University of Würzburg
Institute of Computer Science
Research Report Series

Efficiency of Routing and Resilience Mechanisms in Packet-Switched Networks

Michael Menth, Rüdiger Martin, Matthias Hartmann, and Ulrich Spörlein

Report No. 425 May 2007

University of Würzburg
Institute of Computer Science
Department of Distributed Systems
Am Hubland, 97074 Würzburg, Germany

Efficiency of Routing and Resilience Mechanisms in Packet-Switched Networks

Michael Menth, Rüdiger Martin, Matthias
Hartmann, and Ulrich Spörlein
University of Würzburg
Institute of Computer Science
Department of Distributed Systems
Am Hubland, 97074 Würzburg, Germany

Abstract

This paper compares the efficiency of different routing and resilience mechanisms to avoid congestion in a network for a set of protected failures. A routing mechanism is more efficient than another one if it achieves a lower maximum link utilization in the same networking scenario. With resilience requirements, the maximum link utilization over the set of protected failure scenarios becomes the critical value. We consider standard and optimized configurations of single shortest path (SSP) and equal-cost multipath (ECMP) routing as well as several types of end-to-end (e2e) path protection and MPLS fast reroute (FRR). We investigate how well these resilience mechanisms can cope with different network structures and with different sets of protected failures. The results show that routing optimization reduces the maximum link utilization significantly both with and without protection of failures. The optimization potential for resilient routing is limited by the applied mechanism and heavily depends on the network structure and the set of protected failure scenarios.

1 Introduction

Network failures occur so frequently and can take so long that they are not tolerable for customers of Internet service providers (ISPs). Therefore, service availability is a critical issue in service level agreements (SLAs). Network providers use protection switching and restoration mechanisms to guarantee service continuation if a failure occurs. Various methods are suitable for different objectives.

- End-to-end (e2e) protection switching mechanisms protect primary paths by disjoint backup paths such that the connectivity is restored if a failure occurs on the primary paths. Protection switching implies that the backup paths are set up in advance such that the head end router just needs to switch the traffic over if it is informed about the failure of the primary path.
- Restoration mechanisms establish backup paths after a failure has occurred. Therefore, they are too slow to protect traffic of real-time applications [1]. However, they can survive multiple network failures. For example, IP routing carries the traffic always on least cost

This work was funded by Siemens AG, Munich, and the German Research Foundation (DFG). The authors alone are responsible for the content of the paper.

paths and restores the connectivity as long as the network is physically connected. In contrast, e2e protection switching mechanisms cannot restore the connectivity if the primary and the backup path of a connection fail simultaneously.

- Fast reroute (FRR) is a special type of protection switching. E2E protection switching uses link management protocols [2] to recognize path failures which takes time. FRR mechanisms recognize a failure at its location and redirect the traffic from there to minimize the reaction time. Multiprotocol label switching (MPLS) offers two options for FRR [3] and, currently, FRR mechanisms are also intensively discussed for IP routing [4].

This is just a small but relevant subset of existing resilience mechanisms with their pros and cons. In this work, we study a simple primary/backup path concept and the self-protecting multipath (SPM) as representatives for e2e protection switching, standard and optimized single shortest path (SSP) and equal-cost multipath (ECMP) routing as representatives for restoration mechanisms, and the standard and improved one-to-one and facility backup options of MPLS as representatives for FRR.

In IP backbones, overload occurs mostly due to redirected traffic in case of network failures [5]. Routing and resilience mechanisms should carry traffic over paths with sufficient capacity in such a way that the resulting link utilization is low in the failure-free and in all protected failure scenarios. Our intention is to investigate how well the above mechanisms achieve that goal.

The contribution of this paper is a comprehensive study regarding the efficiency of standard and improved routing and resilience mechanisms. We consider the impact of the network topology and the resilience requirements, i.e., we compare the efficiency for unprotected networks as well as for networks with protection of single link failures, single router failures, and single link and router failures.

Section 2 explains the resilience mechanisms under study in more detail and explains how their configurations can be improved. Section 3 compares the efficiency of routing and resilience mechanisms in different network topologies and with different resilience requirements. Finally, we summarize this work and draw our conclusions in Section 4.

2 Optimization of Resilience Mechanisms

In this section, we present the resilience mechanisms that we consider in our investigation and show how they can be optimized to carry more protected traffic.

2.1 Resilience Mechanisms

As mentioned in Section 1, this work focuses on IP rerouting, end-to-end protection switching, and MPLS fast reroute. We explain them now in more detail.

2.1.1 IP Rerouting

IP routers forward data packets using destination-based routing. They have routing tables that map address prefixes to outgoing interfaces. A router finds the longest one of the prefixes that match a packet's destination IP address and forwards it to the corresponding interface (next hop).

The prefixes can be associated with more than one interface. Single path routing forwards the traffic only to the next hop with the lowest device ID while multi-path routing splits the traffic equally among all possible next hops [6, Section 7.2.7].

The routing tables are usually constructed in a distributed manner by routing protocols like OSPF or IS-IS. They use administrative link costs to calculate the next hops based on least-cost paths. Single shortest path (SSP) routing is default, but we also consider the equal-cost multipath (ECMP) option, which allows multipath routing over all least-cost paths. More precisely, the traffic is equally distributed over all interfaces that are on a shortest paths to its destination. ECMP makes the routing independent of device IDs and spreads the traffic over more links which often leads to more balanced link utilizations.

A salient feature of IP rerouting is its robustness against network failures. The routing protocols adapt the routing tables to the working topology within seconds and restore the connectivity of the network as long as it is physically connected. This rerouting may take seconds, but currently new mechanisms for IP fast rerouting are investigated [4, 7].

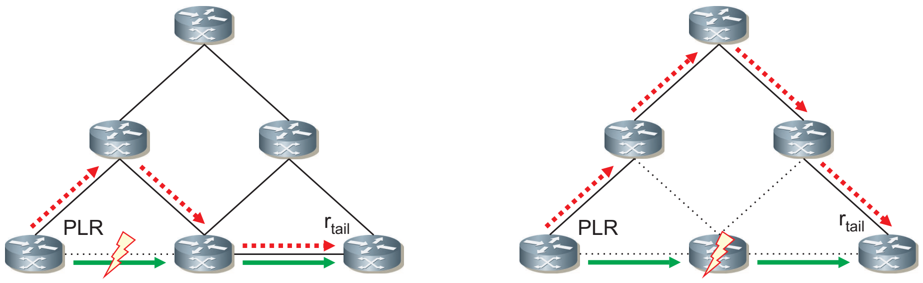
2.1.2 End-to-End Protection Switching

The simplest form of e2e protection switching is the primary/backup path concept. Both a primary and a backup path are established during the connection setup. They are either link or also node disjoint to protect against single link or single node failures. In case of a path element failure, this is recognized by the node immediately upstream to this failure and a path error message is sent to the head end router to switch the traffic from the primary to the backup path. Alternatively, the receipt of an updated link state advertisement or packet (LSA, LSP) from the interior gateway protocol (IGP).

