the data plane can be separated logically or physically (i.e., using separate networks).

4.2 Control Plane Standardization

To ensure that multi-vendor networks can operate together, the control plane must be standardized. Different organizations contribute to control plane standardization:

- The ITU, which develops a framework for ASON.
- The IETF, which develops a framework for GMPLS.
- The OIF, which develops implementation agreements such as the UNI and the NNI.

Several studies, such as [12, 19–21], focus on the difference between these control approaches, but it should be noted that they complement each other [22], since ASON can reference the protocol specifications of the GMPLS protocol suite [21]. The three standardization approaches are described in the following sections.

4.3 ASON

ASON [14] is developed by the ITU and is therefore inspired by concepts used in telecommunication transport networks, with well defined interfaces between clients and servers [12]. The goal of ASON is to improve the complex process of provisioning end-to-end transport services [20] by creating a complete definition of the dataplane, operation and management for automatically switched transport networks [21]. ASON specifies a separate DCN [23], which is used as the control communication infrastructure between optical network elements. It also specifies an architecture and requirements for routing [24], a DCM [25] using specific protocol mechanisms, and neighbor discovery [26]. ASON is not a protocol or a protocol suite, but a reference architecture that defines the control plane components and how they interact with each other. ASON is protocol neutral but requires standardized protocols because it defines communication across multi-vendor networks, and any protocol that satisfies its functionality requirements can be included into ASON.

4.4 GMPLS

GMPLS [13] is developed by the IETF and uses an IP-based control plane. GMPLS is an extension of the MPLS concept, which was developed to apply traffic engineering to IP networks [19]. In GMPLS, the label is generalized to signify a timeslot, a wavelength or a fiber. GMPLS defines a set of protocols and a framework covering how these protocols should be applied together. The most used protocols within the protocol suite are:

- OSPF with TE extensions [27]: used for routing (i.e., resource information dissemination, path computation).

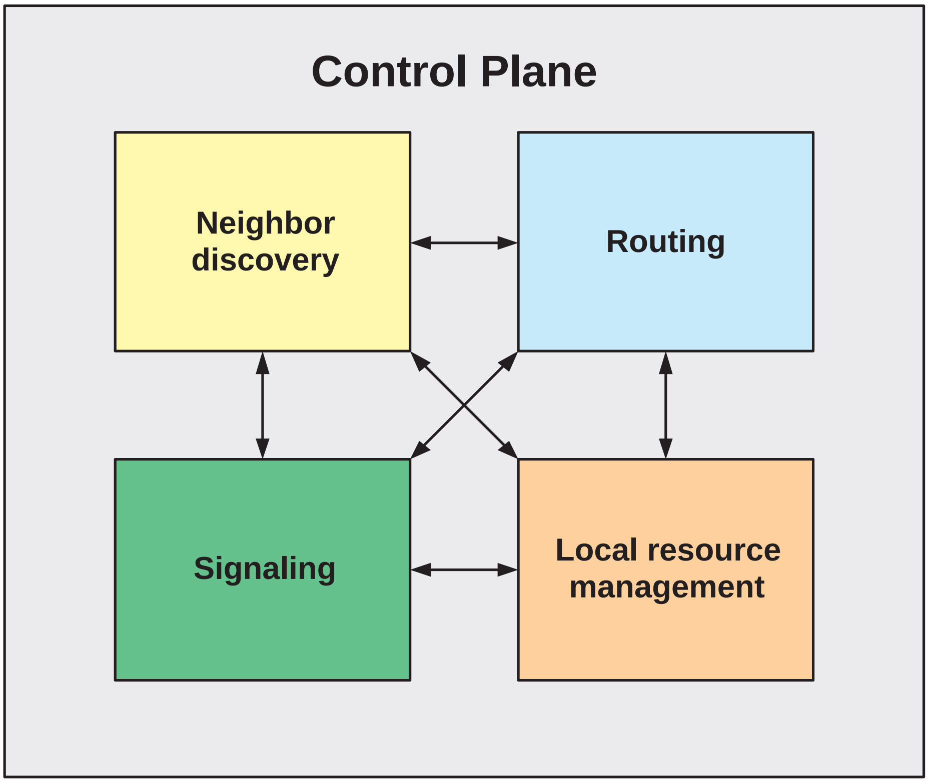

Figure 3: Control plane functions.

