Impact of Multi-Failures in Survivable Networks

Rüdiger Martin, Michael Menth, and Ulrich Spoerlein
Institute of Computer Science, University of Würzburg
Am Hubland, D-97074 Würzburg, Germany
E-mail:{martin|menth|spoerlein}@informatik.uni-wuerzburg.de

Abstract

Link and router failures lead to disconnection in networks, which can possibly be repaired by restoration and protection switching mechanisms within seconds or milliseconds. However, redirected traffic causes congestion unless sufficient backup capacity is provided for failure scenarios. In previous work we showed that the required backup capacity for the protection switching mechanism "self-protecting multipath" (SPM) can effectively be reduced by optimized load balancing when resilience against single failures is needed. In this work, we look at double-failure resilience, compare the backup capacity demands for different levels of multi-failure survivability both for the optimized SPM and shortest path routing (SPR), and study the impact of unprotected multi-failures in such networks.

1 Introduction

Network element failures in IP networks lead to traffic rerouting and, therefore, potentially to congestion and traffic loss. Router failures are more severe than link failures because they correspond to the failure of several links and traffic originating from them or being destined to them is lost. To maintain the mere connectivity of the network, restoration or protection switching mechanisms deviate the traffic over backup paths around the failure location. Restoration mechanisms like single shortest path re-routing (SPR) re-converge after a network failure and maintain the network connectivity as long as at least one path from source to destination exists through the network. In contrast, protection switching mechanisms react faster than restoration mechanisms as they rely on a preplanned disjoint primary/backup path structure. However, if both the primary and the backup path are affected by network failures, the end-to-end (e2e) connectivity is lost even though there is still a working path in the network. In such a case, traffic forwarding may fall back on SPR to maintain connectivity at the price of a slow reaction.

During local outages, redirected traffic increases the load on backup paths. This may lead to congestion, to excessive packet loss and delay, i.e. to severe quality of service (QoS) degradation. Thus, a network being truly resilient against a set of protected failure scenarios $\mathcal{S}$ requires not only intelligent restoration or protection switching, but also sufficient backup capacity. In particular, truly resilient networks require so much capacity that redirected traffic can be accommodated in all protected failure scenarios $\mathcal{S}$. Usually, the set of protected failure scenarios $\mathcal{S}$ comprises all single link failures (L) and sometimes also all single router failures (R).

In previous work [1], we have studied the impact of double failures on the potential congestion for networks being truly resilient to single failures (L,R). We showed for the protection switching mechanism "self-protecting multipath" (SPM) that optimized load balancing can reduce the required backup capacity significantly. In this work, we dimension networks for resiliency against single *and* double failures whereby we address different degrees of survivability: resilience against double link failures (LL), simultaneous link and router failures (LR), and double router failures (RR). We compare the capacity demands for several resilience levels both for the SPM and for SPR, and illustrate the impact of unprotected double failures in networks being resilient for L, R, and LL.

The paper is structured as follows. Section 2 gives a short overview on resilience mechanisms and in particular explains the SPM. Section 3 analyzes the impact of unplanned double failures on the connectivity and the lost traffic for SPR and SPM in networks resilient to single failures. Section 4 in contrast analyzes the impact of unplanned double failures in networks resilient to single failures and double link failures. Finally, in Section 5 we summarize this work and draw our conclusions.

2 Resilience Mechanisms and Backup Capacity Minimization

In this section we give a brief overview on resilience mechanisms to distinguish their basic functionality in this context. A broader and more complete overview on resilience mechanisms can be found, for instance, in [2]. They can be divided into restoration and protection schemes. Restoration sets up a new paths after a failure while protection switching pre-establishes backup paths in advance.

2.1 Restoration

Restoration tries to find new routes or set up explicit backup paths when the traffic cannot be forwarded anymore due to link or node failures. Usually, restoration is applied by IP routing. The disadvantage of such methods is obvious: they are slow. However, the reconvergence of the IP routing algorithm is a very simple and robust restoration mechanism [3, 4, 5] which works for both single path routing with SPR and multipath routing with the equal cost multipath (ECMP) option. In particular, connectivity is maintained as long as source and destination are physically connected in the network.