2.1.3 MPLS Fast Reroute

MPLS fast reroute (MPLS-FRR) is a protection switching mechanism implementing the local repair principle [3]. It provides a point of local repair (PLR) at any router within a label switched path (LSP) such that the traffic can be rerouted at any possible failure location. The advantage of this method is that PLRs can recognize the failure faster than the head end router of the path and, therefore, the reaction time of MPLS-FRR is shorter than the one of e2e protection mechanisms. MPLS-FRR offers two backup options that are presented in the following.

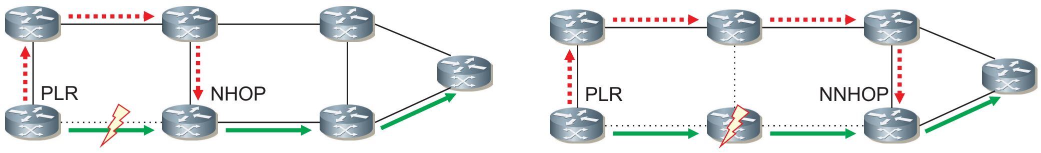
One-to-One Backup One-to-one backup provides for any path at any PLR a separate backup path that redirects the traffic towards its destination r_{tail}. Figures 1(a)–1(b) illustrate the standard path layout of these backup paths. They follow the shortest paths from the PLR to the respective destination r_{tail} and avoid the potentially failed elements, i.e. the link and the node after the PLR, because these network elements must not be contained in the backup paths. These backup paths are called detours. To reduce the complexity of the state maintenance, detour LSPs towards the same destination may be merged to a single LSP when they meet on the way to the destination. However, this does not impact the path layout.



(a) $LinkDetour(PLR, r_{tail})$. (b) $RouterDetour(PLR, r_{tail})$.

Figure 1: One-to-one backup uses detour tunnels.

Facility Backup Facility backup provides protection switching for every network element. The standard path layout uses shortest paths without the failed network elements to set up so-called link and router bypasses. Figure 2(a) illustrates a link bypass. A link failure is protected by a backup path around this link, i.e., the backup path starts at the PLR and ends at the next hop (NHOP). This backup path deviates all flows when this link fails and acts like a tunnel. Similarly, a router failure is protected by a backup path from the PLR to the next next hop (NNHOP) of the respective path (cf. Figure 2(b)). Note that several backup paths are required to protect a single router failure since traffic comes from and leaves for different interfaces of the protected router.



(a) $LinkBypass(PLR, NHOP)$. (b) $RouterBypass(PLR, NNHOP)$.

Figure 2: Facility backup uses bypass tunnels.

2.2 Routing Optimization

Routing mechanisms can be configured in such a way that the utilization of the links in the networks is minimized which improves the QoS of the traffic and leaves room to compensate traffic fluctuations [8–11]. In networks with resilience requirements routing optimization becomes more difficult. The resilience mechanisms mentioned above just maintain the mere connectivity in case of a failure. Redirected traffic can cause congestion on the backup links and affect the QoS of both primary and backup traffic.

Let s denote a single failure scenario which describes the failed network elements, i.e., the empty set $\emptyset$ is the failure-free scenario. The routing should be configured in such a way that the maximum utilization $\rho_{\mathcal{S}}$ of all links in the network is minimized during failure-free operation and in all intentionally protected failure scenarios $\mathcal{S}$. We call this optimization a configuration approach as the optimized routing is used to configure networks with given link bandwidths [12].

In contrast, we call the joint optimization of the routing and the link bandwidths a capacity dimensioning approach [13, 14]. The objective is to design a cost-effective network that needs the least resources, i.e. working and backup capacity, to carry a given traffic matrix in all protected failure scenarios. Optimization for capacity dimensioning is more difficult than for configuration since more parameters must be set. However, in this work, we consider only the above mentioned routing optimization for network configuration.

2.2.1 Optimization of IP Routing

The standard configuration of IP routing uses the hop count metric, i.e., the cost for any link is set to 1. However, the link costs can be adjusted by heuristic algorithms in such a way that the maximum link utilization $\rho_{\mathcal{S}}$ of the network for any protected failure scenario $s \in \mathcal{S}$ is minimized [15–18]. In this paper, we use the method from [19] for the optimization of IP link costs both for SSP and ECMP routing and refer to these options by optSSP and optECMP.

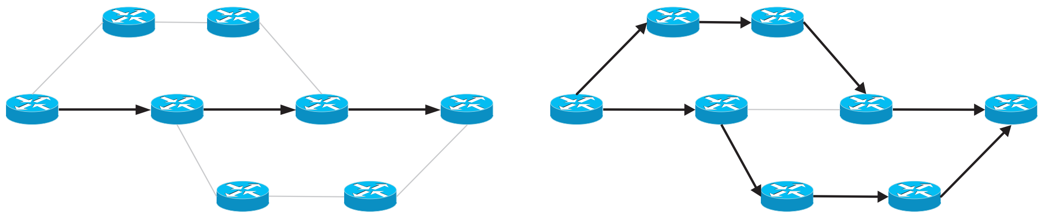
2.2.2 Optimization of Explicit E2E Paths

We first present non-confluent shortest paths (NCSPs) as a very simple heuristic for the path layout of unoptimized explicit paths. Then, we introduce the self-protecting multipath (SPM) as a general e2e protection switching mechanism and derive optimized explicit paths and primary/backup paths from that structure.

Unoptimized Non-Confluent Shortest Paths (NCSPs) With SSP routing in IP networks, the traffic follows the shortest paths and, in addition, the flows towards the same destination take the same shortest paths when they meet at any point in the network. This leads to a strong traffic concentration on some links which we call a Lemming effect. With MPLS, explicit routes can be established that do not need to have this Lemming effect. We obtain such paths using the following algorithm and call them non-confluent shortest paths (NCSPs). A counter tracks the number of flows over a link during the path layout process, and the links with a low counter value are preferentially taken when new shortest paths are requested and several equal cost paths exist.