- RSVP with TE extensions [28]: used for signaling (i.e., connection provisioning and maintenance, label assignment).

- LMP [29]: used for link management (i.e., neighbor discovery, fault localization).

4.5 UNI and NNI

The OIF specifies the UNI [15] and NNI [16] based on needs of service providers and equipment vendors. They have the following characteristics [12]:

- UNI: defines the interface between the client and the network, and is used by the client to request a service from the network.

- NNI: defines the interface between different network domains. The NNI is further split into an E-NNI and an I-NNI depending on whether the NNI is located between or within administrative domains, respectively.

The OIF also aims a bringing the concepts of ASON and GMPLS together and mediates between the respective standardization bodies [12, 30].

5 Recovery methods

For mesh networks, there are two well-known recovery methods, span protection and path protection [1], whose efficiency has been evaluated in a plethora of studies, e.g. [31] [32]. A newer method, called local-to-egress [33], where the traffic is re-routed on a per-connection basis between the upstream failure adjacent node and the destination node, has a good performance trade-off in terms of notification time and capacity efficiency [34]. Its operation is illustrated in figure 4.

However, there also exists a tradeoff between capacity efficiency and the complexity of fully individual connection re-routing in the local-to-egress protection method. Furthermore, with the prices for fiber (i.e., capacity) decreasing [35], complexity, manageability and speed become more important decision factors than capacity usage for protection method selection.

With the aim of reducing the complexity of the protection method without sacrificing restorability, a variation of the local-to-egress protection method called Shortcut Span Protection (SSP) [6] has been developed. In SSP, the traffic is bundled between the failure adjacent node and the egress node if several affected connections have the same destination node.

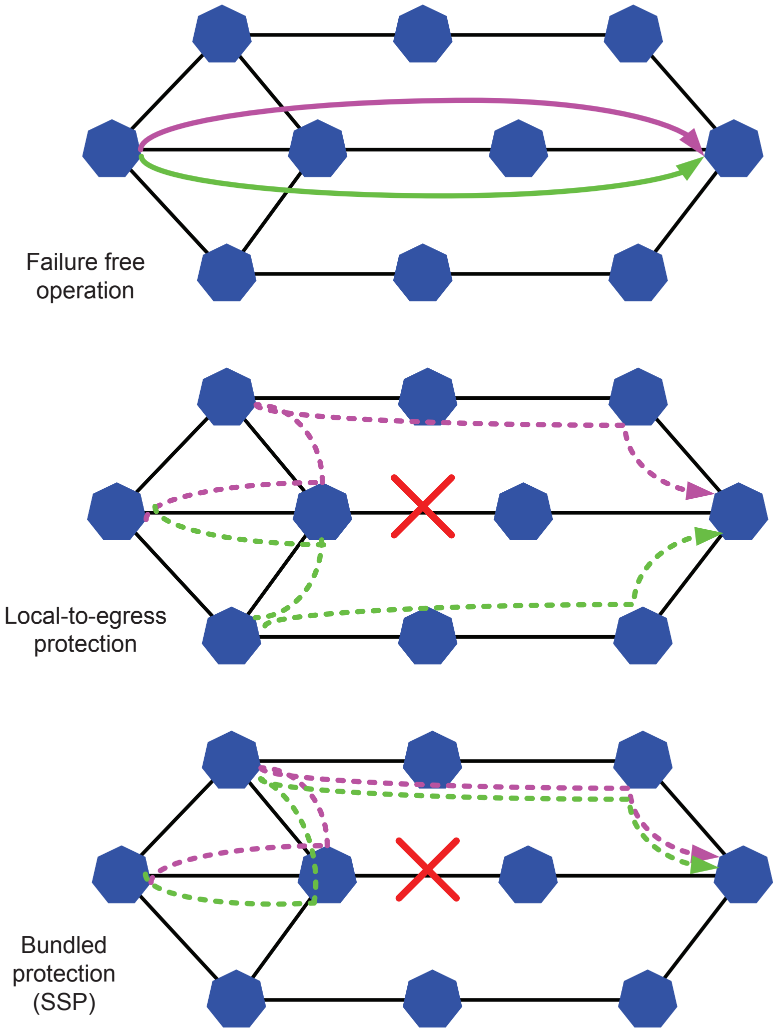

Figure 4: Shortcut Span Protection.