2.2 Protection Switching Mechanisms

Protection addresses the problem of slow reconvergence speed. It is usually implemented in multiprotocol label switching (MPLS) technology due to its ability to pre-establish explicitly routed backup paths in advance. Depending on the place where the reaction to failures is done, protection switching mechanisms can be distinguished into end-to-end and local protection.

2.2.1 End-to-End Protection Switching

In case of end-to-end protection switching the reaction to a failure along a path is executed at the path ingress router.

Primary and Backup Paths The classical end-to-end protection switching concept is the concept of primary and backup paths. Backup paths are set up simultaneously with primary paths and in case of a failure, the traffic is just shifted at the path ingress router from a broken primary path to the corresponding backup path. This is called ent-to-end protection. It is faster than restoration methods, but the signalling of the failure to the path ingress router takes time and traffic being already on the way is lost.

Self-Protecting Multipath The self-protecting multipath (SPM) has been presented first in [6]. Its path layout consists of disjoint paths and the traffic is distributed over all of them according to a traffic distribution function (see Figure 1). If a single path fails, the traffic is redistributed over the working paths according to another traffic distribution function. Thus, a specific load balancing function $\mathbf{l_d^f}$ is required for each demand d and for every pattern $\mathbf{f}$ of working and non-working paths. Opposed to the conventional primary and backup paths concept, the SPM does not distinguish between a dedicated primary and backup paths. Both under failure-free conditions and in case of network failures, the traffic may be spread over several of the disjoint paths. And in contrast to optimum primary and backup paths [7], the SPM performs a traffic shift only if at least one of its disjoint paths is affected by a failure. Thus, the reaction is based on local information and signalling of remote failures across the network is not required. This is important as the connectivity in such a situation is compromised. The path layout for the SPM is calculated preferably by the k-disjoint-shortest-path algorithm [8] to maximize its number of disjoint paths and the load balancing function can be optimized by non-integer linear programs [9, 10].

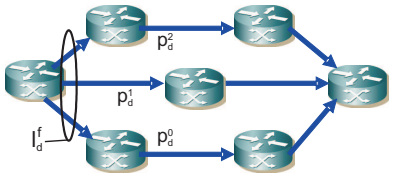


Figure 1: The SPM distributes the traffic of a demand d over disjoint paths $\mathbf{P_d} = (\mathbf{p_d^0}, ..., \mathbf{p_d^{k_d-1}})$ according to a traffic distribution function $\mathbf{l_d^f}$ which depends on the pattern $\mathbf{f}$ of working and non-working paths.

2.2.2 Local Protection Switching

Local protection schemes tackle the problem of lost traffic in case of end-to-end protection during the signalling period. Backup paths towards the destination are set up not only at the ingress router of the primary path but also at almost every node of the path. Then, a backup path is immediately available if the path breaks at some location. Local protection switching can be implemented by MPLS-FRR [11]. Currently, fast reroute mechanisms are also under discussion and development for IP routing (IP-FRR) to provide a fast local reaction in IP networks. [12, 13]

3 Networks with Resilience against Single Link and Router Failures

In this section, we review the work of [1] where we studied the impact of double failures in networks that are resilient to single failures only. That means, we dimension networks with so much capacity that single link or node failures do not lead to congestion, evaluate the congestion arising from different double failures (LL, LR, RR), and compare the results for both SPR and SPM routing.

We first explain our methodology to assess the required backup capacity. Then, we describe the optimization of the traffic distribution functions of the SPM. Finally, we analyze the impact of multi-failures in networks with single-failure resilience.

3.1 Calculation of Required Backup Capacity

The traffic matrix and the routing determine the load on the links. Thus, the required link bandwidths can be calculated for a given traffic matrix and routing. If a failure occurs in the network, the routing changes due to protection switching or rerouting which leads then to different capacity demands for the links. We consider a set of protected failure scenarios $\mathcal{S}$ and provide the link with the maximum capacity demands for all these failures. This leads to resilient network provisioning, i.e., protected failures do not cause congestion due to redirected traffic in such a network. The required network capacity is the sum of the capacities of all links in the network. We denote the required network capacity for SPR in a non-resilient network by $C^{\emptyset}_{SPR}$ and $C^{\mathcal{S}}_{SPR}$ is the required capacity in a resilient network to cover all protected failure scenarios $\mathcal{S}$. The relative required backup capacity is then $\frac{C^{\mathcal{S}}_{SPR}-C^{\emptyset}_{SPR}}{C^{\emptyset}_{SPR}} \cdot 100\%$. Similarly, we can calculate the required backup capacity for other restoration or protection switching mechanisms, but we always use $C^{\emptyset}_{SPR}$ as a reference to calculate the required backup capacity since SPR yields the minimum network capacity to support the traffic matrix in the network.