NCSPs may be used to implement the e2e primary/backup concept (NCSP-PB). To obtain a pair of disjoint shortest paths, we use a combination of the 2-disjoint-shortest-paths (2-DSP) computation from [20] and our NCSP approach. We use the shorter path as primary and the longer one as backup path. The DSP computation is required because for some “trap topologies” the shortest path prohibits a disjoint backup paths (cf. Figure 3(a)) although disjoint paths exist in the network (cf. Figure 3(b)).

Self-Protecting Multipath (SPM) The self-protecting multipath (SPM) is an e2e protection switching mechanism and can be considered as a generalization of the primary/backup path concept. Its path layout is obtained by a combination of the NCSP and k-DSP computation, i.e., the maximum link utilization over the set of protected failure scenarios up to k disjoint path are considered which yields a k-SPM. The path layout of a 3-SPM is depicted in Figure 4. The traffic



(a) Single shortest path routing prohibits the existence of a disjoint backup path.

(b) The disjoint-shortest-path computation finds disjoint paths.

Figure 3: Path layouts in the trap topology.

is distributed over the disjoint paths according to a load balancing function that depends on the pattern of working and broken paths. To protect against single failures, the 3-SPM requires 4 different traffic distribution functions: one for the failure-free scenario and one for the failure of each of its three paths. The optimization of the load balancing function takes into account the set of protected failure scenarios $\mathcal{S}$. It is numerically well tractable for networks with a size of up to 60 nodes and can improve the protected throughput to a large extent [21]. However, load balancing can be problematic due to distribution inaccuracies [22, 23]. Without losing the savings potential of the SPM, heuristics can optimize the load balancing functions of the SPM in such a way that its paths carry either 0% or 100% of the traffic, i.e., the load balancing function acts like a path selection function. These heuristics are very fast and can optimize the SPMs of large networks of up to 200 nodes within several minutes. We call this method integer SPM (iSPM) [12] and use it as default for the SPM throughout this paper.

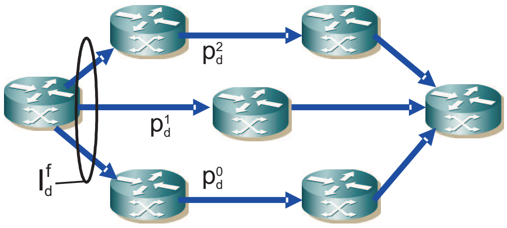


Figure 4: The k-SPM distributes the traffic of a demand d over up to k disjoint paths paths p_d^0, ..., p_d^{k-1} according to a traffic distribution function l_d^f which depends on the pattern f of working and non-working paths.

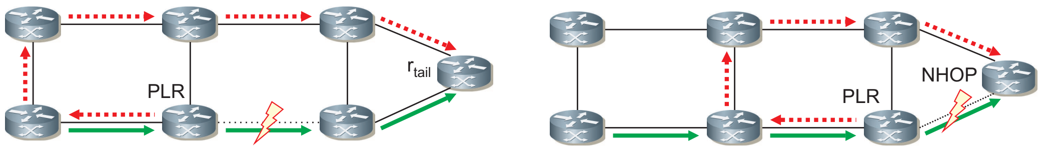
Optimized Explicit Paths (optE2E) The straightforward optimization of the explicit paths uses an integer linear program (ILP) to find the best path layout (optE2E-ILP). ILPs are difficult to solve as they are time and memory consuming for medium and large size networks and, therefore, we do not use this method. We rather use the k-iSPM optimized only for the failure-free scenario $\mathcal{S} = \{\emptyset\}$. That means, the optimization chooses for any ingress-egress pair one path out of k disjoint paths in such a way that the resulting set of e2e paths leads to a low maximum link utilization $\rho_\emptyset$ in the failure-free scenario. We investigate this method with and without the restriction of $k \leq 2$ and call the respective paths 2-optE2E and k-optE2E.

Optimized Primary/Backup Paths (optPB) The most obvious optimization of the primary/backup paths concept selects the path layout of the primary and the backup path in such a way that the maximum link utilization $\rho_{\mathcal{S}}$ is minimized over $\mathcal{S}$. This is a quadratic integer problem and, therefore, it is rather difficult to solve and very time-consuming already for small networks. Instead, we use the 2-iSPM to approximate an optimum primary/backup path system. The path of the 2-iSPM which is used during the failure-free operation is the primary path and the other one is the backup path. Note that the general k-iSPM (k>2) has more flexibility than the primary/backup path concept because it uses different backup paths depending on the failure symptom.

2.2.3 Improved Configurations of MPLS Fast Reroute

In the following, we present heuristics for the path layout of both MPLS-FRR options. Both approaches increase the spreading of the backup traffic and decrease thereby the required backup capacity. More efficient path layouts can certainly be found, but they are more complex and only a few research papers address this issue [24–27].

One-to-One Backup The backup capacity requirements for one-to-one backup can be reduced by modifying the link detours as shown in Figure 5(a). All link detours except the first link within a path step one link back within the path and then take the same path as the corresponding router detour at this location [28]. We call this a push back detour.



(a) The $PushBackDetour(PLR, r_{tail})$ substitutes all $LinkDetour(PLR, r_{tail})$ of a path (except PLR is origin).

(b) $LinkBypasses(PLR, NHOP)$ are substituted by $RouterBypasses(PLR, NNHOP)$ and the bypass for the last link of the primary path is substituted by a $PushBackBypass(PLR, NHOP)$ except if PLR is also the origin.

Figure 5: Improved path layout for MPLS FRR.

Facility Backup The backup capacity requirements for the facility backup can be reduced by modifying the link backup as follows. Flows use the router bypasses instead of the link bypasses wherever possible. The last link of a flow is protected by a push back bypass. Figure 5(b) illustrates how the respective backup path sends the traffic one link back from which it came from and takes then the same path as the router bypass at this location. If a flow contains only a single link, this link is further protected by the conventional link bypass [29].

3 Results

In this section, we first explain the general experiment setup and the performance measure for the subsequent investigations. Then, we study how well different routing mechanisms can distribute the traffic in the network to achieve low link maximum utilizations $\rho_{\mathcal{S}}$ by their relative efficiency. We extent these experiments towards resilience mechanisms and the protection of single link failures. We illustrate the impact of the network structure on the ability of different resilience mechanisms to keep the maximum link utilization $\rho_{\mathcal{S}}$ low and, finally, we show how the protection of other failures influences the maximum link utilization $\rho_{\mathcal{S}}$.