The method is illustrated in Figure 4. The advantage of the proposed method lies in a less complex route calculation and signaling process, since all connections going to the same destination node must follow the same route from the upstream failure adjacent node, which significantly eases the control plane load.

6 Shortcut Span Protection

In this section we will describe the Mixed Integer Programming model of the short-cut span-protection model. We model the network with a graph of $G(V, L)$, where $i, j, q, r, k, l \in V$ is the nodes, i.e. switches, of the network and links between the nodes i and j, $\{ij\} \in L$, i.e. fibre connections, of the network. The communication is however directed and each link $\{ij\}$ can accomodate communication in both directions, i.e. the arcs (ij) and (ji) are both using link $\{ij\}$. We assume that the needed capacity is additive, i.e. the total needed capacity of link $\{ij\}$ is the sum of the directed flow (ij) and (ji).

Furthermore there is a demand matrix $D^{(kl)} \geq 0$ which quantifies the volume of the communication demand from node k to node l. We model the problem with a set of paths for each oriented pair of nodes k and l: $p \in P^{(kl)}$ from node k to node l. The set of paths is both used to satisfy the communication demand in the non-failure scenario and for re-routing the communication demand when a fibre (link) has failed. The non-failure traffic is represented by the variables $x_p^{(kl)} \in R^+$, where k is the origin node and l is the terminating node of demand $D^{(kl)}$. Each arc used of the path is recorded in an incidence matrix $A_{p,(ij)}^{(kl)}$, which takes the value 1 if path p from node k to node l uses arc (ij). Furthermore we use the variables $y_p^{(qr),l}$ to represent the re-routed traffic from the origin node q of the failed arc (qr) to the destination node l. The planning objective is to minimize the required network capacity, taking into account that in case one cable breaks, communication is restored. The model is given below in the Equations (1)-(5).

In the modeldefined above with the Equations (1)-(5), the objective function in Equation (1) calculates the cost of the necessary network capacity, which should be minimized. Equation (2) ensures that the non-failure communication demand is satisfied. Equation (3) ensures that if any of the arcs of a non-failure traffic paths fails, enough backup path capacity is installed to recover the failure. Equation (4) calculates the maximal necessary link capacity $z_{\{ij\}}$ in case of any (other) link failure $\{qr\}$. Notice that in Equation (4) the necessary capacity for each bi-directional link $\{ij\}$ is the traffic in both directions (ij) plus (ji). Furthermore, if a link $\{qr\}$ fails, both arcs of the link (qr) and (rq) fails.

The model defined above with the Equations (1)-(5) assumes knowledge of all paths, both for routing and for protection. Alternatively the problem could have been formulated as a flow model, but the above model enables solution using column generation. To simplify the problem and to enable faster solution, we perform shortest path routing of the non-failure traffic, i.e. we choose the shortest path and fix the variable $x_{shortest}^{(kl)} = 1$. For the protection paths $y_p^{(qr),l}$ we start with a subset of the paths $p \in P'^{(kl)} \subseteq P$. Given a solution of the restricted master problem, we can calculate improving paths for all $(qr), l$ sub-problems. Given the dual variables $\alpha^{(qr),l} \geq 0$ from Equation (3) and $\beta^{\{ij\},\{qr\}} \leq 0$ from Equation (4), we can calculate the optimal reduced cost as shown below Equation (6).

$$c^{(qr),l} = -\alpha^{(qr),l} - \sum_{(qr)|A_{p,(qr)}^{(kl)}=1} \beta^{\{ij\},\{qr\}} \quad \forall\,(qr),l \qquad (6)$$

Using column generation we can now find solution to the model defined by the Equations (1)-(5).