3.2 Capacity Savings by the Optimized SPM

In packet-switched networks, backup resources can be shared among different aggregates in different failure scenarios. This backup capacity sharing can intentionally be used to minimize the required backup capacity and, thereby, reduce the network costs. We assessed this potential in [9], where we optimized the load balancing function of the SPM for all single link and router failures (L, R) to reduce the required backup capacity using linear programs (LPs). The study was conducted in the Labnet03 network from the KING project [14] and in 240 different random networks constructed according to the algorithm in [15]. The topology of the Labnet03 is given in Figure 2. It is typical for North-American core networks. It comprises $n = 20$ nodes and $m = 53$ bidirectional links. The network has a resilient structure since a single link or node failure cannot divide the network into two different components. However, the simultaneous failure of the nodes Hou and Atl separate the nodes NeO, Orl, and Mia from the remaining network.

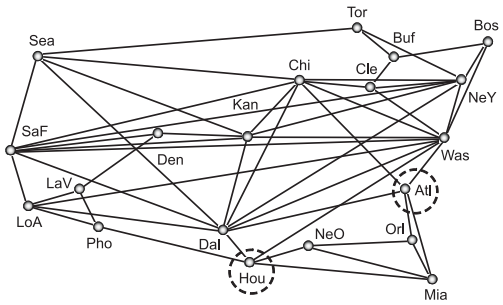


Figure 2: Topology of the Labnet03: the simultaneous failure of Hou and Atl separates the network into two disconnected islands.

Following the (L,R)-resilient dimensioning approach, we need 93% backup capacity relative to a non-resilient dimensioning approach for SPR in case of a homogeneous traffic matrix, but only 48% backup capacity is required under the same conditions for the SPM. For the heterogenous traffic matrix given in [15] these values are 87% and 39%, respectively. In [1] we studied the resiliency of SPM networks dimensioned for single failures (L, R) while for this work we additionally consider optimized SPM networks dimensioned to survive single failures (L, R) and double link failures (LL) without congestion. To that end, we need to extend our optimization algorithm for double failures. We abbreviate these differently optimized SPM structures by SPM$^{\text{s-opt}}$ (single failures) and by SPM$^{\text{d-opt}}$ (including double failures).

3.3 Impact of Double Failures in Networks with Resilience against Single Link and Router Failures

As a resilient SPM$^{\text{s-opt}}$ network requires significantly less capacity than a resilient SPR network, we compare the impact of the following unprotected double failures scenarios:

LL: all double link failures,

LR: all simultaneous and independent link and router failures,

RR: all double router failures, and

DF: all double failures (LL $\cup$ LR $\cup$ RR).

The performance measures of interest are:

D: the percentage of disconnected traffic,

K: the percentage of traffic experiencing congestion,

L(g): the percentage of lost traffic per aggregate, and

L: the percentage of lost traffic in general.

In the following, we review these results that were presented in [1] for the Labnet03 network and a homogeneous traffic matrix.

3.3.1 Disconnected Traffic

The connectivity of an aggregate may be compromised by link and router failures. It is disconnected if no path can be found between its endpoints by the routing. SPR always finds a route through the network as long as it is physically connected. In contrast, the explicit routes of the SPM are not automatically reorganized when broken. If the SPM has only two disjoint paths from a source to a destination, a double failure can hit both of them and disconnect the traffic aggregate. Then, the connectivity is interrupted and the traffic is lost in case of SPM (SPM$^{\text{s-opt}}$-INTR). A repair option is to forward the disconnected traffic by SPR as fallback solution (SPM$^{\text{s-opt}}$-SPR) if possible.
The set $\mathcal{G}$ comprises all traffic aggregates $g \in \mathcal{G}$ in the network, and the rate of these aggregates is denoted by $c(g)$. The function $D(g,s)$ yields 0 if the aggregate $g \in \mathcal{G}$ is still connected in failure scenario s, otherwise it yields 1. The percentage of the disconnected traffic for a specific failure scenario $s \in \mathcal{S}$ is

$$E_{\mathcal{G}}(D(\cdot,s)) = \frac{\sum_{g\in\mathcal{G}} c(g)\cdot D(g,s)}{\sum_{g\in\mathcal{G}} c(g)}. \quad (1)$$