3.1 Experiment Setup and Performance Measure

In [30] we have shown that the required backup capacity of a network depends significantly on its topological characteristics. We construct random networks for our experiments using the generator from [30]. They have a different size in terms of nodes $n \in \{10, 15, 20, 25, 30, 35, 40, 45, 50\}$, a different average node degree $\delta_{avg} \in \{3, 4, 5, 6\}$ which is the fraction $\delta_{avg} = \frac{m}{n}$ of the number of unidirectional links m and the number of nodes n. Furthermore, the degree of individual nodes may deviate by at most $\delta_{dev}^{max} \in \{1, 2, 3\}$ from the average node degree. We use 15 instances of each possible combination which yields 1620 different random networks that were evaluated for each routing or resilience mechanism in each experiment. The presentation of the results is very condensed and accounts only for the most relevant topological characteristics. We assumed that all links of the networks have the same capacity and that the corresponding traffic matrices are homogeneous, i.e., the same traffic rate is exchanged between any two nodes. We will justify this approach at the end of this section.

The primary performance measure of our study is the maximum link utilization $\rho_{\mathcal{S}}^X$ in the network over all protected failure scenarios $s \in \mathcal{S}$ which is obtained with a certain routing or resilience mechanism X. It is an indicator for the absolute efficiency of X with protection of $\mathcal{S}$. If unprotected failures occurs, the maximum link utilization can be significantly larger than $\rho_{\mathcal{S}}$, congestion can occur, and traffic might be lost. This has been studied in [31].

However, the maximum link utilization is not very expressive for comparisons as it depends on the link capacities and the traffic matrix. Therefore, we rather consider the *efficiency ratio* $f_{\mathcal{S}}^X(Y) = \rho_{\mathcal{S}}^X / \rho_{\mathcal{S}}^Y$, and compare the relative efficiency of different resilience mechanisms X and Y for the same set of protected failure scenarios $\mathcal{S}$. The value $f_{\mathcal{S}}^X(Y)$ indicates how much traffic can be transported with routing or resilience mechanism Y in comparison to X under the condition that the same maximum link utilization is achieved.

Similarly, we use the efficiency ratio $f_{\mathcal{S}}^X(\mathcal{S}') = \rho_{\mathcal{S}}^X / \rho_{\mathcal{S}'}^X$ and compare the impact of different sets of protected failure scenarios $\mathcal{S}$ and $\mathcal{S}'$ on the efficiency of X. Its interpretation is analogous to the one of $f_{\mathcal{S}}^X(Y)$. For the sake of a simple specification of $\mathcal{S}$, we abbreviate the failure-free scenario by $\emptyset$, the set of all single link failures by L, the set of all single router failures by R, and the set of all single link and single router failures by LR.

The structures, the link capacities, and the traffic matrices of the networks are certainly not realistic, but they serve our goals for two reasons. Firstly, our intention is the performance comparison of the resilience mechanisms by a parametric study regarding topological characteristics instead of investigating a few specific real world networks. Secondly, the absolute values of the link capacities and the traffic matrix determine the maximum link utilization $\rho_{\mathcal{S}}^{X}$ in a network. However, their scaling does not impact the efficiency ratios $f_{\mathcal{S}}^{X}(Y)=\rho_{\mathcal{S}}^{X}/\rho_{\mathcal{S}}^{Y}$ or $f_{\mathcal{S}}^{X}(\mathcal{S}')=\rho_{\mathcal{S}}^{X}/\rho_{\mathcal{S}'}^{X}$ as long as the respective experiments are conducted with the same network and traffic matrix.

3.2 Efficiency of Routing Mechanisms without Failure Protection

We compare the efficiency of different routing mechanisms relative to the one of standard SSP routing when no failures are protected, i.e. $\mathcal{S}=\{\emptyset\}$. Figure 6 shows the average efficiency ratios $f_{\emptyset}^{SSP}(Y)$ from all sample networks depending on the network size. Each point in the figure is an average value from 180 different networks. At first sight, we observe that the efficiency ratios for all routing mechanisms are larger than 1.0, i.e., their maximum link utilization is smaller than the one of SSP routing. Thus, SSP routing is less efficient than the other routing algorithms.

Optimized e2e explicit paths (optE2E) based on iSPM are most efficient. They increase the transmission capacity of the network by 60–140% compared to SSP routing and give thereby a lower bound on the optimization potential. There is hardly any difference whether 2-iSPM or k-iSPM is used for the selection of the paths. The efficiency of optimized ECMP routing is similar to the one of optE2E for small networks, but for large networks it is about 20% less efficient. Optimized SSP routing is about 20% less efficient than optECMP in small networks, but this difference decreases with increasing network size. The unoptimized routing mechanisms are clearly less efficient than the optimized methods. However, the NCSPs are 20% better than standard SSP routing in small networks and up to 50% in large network. The improvement results from the avoidance of the Lemming effect which is caused by destination based routing. Standard ECMP routing is also 35–40% better than standard SSP routing because it leads to a better traffic distribution in the network. Looking at all curves, we realize that the difference among the optimized routing algorithms is clearly visible, but the difference between optimized and unoptimized routing algorithms is larger. Thus, the routing efficiency can significantly be improved by optimization while the choice of the specific routing mechanism is secondary for networks without resilience requirements.

The efficiency of optimized routing mechanisms increases clearly with the network size. We explain that phenomenon in the following. In our study, we have a homogeneous traffic matrix and random networks with equal link bandwidths. Thus, there are mismatches between the bandwidth and the traffic rate on the links. As the possibility for strong mismatches increases with the network size, the potential to reduce the maximum link utilization $\rho_{\emptyset}^{SSP}$ by routing optimization also increases. Hence, although random networks are not realistic examples, they help to illustrate how well routing algorithms can exploit increasing optimization potentials.