The model defined above with the Equations (1)-(5) assumes that traffic can be bifurcated in any way. This may not be a critical problem for the non-failure traffic, but handling lots of different paths is a problem when having to execute backup actions fast in the switches in the network. To achieve this, we introduce a new binary variable $v_p^{(rq),l} \in \{0,1\}$ for each path, for each protection path. We will require that at most *one* of the protection paths are used. This is achieved by introducing two new constraints, which links the backup path variables $y_p^{(rq),l}$ with the new binary variables $v_p^{(rq),l}$.

$$\begin{aligned} y_p^{(rq),l} &\leq M \cdot v_p^{(rq),l} \quad \forall p,(kl),l \quad \alpha^{(kl)} && (7) \\ \sum_p v_p^{(rq),l} &\leq 1 \quad \forall (kl), \quad \alpha^{(kl)} && (8) \end{aligned}$$

The introduction of binary variables means that column generation cannot be utilized. Instead we opt for the following practical approach: First the basic Linear Programming model defined by Equations (1)-(5) is solved using column generation. Then the new variables $v_p^{(rq),l}$ are added, one for each corresponding (generated) variable $y_p^{(rq),l}$ and the linking constraints are added. Then the corresponding Mixed Integer Programming is then solved using a standard MIP solver.

7 Simulation Study

The capacity efficiency of the SSP method depends on the route selection of primary paths and the backup paths. Hence, to evaluate the efficiency of SSP, the following optimization problem must be solved: Route the primary and backup paths using as little network capacity as possible. To do this, a LP is used to model the capacity usage and route the primary paths and backup paths optimally. The LP model is based on a graph representing the network such that the graph nodes correspond to network switches and the graph edges corresponds to the network spans. The objective is to find the total required capacity for the network. The following constraints are setup:

- **Demand constraint**: requires that for each demand enough capacity is assigned to the primary path.
- **Backup constraint**: ensures that if a span fails and a number of primary paths which use that span and which end at a given node, enough capacity is assigned on the path to that node.
- **Capacity constraint**: calculates the necessary capacity on each span for all failure situations.

In order to evaluate the effectiveness of SSP it is tested by optimizing over a set of 5 networks for a demand volume of 1 between all pairs of nodes in the network. In Table 1 the network properties are summarized. The contents of each column in the table is given as:

- **Network:** Network name
- **Nodes:** Number of nodes in the network
- **Spans:** Number of spans in the network

$$\min \qquad \sum_{\{ij\}} c_{\{ij\}} \cdot z_{\{ij\}} \tag{1}$$

subject to:

$$\sum_{p} x_p^{(kl)} \geq D^{(kl)} \quad \forall\,(kl) \tag{2}$$

$$\sum_{p} y_p^{(qr),l} - \sum_{k} \sum_{p} A_{p,(qr)}^{(kl)} \cdot x_p^{(kl)} \geq 0 \quad \forall\,(qr), l \tag{3}$$

$$\begin{aligned} &\sum_{(kl)} \sum_{p} [A_{p,(ij)}^{(kl)} + A_{p,(ji)}^{(kl)}] x_p^{(kl)} \\ &+ \sum_{l} \sum_{p} [A_{p,(ij)}^{(qr)} + A_{p,(ji)}^{(qr)}] y_p^{(qr),l} + \sum_{l} \sum_{p} [A_{p,(ij)}^{(rq)} + A_{p,(ji)}^{(rq)}] y_p^{(rq),l} \leq z_{\{ij\}} \quad \forall\,\{ij\}, \{qr\} \end{aligned} \tag{4}$$

$$x_p^{(kl)}, y_p^{(qr),l} \in [0,1] \quad , \quad z_{\{ij\}} \in R^+ \tag{5}$$

Network	Nodes	Spans	Average Nodal Degree	Non-Failed Capacity
Cost239 [36]	11	26	4.73	86
PanEuropean	13	21	3.23	158
USANetwork [37]	28	45	3.21	1273
Italy [38]	33	68	4.12	1718
France [37]	43	71	3.30	3473

Table 1: Network properties of test networks.

- **Average Nodal Degree:** Average nodal degree (i.e. density of the network) in the network
- **Non-Failure Capacity:** Non-Failure network capacity, i.e., the summed capacity necessary for non-failure routing (i.e. when all spans are operational).