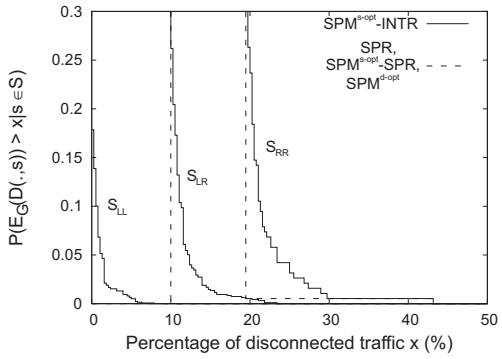
This is the base for the calculation of the complementary cumulative distribution function (CCDF) $P(E_{\mathcal{G}}(D(.,s)) > x | s \in \mathcal{S})$ of the percentage of disconnected traffic under the condition that the failure scenario s belongs to the set $\mathcal{S}$.
Figure 3(a) shows the CCDF of the disconnected traffic for SPR and SPM. We first discuss the results for SPR. In case of double link failures (LL), all aggregates remain connected leading to a straight vertical line at $x = 0$. For the link and router failures (LR), the aggregates starting or ending at the failed router are disconnected. These are exactly $2n$ out of $n\cdot(n–1)$ aggregates which leads to a straight vertical line at $\frac{38}{380} = 0.1$ due to assumption of a homogeneous traffic matrix. When two routers fail (RR), at most $(n-2)\cdot(n-3)$ out of $n\cdot(n-1)$ aggregates remain connected for every $s \in$ RR. Therefore, we have an almost straight line at $\frac{380-326}{380} = 0.195\%$. Only the simultaneous outage of router Hou and Atl effects the separation of the Labnet03 network which leads to the disconnection of 43% of all aggregates. However, this special case out of $|\text{RR}| = 190$ yields a very low probability for the outage of such a large amount of traffic. The SPM$^{\text{s-opt}}$-INTR leads to disconnection more easily than SPR due to the missing repair option. However, Figure 3(a) shows that SPM$^{\text{s-opt}}$-INTR leads to at most 12% more disconnected traffic compared to SPR for all considered double failure scenarios. In addition, in more than 95% of the cases, SPM$^{\text{s-opt}}$-INTR disconnects only at most 2% more traffic than SPR. The SPM$^{\text{s-opt}}$-SPR with repair option leads to the same connectivity as SPR.

3.3.2 Congested Traffic

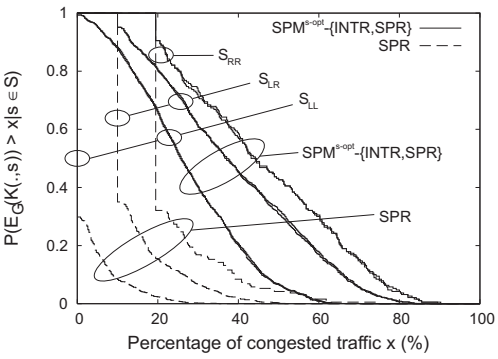
In case of a failure, traffic is redirected and may lead to congestion on backup paths if capacity is missing. For each aggregate we take the missing relative capacity of the links within its path to estimate an upper bound of its lost traffic. If there is enough capacity, the function $K(g,s)$ yields 0, otherwise it yields 1, thus, it indicates whether the traffic is forwarded over a congested link. The x-axis of Figure 3(b) presents the percentage of the traffic that suffers from disconnection or congestion. Therefore, the curves in Figure 3(a) provide a lower bound to the curves in Figure 3(b). Depending on the type of double failure up to 30%, 50%, or 65% of the aggregates may be affected for SPR. The SPM$^{\text{s-opt}}$ is more sensitive to double failures than SPR in the sense that up to 65%, 80%, or 85% of the traffic suffers from connection loss or congestion. The two variants SPM$^{\text{s-opt}}$-INTR and SPM$^{\text{s-opt}}$-SPR yield very similar results. We observe slightly less congested traffic for SPM$^{\text{s-opt}}$-INTR than for SPM$^{\text{s-opt}}$-SPR because in some cases, discarding traffic prevents congestion on potential backup paths.