3.3 Efficiency of Resilience Mechanisms with Protection of Single Link Failures

We conduct the same experiments as in Section 3.2 but now with protection of single link failures. That means, we consider the maximum link utilization from the failure-free operation

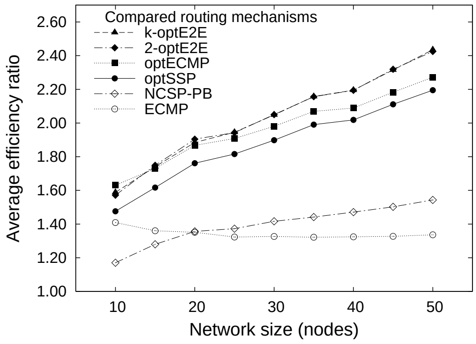
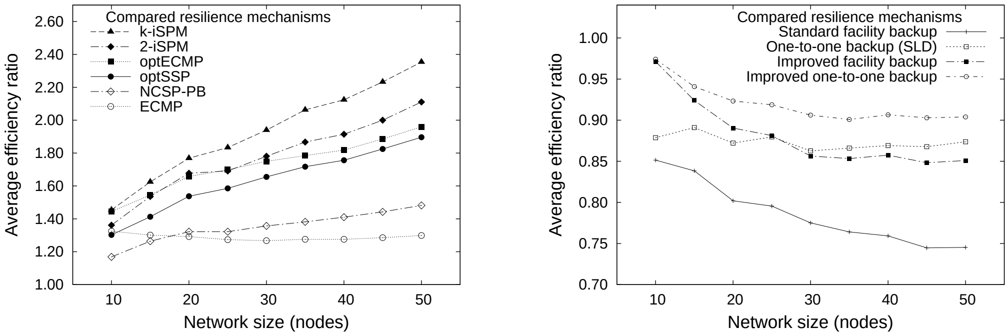


Figure 6: Efficiency ratios $f_{\emptyset}^{SSP}(Y)$ of various routing methods Y compared to default SSP routing without protection of any failures depending on the network size (nodes).

and all single link failure scenarios, and calculate the efficiency ratios $f_{L}^{SSP}(Y)$ of the resilience mechanism Y relative to SSP (re)routing.



(a) IP restoration and e2e protection switching.

(b) MPLS fast reroute.

Figure 7: Efficiency ratios $f_{L}^{SSP}(Y)$ of various resilience mechanisms Y compared to standard SSP (re)routing with protection of single link failures depending on the network size (nodes).

Figure 7(a) shows the efficiency ratios of the resilience mechanisms that correspond to the routing mechanisms studied in Figure 6. Note that iSPM corresponds to *k*-optE2E and the optimized simple primary/backup paths (2-iSPM) corresponds to 2-optE2E. At first sight, Figure 7(a) is very similar to Figure 6 since the qualitative behavior of the efficiency ratios is the same for all mechanisms. However, the efficiency ratios with link protection are about 5–30% lower than without any protection. In particular, 2-iSPM is about 25% worse than 2-optE2E while *k*-iSPM achieves almost the same efficiency ratios as *k*-optE2E. Thus, the advantage of multipath mechanisms becomes obvious for routing optimization with resilience requirements. They lead to a larger optimization potential than simple primary/backup paths mechanisms. The efficiency ratios for optimized IP routing (optSSP, optECMP) are with link protection about 20% smaller than without any protection, too. The efficiency of the unoptimized NCSP based primary/backup path concept and standard ECMP (re)routing is with link protection only slightly lower than without any protection. With link protection, the difference of the efficiency ratios between optimized and unoptimized resilience mechanisms is again very large, but the difference among the optimized resilience mechanisms is also considerable. Thus, the choice of the resilience mechanism does matter.

Figure 7(b) shows the efficiency ratios for MPLS FRR mechanisms relative to SSP (re)routing. They are all smaller than 1.0, i.e., the maximum link utilizations of the MPLS FRR mechanisms are larger than the one of SSP routing. Thus, SSP routing is more efficient than the MPLS FRR mechanisms. The standard facility backup (bypass) has the smallest efficiency ratios between 0.75 and 0.85, followed by the standard one-to-one backup (detour) with ratios between 0.87 and 0.89. The improved bypass achieves values between 0.85 and 0.97 and the improved detour lies between 0.90 and 0.97. Thus, facility backup requires the reservation of more backup capacity than one-to-one backup and the improved path layout for both FRR options leads to significantly larger efficiency ratios. We explain these findings in the following.

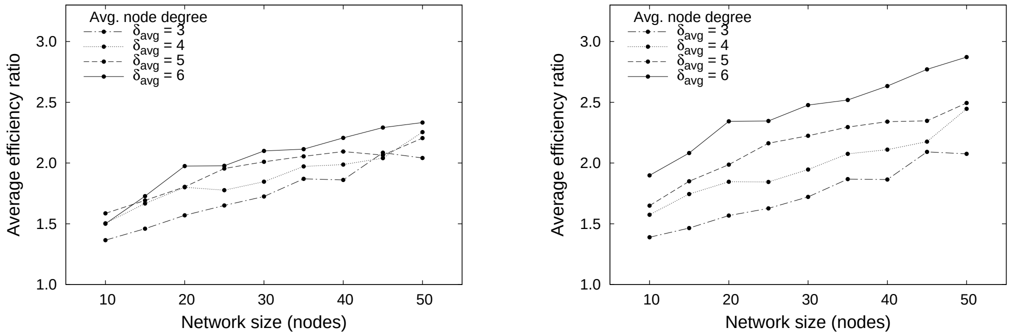
With the standard facility backup, the point of local repair (PLR) intentionally redirects all backup traffic over the same bypass tunnel when a link fails. As a consequence, the utilization of the corresponding backup links is very high in that case such that the maximum link utilization of SSP routing is exceeded by far. With one-to-one backup, the PLR distributes the traffic over different paths towards the destination. This leads to some distribution of the backup traffic and to lower utilization values of the backup links in failure cases. The improved facility and one-to-one backup versions differ from the standard versions by the substitution of link bypasses and detours through router bypasses and detours as well as by the introduction of push back bypasses and detours. These mechanisms lead to a better distribution of the backup traffic and, thereby, to a lower utilization on the backup links in failure cases. Similar results in a different context can be found in [28, 29].

We considered only simple improvements for MPLS FRR that can be deployed without a central configuration tool. However, we expect that its efficiency can be more improved by a rigorous optimization in a central path computation element (PCE) with global knowledge [32].

Note that Figures 7(a) and 7(b) do not inform about the required backup capacity. This issue is addressed in Section 3.5.

3.4 Impact of the Network Structure on the Efficiency of Resilience Mechanisms

Figures 8(a) and 8(b) illustrate the efficiency of optimized SSP routing and optimized e2e paths based on *k*-iSPM (*k*-optE2E) relative to standard SSP routing without protection of any failures. They show that the efficiency ratios increase not only with the network size but also with the average node degree, i.e., highly meshed networks have a larger potential for routing optimization than networks with a rather low average node degree. In sparsely meshed networks, *k*-optE2E is hardly better than optimized SSP routing since the topology offers only a few choices to route the traffic on disjoint paths. In well meshed networks, many disjoint paths can be found between two endpoints which creates a large optimization potential. As a consequence, the efficiency ratio of *k*-optE2E increases with the average node degree which illustrates also the increased optimization potential of such networks. However, optimized SSP routing can take only rather little advantage of that potential.