The following protection methods are evaluated and compared in terms of protection overbuild:

- **Complete rerouting (CR)**: allows the re-routing of non-failed connections as well [39]. Not practical for real networks, used for benchmarking only.
- **Path protection (PP)**: connections are recovered on an end-to-end basis.
- **Local-to-egress protection (LtE)**: recovery between the upstream failure adjacent node and the destination node.
- **Shortcut span protection (SSP)**: as local-to-egress, but all protection paths for a given destination must follow the same route [6].
- **Span protection (SP)**: the failure is restored between the failure adjacent nodes.

8 Results

This section presents the capacity usage of SSP in comparison to CR, PP, LtE and SP. In figure 5, the capacity usage is depicted as relative protection overbuild, defined as: necessary extra network capacity relative to the non-failure network capacity.

The results show the following ordering of protection capacity, starting from the lowest usage: Complete re-routing → path protection → local-to-egress protection → span protection → SSP. This tendency shows that more freedom in terms of route choice results in a better capacity efficiency. SSP uses most resources. For local-to-egress protection the requirement of bundling results in a higher capacity usage as can be seen in SSP.

The pattern in the different networks follow each other; networks with many nodes the capacity usage increase of SSP is larger than in other network instances. This is likely due to the topological characteristics of the networks.

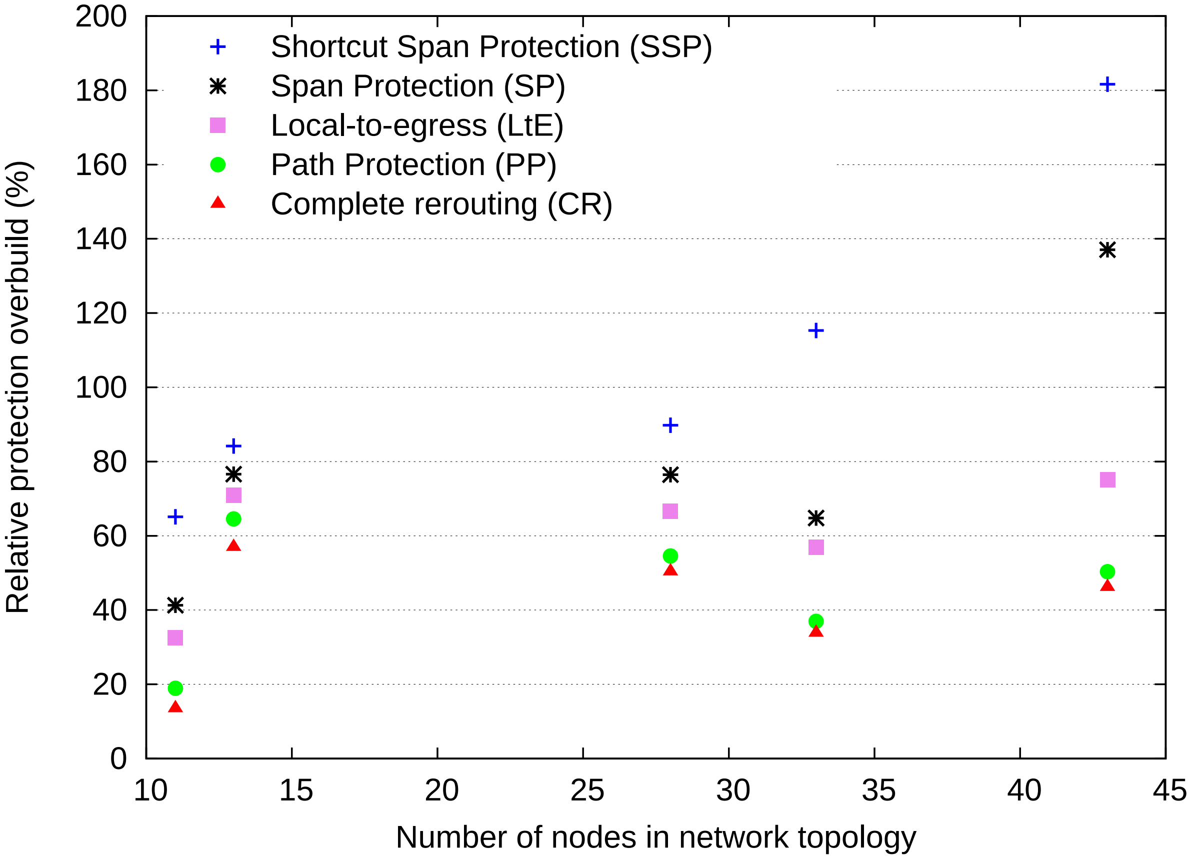

Figure 5: Relative protection overbuild.

9 Conclusion

In this study, the capacity usage of SSP has been evaluated. In comparison to local-to egress protection, which is the closest related protection method in terms of involved nodes, the capacity usage of SSP is higher. The increase in capacity can however be compensated by an easier control since all recovery requests are bundled to the same route to a particular destination. This bundling simplifies route computation and signalling and hence also eases the load on the control plane.

References:

[1] J.-P. Vasseur, M. Pickavet, and P. Demeester, *Network Recovery, Protection and Restoration of Optical, SONET-SDH, IP, and MPLS*. Morgan-Kaufmann Publishers, Elsevier, 2004, ISBN: 0-12-715051-x.

[2] W. Grover, *Mesh-Based Survivable Networks - Options and Strategies for Optical, MPLS, SONET, and ATM Networking*. Prentice-Hall, 2004, ISBN: 0-13-494576-X.

[3] K. Kim and B. Yae, “Protection switching scheme for ng-sdh based switching system,” *WSEAS TRANSACTIONS on SYSTEMS*, 2006.

[4] S. Ruepp, J. Buron, N. Andriolli, and L. Dittmann, “Nodal stub release in all-optical networks,” *IEEE Commun. Lett.*, vol. 12, no. 1, pp. 47–49, Jan. 2008.

[5] S. Ruepp, J. Buron, and N. Andriolli, “Wavelength-converter saving span restoration in GMPLS controlled WDM optical networks,” in *Proc. Conference of Optical Internet, COIN*, July 2006.

[6] T. Stidsen and S. Ruepp, “Shortcut span protection,” in *Extended Abstract for Informs Telecom*, 2006.

[7] S. Ruepp, L. Dittmann, M.Berger, and T. Stidsen, “Recovery request bundling,” in *Proc. CISST Conference at Harvard University*, 2010.

[8] I. Atov and R. J. Harris, “Lp-based algorithm for optimization in multiservice ip networks,” *WSEAS Transactions on Communications*, 2003.

[9] Y. Donso, C. Alvaro, A. Perez, and I. Herazo, “An approach to the optimizastion fo convergent networks on ip/mpls with an optical gmpls backbone in multicast,” *WSEAS Transactions on Communications*, 2006.

[10] F. Palmieri and U. Fiore, “An evolutionary genetic-based approach for traffic engineering in gmpls networks,” *WSEAS Transactions on Communications*, 2005.

[11] International Telecommunication Union (ITU-T), “Recommendation I.321: B-ISDN protocol reference model and its application.”

[12] G. Bernstein, B. Rajagopalan, and D. Saha, *Optical Network Control - Architecture, Protocols and Standards*. Boston, USA: Pearson Education Inc., 2004, ISBN: 0-20-175301-4.

[13] E. Mannie (ed.), “Generalized multi-protocol label switching (GMPLS) architecture,” *RFC 3945*, Oct. 2004.

[14] International Telecommunication Union (ITU-T), “Recommendation G.8080: Architecture for the automatically switched optical network (ASON).”

[15] OIF, “User network interface (UNI) 1.0 signaling specification, release 2,” Feb. 2004.

[16] ——, “Intra-carrier E-NNI signaling specification,” Feb. 2004.

[17] P. Blair and J. B. (Ovisor Technologies), “ROADMs - the traffic cops of agile optical networks,” Europhotonics, European converage of optics, lasers, imagine, fibre optics, electro-opticas and photonic component manufacturing - Laurin Publications, Feb./Mar. 2007.

[18] B. Mukherjee, *Optical WDM Networks*. Springer, 2006, ISBN: 0-387-29055-9.

[19] A. Farrel and I. Bryskin, *GMPLS Achitecture and Applications*. Morgan Kaufmann, Elsevier, 2006, ISBN: 0-12-088422-4.