(a) Efficiency ratio $f_{\emptyset}^{SSP}(optSSP) = \rho_{\emptyset}^{optSSP}/\rho_{\emptyset}^{SSP}$ for optimized SSP routing.

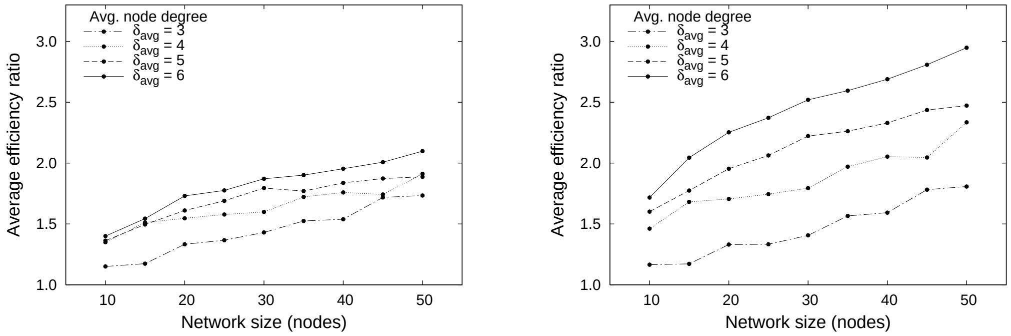
(b) Efficiency ratio $f_{\emptyset}^{SSP}(k\text{-optE2E}) = \rho_{\emptyset}^{k\text{-optE2E}}/\rho_{\emptyset}^{SSP}$ for *k*-optE2E.

Figure 8: Efficiency ratios for optimized SSP and *k*-optE2E relative to unoptimized SSP *without protection of any failures (∅)* depending on the network size and the average node degree.

Figures 9(a) and 9(b) illustrate the efficiency ratios of optimized SSP routing and the *k*-iSPM compared to default SSP routing with protection against single link failures. They are very similar to Figures 8(a) and 8(b). However, in networks with a low node degree of $\delta_{avg} = 3$, the efficiency ratios are clearly smaller with protection than without protection and in this particular case, they are again approximately equal for optSSP and *k*-iSPM. In contrast, in networks with a high node degree of $\delta_{avg} = 6$, the efficiency ratios for optSSP are significantly smaller with protection than without protection while they are the same for *k*-optE2E and *k*-iSPM. Obviously, the constraints for destination based routing prohibit an effective optimization of SSP routing in well meshed networks. Thus, in sparsely meshed networks, optimized SSP routing and the *k*-iSPM need about the same backup capacity while in well meshed networks, the *k*-iSPM is significantly more efficient.

3.5 Impact of the Protection Variant on the Efficiency of Resilience Mechanisms

In this section, we use the *k*-iSPM and the facility backup option of MPLS fast reroute as candidates for end-to-end and local protection mechanisms to test the impact of the protection variant on the efficiency. We consider the following protection variants: no protection (∅), protection of single link failures (*L*), protection of single router failures (*R*), and protection of single link and single router failures (*LR*). We calculate the efficiency ratios $f_{\emptyset}^{k\text{-iSPM}}(Y) = \frac{\rho_Y^{k\text{-iSPM}}}{\rho_{\emptyset}^{k\text{-iSPM}}}$ and $f_{\emptyset}^{Bypass}(Y) = \frac{\rho_Y^{Bypass}}{\rho_{\emptyset}^{SSP}}$ for the protection variants $Y \in \{L, R, LR\}$. We use standard SSP routing as the unprotected baseline for facility backup because standard MPLS FRR takes the shortest paths. The results are compiled in Figures 10(a) and 10(b).



(a) Efficiency ratio $f_L^{SSP}(optSSP) = \rho_L^{optSSP}/\rho_L^{SSP}$ for optimized SSP routing.

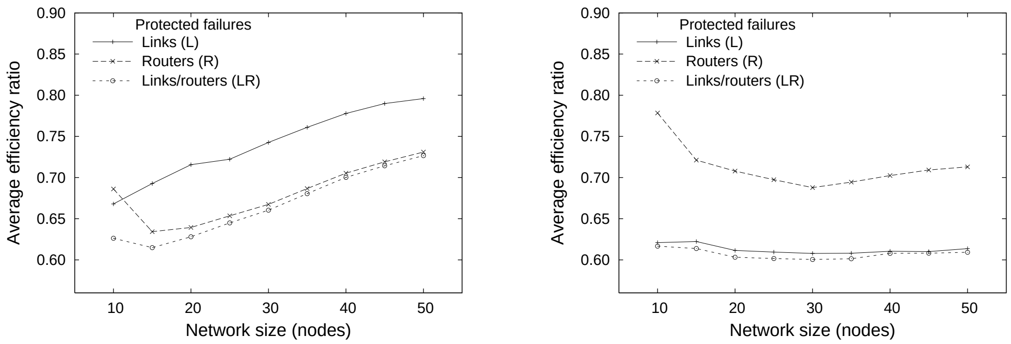
(b) Efficiency ratio $f_L^{SSP}(k\text{-iSPM})=\rho_L^{k\text{-iSPM}}/\rho_L^{SSP}$ for *k*-iSPM.

Figure 9: Efficiency ratios for optimized SSP and *k*-iSPM relative to unoptimized SSP *with protection of single link failures (L)* depending on the network size and the average node degree.

The curves for *L*, *R*, and *LR*-protection are clearly below 1.0. Networks with protection need some of their capacity to carry backup traffic and lead therefore to a larger maximum link utilization than networks without protection which decreases the efficiency ratios $f_{\emptyset}^{Y}(X)$ below 1 for any protection mechanism Y. For MPLS FRR, the efficiency ratios for link and router protection are about 0.6 and 0.72, respectively, and they are almost independent of the network size. For the *k*-iSPM, the efficiency ratios increase with increasing network size as we already observed in Sections 3.2, 3.3, and 3.4.

We verify that the efficiency ratio for *LR*-protection is lower than for the protection of only *L* or *R*. We realize that *L*-protection achieves larger efficiency ratios than *R*-protection for the *k*-iSPM while this is vice versa for facility backup. When a router fails, its adjacent links also fail. Thus, more capacity is missing in the presence of router failures than in the presence of link failures. However, this is not reflected by the efficiency ratios of the facility backup due to the following reason. The point of local repair (PLR) intentionally redirects all backup traffic over the same link bypass tunnel when a link fails. As a consequence, the utilization $\rho_s^{Bypass}(l)$ of the corresponding backup links l is very high in that particular failure scenario s such that the maximum link utilization ρ_L^{Bypass} is very high. The effect of this problem is reduced for router bypasses as they push back the traffic to different locations from where it is redistributed which reduces the overall amount of backup traffic on individual links. This is depicted in Figure 11. In general, e2e resilience mechanisms lead to less backup capacity requirements than local resilience mechanisms. A comparison of local (line) and e2e restoration in [33] supports this observation.

In Figure 10(a), the efficiency ratios for router protection are clearly larger for networks with 10 nodes than for networks with 15 nodes. This is due to the fact that networks with only 10 nodes need to carry 20% less traffic if a router fails since the traffic from and to this router is removed. This effect vanishes quickly for larger networks.



(a) Efficiency ratio $f_{\emptyset}^{k\text{-iSPM}}(Y) = \rho_Y^{k\text{-iSPM}}/\rho_{\emptyset}^{k\text{-iSPM}}$ of k-iSPM.

(b) Efficiency ratio $f_{\emptyset}^{Bypass}(Y) = \rho_Y^{Bypass}/\rho_{\emptyset}^{Bypass}$ of the MPLS facility backup relative to standard SSP routing without protection.

Figure 10: Efficiency ratio for k-iSPM and MPLS facility backup for different protection variants Y relative to the unprotected variant $\emptyset$.

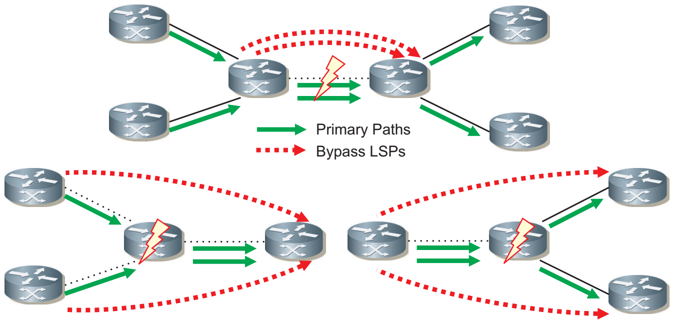


Figure 11: In contrast to link bypasses, router bypasses push back the traffic to different locations from where it is redistributed over different backup paths to the destination.

The fact that MPLS FRR mechanisms can support clearly less traffic than e2e protection mechanisms can be compared with cars and roads under construction. FRR resembles uninformed car drivers take their usual way and local detours at the construction site together with many other uninformed car drivers. They get stuck in a traffic jam since the detour road does not have enough capacity. If car drivers are warned early, they behave like e2e protection mechanisms and bypass the highway under construction in a wider area. The traffic on these roads hardly increases and, therefore, the drivers do not encounter a traffic jam.

4 Summary and Conclusion

A routing mechanism X is efficient if it can well exploit the network capacity, i.e., if it can transport the traffic matrix while keeping the maximum link utilization low. We compared the efficiency of the following routing or restoration and protection switching mechanisms: standard and optimized single shortest path (SSP, optSSP) and equal cost multipath (ECMP, optECMP) routing and rerouting, non-confluenting shortest paths (NCSP) and two versions of optimized explicit path routing (2-optE2E, *k*-optE2E), the standard and optimized primary/backup path concept (NCSP-PB, 2-iSPM), the (integer) self-protecting multipath (*k*-iSPM), as well as the default and improved facility and one-to-one backup options of MPLS fast reroute (FRR). We compared their efficiency without protection of any failures and for protection of single link failures, single router failures, and single link and router failures. We briefly summarize the most important findings of our study.

- Without protection, optimized routing is much more efficient than unoptimized routing. In comparison to that difference, the difference of the efficiency among the optimized routing mechanisms (optSSP, optECMP, 2-optE2E, *k*-optE2E) is rather small although it is clearly visible.

- With protection, the *k*-iSPM is the most efficient resilience mechanism followed by 2-iSPM, optECMP, and optSSP. The difference among them is significant. Standard and improved MPLS FRR are less efficient than standard SSP routing.

- In sparse networks, optSSP (re)routing is as efficient as *k*-optE2E routing and the *k*-iSPM, respectively. However, the superiority of *k*-optE2E and the *k*-iSPM becomes obvious in well meshed networks: they are 50% more efficient than optSSP and 200% more efficient than standard SSP routing.

- With protection of failures, protection switching and restoration mechanisms can carry only 60–80% of the traffic they can transport without failures. Usually, the protection of router failures needs more backup capacity than the protection of link failures unless the resilience mechanism lacks sufficient distribution of backup traffic in case of link failures.

We have shown that routing optimization can significantly improve the protected and unprotected throughput in a network and that the achievable improvement depends on the resilience mechanism. Apart from efficiency, there are also other important aspects that make routing and resilience mechanisms attractive. Shortest path routing mechanisms (SSP, ECMP) are very robust against unplanned and simultaneous multiple failures and MPLS FRR mechanisms react faster than e2e protection or restoration mechanisms. Currently, IP FRR mechanisms are under study, but their standardization is not finalized. We expect that their bandwidth efficiency is similar to or even worse than the one of the MPLS FRR methods, but quantitative results are not yet available. Certainly, their introduction will pose new challenging optimization problems.

References

[1] G. Iannaccone, C.-N. Chuah, S. Bhattacharyya, and C. Diot, “Feasibility of IP Restoration in a Tier-1 Backbone,” *IEEE Network Magazine (Special Issue on Protection, Restoration and Disaster Recovery)*, March 2004.

[2] J. Lang (Ed.), “RFC4204: Link Management Protocol (LMP),” Oct. 2005.

[3] P. Pan, G. Swallow, and A. Atlas, “RFC4090: Fast Reroute Extensions to RSVP-TE for LSP Tunnels,” May 2005.

[4] S. Rai, B. Mukherjee, and O. Deshpande, “IP Resilience within an Autonomous System: Current Approaches, Challenges, and Future Directions,” *IEEE Communications Magazine*, pp. 142–149, Oct. 2005.

[5] S. Iyer, S. Bhattacharyya, N. Taft, and C. Diot, “An Approach to Alleviate Link Overload as Observed on an IP Backbone,” in *IEEE Infocom*, (San Francisco, CA), April 2003.