[20] S. Tomic, B. Statovci-Halimi, A. Halimi, W. Müllner, and J. Frühwirth, “ASON and GMPLS - overview and comparison,” *Photonic Network Communications*, vol. 7, no. 2, pp. 111–130, 2004.

[21] N. Larkin, “ASON and GMPLS - the battle of the optical control plane: An overview of ongoing work of the IETF and ITU to standardize optical control plane protocols,” Data Connection Whitepaper, Aug. 2002. [Online]. Available: http://www.dataconnection.com/network/download/whitepapers/asongmpls.pdf

[22] D. Papadimitriou, J. Drake, J. Ash, A. Farrel and L. Ong (eds.), “Requirements for generalized MPLS (GMPLS) signaling usage and extensions for automatically switched optical network (ASON),” *RFC 4139*, July 2005.

[23] International Telecommunication Union (ITU-T), “Recommendation G.7712: Architecture and specification for the data communications network (DCN).”

[24] ——, “Recommendation G.7715: Architecture and requirements for routing.”

[25] ——, “Recommendation G.7713: Distributed connection management (DCM).”

[26] ——, “Recommendation G.7714: Neighbor discovery.”

[27] K. Kompella and Y. Rekhter (eds.), “OSPF extensions in support of generalized multi-protocol label switching (GMPLS),” *RFC4203*, Oct. 2005.

[28] D. Katz, K. Kompella and D. Yeung (eds.), “Traffic engineering (TE) extensions to OSPF version 2,” *RFC 3630*, Sept. 2003.

[29] J. Lang (ed.), “Link management protocol (LMP),” *RFC4204*, Oct. 2005.

[30] Optical Internet Forum, “Intra-carrier E-NNI signaling specification,” *OIF-E-NNI-Sig-01.0*, Feb. 2004.

[31] J. Wang, L. Sahasrabuddhe, and B. Mukherjee, “Path vs. subpath vs. link restoration for fault management in IP-over-WDM networks: Performance comparisons using GMPLS control signaling,” *IEEE Commun. Mag.*, vol. 40, no. 11, pp. 80–87, Nov. 2002.

[32] S. Ruepp, N. Andriolli, J. Buron, L. Dittmann, and L. Ellegard, “Restoration in all-optical GMPLS networks with limited wavelength conversion,” *Computer Networks Special Issue on Opportunities and Challenges in Optical Networks*, 2008.

[33] A. Authenrieth and A. Kirstdter, “Engineering end-to-end IP resilience using resilience-differentiated QoS,” *IEEE Commun. Mag.*, pp. 50–57, January 2002.

[34] C. Gruber, “A comparison of bandwidth requirements of path protection mechanisms,” *ICN 2005, LNCS Springer*, vol. 3420, pp. 133–143, 2005.

[35] “Optical fiber supply meets expanding application,” *SK Opto-Electronics Newsletter*, vol. 12, pp. 50–57, February 2003.

[36] P. Batchelor, B. Daino, P. Heinzmann, D. R. Hjelme, P. Leuthold, R. Inkret, G. D. Marchis, H. A.Jager, F. Matera, M. Joindot, B. Mikac, A. Kuchar, H.-P. Nolting, E. Coquil, J. Späth, F. Tillerot, B. Caenegem, N. Wauters, and C. Weinert, “Study on the implementation of optical transparent transport networks in the european environment-results of the research project COST 239,” *Photonic Network Communications*, vol. 2, no. 1, pp. 15–32, May 2000.

[37] J. Doucette, D. He, W. Grover, and O. Yang, “Algorithmic approaches for efficient enumeration of candidate p-cycles and capacitated p-cycle network design,” in *Proc. Workshop on Design of Reliable Communication Networks (DRCN)*, 2003, pp. 212–220.

[38] W. Grover, J. Doucette, M. Clouqueur, D. Leung, and D. Stamatelakis, “New options and insights for survivable transport networks,” *IEEE Commun. Mag.*, vol. 40, no. 1, pp. 15–32, 2002.

[39] T. Stidsen and P. Kjaerulff, “Complete rerouting protection,” *Journal of Optical Networking*, vol. 5, no. 6, pp. 481–492, 2006.