[6] D. Oran, “RFC1142: OSI IS-IS Intra-Domain Routing Protocol,” Feb. 1990.

[7] M. Menth and R. Martin, “Network Resilience through Multi-Topology Routing,” in 5^{th} *International Workshop on Design of Reliable Communication Networks (DRCN)*, (Island of Ischia (Naples), Italy), pp. 271 – 277, Oct. 2005.

[8] B. Fortz and M. Thorup, “Internet Traffic Engineering by Optimizing OSPF Weights,” in *IEEE Infocom*, (Tel-Aviv, Israel), pp. 519–528, 2000.

[9] B. Fortz, J. Rexford, and M. Thorup, “Traffic Engineering with Traditional IP Routing Protocols,” *IEEE Communications Magazine*, vol. 40, no. 10, pp. 118–124, 2002.

[10] M. Pióro, Á. Szentesi, J. Harmatos, A. Jüttner, P. Gajowniczek, and S. Kozdrowski, “On Open Shortest Path First Related Network Optimisation Problems,” *Performance Evaluation*, vol. 48, pp. 201 – 223, 2002.

[11] M. Pióro and D. Medhi, *Routing, Flow, and Capacity Design in Communication and Computer Networks*. Morgan Kaufman, 2004.

[12] R. Martin, M. Menth, and U. Spoerlein, “Integer SPM: Intelligent Path Selection for Resilient Networks,” in *IFIP-TC6 Networking Conference (Networking)*, (Atlanta, GA, USA), May 2007.

[13] G. Willems, P. Arijs, W. V. Parys, and P. Demeester, “Capacity vs. Availability Trade-offs in Mesh-Restorable WDM Networks,” in *International Workshop on the Design of Reliable Communication Networks (DRCN)*, (Budapest, Hungary), Oct. 2001.

[14] M. Menth, R. Martin, and U. Spoerlein, “Network Dimensioning for the Self-Protecting Multipath: A Performance Study,” in *IEEE International Conference on Communications (ICC)*, (Istanbul, Turkey), June 2006.

[15] B. Fortz and M. Thorup, “Robust Optimization of OSPF/IS-IS Weights,” in *International Network Optimization Conference (INOC)*, (Paris, France), pp. 225–230, Oct. 2003.

[16] D. Yuan, “A Bi-Criteria Optimization Approach for Robust OSPF Routing,” in 3^{rd}*IEEE Workshop on IP Operations and Management (IPOM)*, (Kansas City, MO), pp. 91 – 98, Oct. 2003.

[17] A. Nucci, B. Schroeder, S. Bhattacharyya, N. Taft, and C. Diot, “IGP Link Weight Assignment for Transient Link Failures,” in 18th *International Teletraffic Congress (ITC)*, (Berlin), Sept. 2003.

[18] A. Sridharan and R. Guerin, “Making IGP Routing Robust to Link Failures,” in *IFIP-TC6 Networking Conference (Networking)*, (Ontario, Canada), May 2005.

[19] M. Menth, M. Hartmann, and R. Martin, “Robust IP Link Costs for Multilayer Resilience,” in *IFIP-TC6 Networking Conference (Networking)*, (Atlanta, GA, USA), May 2007.

[20] R. Bhandari, *Survivable Networks: Algorithms for Diverse Routing*. Norwell, MA, USA: Kluwer Academic Publishers, 1999.

[21] M. Menth, R. Martin, and U. Spoerlein, “Optimization of the Self-Protecting Multipath for Deployment in Legacy Networks,” in *IEEE International Conference on Communications (ICC)*, (Glasgow, Scotland, UK), June 2007.

[22] R. Martin, M. Menth, and M. Hemmkeppler, “Accuracy and Dynamics of Hash-Based Load Balancing Algorithms for Multipath Internet Routing,” in *IEEE International Conference on Broadband Communication, Networks, and Systems (BROADNETS)*, (San Jose, CA, USA), Oct. 2006.

[23] R. Martin, M. Menth, and M. Hemmkeppler, “Accuracy and Dynamics of Multi-Stage Load Balancing for Multipath Internet Routing,” in *IEEE International Conference on Communications (ICC)*, (Glasgow, Scotland, UK), June 2007.

[24] H. Saito and M. Yoshida, “An Optimal Recovery LSP Assignment Scheme for MPLS Fast Reroute,” in *International Telecommunication Network Strategy and Planning Symposium (Networks)*, pp. 229–234, June 2002.

[25] G. Li, D. Wang, C. Kalmanek, and R. Doverspike, “Efficient Distributed Path Selection for Shared Restoration Connections,” in *IEEE Infocom*, 2002.

[26] D. Wang and G. Li, “Efficient Distributed Solution for MPLS Fast Reroute,” in 4rd*IFIP-TC6 Networking Conference (Networking)*, (Waterloo, Onatrio, Canada), pp. 502 – 513, May 2005.

[27] G. Li, D. Wang, and R. Doverspike, “Efficient Distributed MPLS P2MP Fast Reroute,” in *IEEE Infocom*, Apr. 2006.

[28] R. Martin, M. Menth, and K. Canbolat, “Capacity Requirements for the One-to-One Backup Option in MPLS Fast Reroute,” in *IEEE International Conference on Broadband Communication, Networks, and Systems (BROADNETS)*, (San Jose, CA, USA), Oct. 2006.

[29] R. Martin, M. Menth, and K. Canbolat, “Capacity Requirements for the Facility Backup Option in MPLS Fast Reroute,” in *IEEE Workshop on High Performance Switching and Routing (HPSR)*, (Poznan, Poland), June 2006.

[30] M. Menth, *Efficient Admission Control and Routing in Resilient Communication Networks*. PhD thesis, University of Würzburg, Faculty of Computer Science, Am Hubland, July 2004.

[31] M. Menth, R. Martin, and U. Spoerlein, "Impact of Unprotected Multi-Failures in Resilient SPM Networks: a Capacity Dimensioning Approach," in *IEEE Globecom*, (San Francisco, California, USA), Nov. 2006.

[32] A. Farrel, J.-P. Vasseur, and J. Ash, "RFC4655: A Path Computation Element (PCE)-Based Architecture," Aug. 2006.

[33] K. Murakami and H. S. Kim, "Optimal Capacity and Flow Assignment for Self–Healing ATM Networks Based on Line and End-to-End Restoration," *IEEE/ACM Transactions on Networking*, vol. 6, pp. 207–221, Apr. 1998.