3.3.3 Lost Traffic

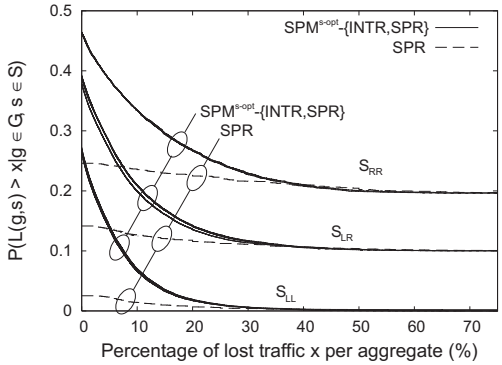
We consider now the percentage of the traffic from the perspective of individual aggregates. We calculate an upper bound $L(g,s)$ of the traffic that is lost due to disconnection or congestion for a specific $g \in \mathcal{G}$ in a specific failure scenario $s \in \mathcal{S}$. Figure 3(c) shows the corresponding CCDF which is calculated by $P(L(g,s) > x | g \in \mathcal{G}, s \in \mathcal{S})$. Again, we differentiate the three different sets of double failures (LL,LR,RR). The percentage of disconnected aggregates in Figure 3(a) is a lower bound for the corresponding CCDFs in Figure 3(c) because the disconnection of an aggregate leads to 100% traffic loss. Traffic redirection by SPR causes up to 25%–35% additional traffic loss but only in very rare cases. The SPM$^{\text{s-opt}}$ leads to a larger number of congested aggregates than SPR (cf. Figure 3(b)), but Figure 3(c) shows that the traffic loss is mostly rather small ($<$20%) if congestion occurs.
The percentage of the overall lost traffic is $E_{\mathcal{G}}(L(.,s)) = \frac{\sum_{g\in\mathcal{G}} c(g)\cdot L(g,s)}{\sum_{g\in\mathcal{G}} c(g)}$. Figure 3(d) shows the CCDF of this quantity with respect to the considered set of failure scenarios $\mathcal{S}$. The curves for the disconnected traffic in Figure 3(a) provide lower bounds and the curves for the congested traffic in Figure 3(b) provide upper bounds to the curves for lost traffic in



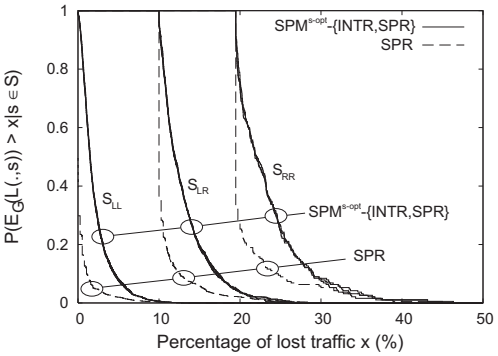
(a) CCDF of the percentage of disconnected traffic.



(b) CCDF of the percentage of disconnected and congested traffic.



(c) CCDF of the percentage of lost traffic per aggregate.



(d) CCDF of the percentage of overall lost traffic.

Figure 3: Impact of double failures on the disconnection, congestion, and traffic loss for SPR and SPM$^{\text{s-opt}}$-variants in the Labnet03 network dimensioned for resilience against single link and router failures.

Figure 3(d). Although lot of traffic is congested in SPR networks, much less traffic is really lost. The maximum lost traffic for SPM$^{\text{s-opt}}$ does not visibly go beyond the one for SPR.

We further average the percentage of the overall lost traffic over the considered sets of double failure scenarios. The results are summarized in Table 1. For SPM$^{\text{s-opt}}$ about 2% more traffic is lost in LL, LR, or RR than for SPR or ECMP.

Table 1: Lost traffic due to double failures in Labnet03 resilient to single failures in %.

failure set	SPR	SPM$^{\text{s-opt}}$-INTR	SPM$^{\text{s-opt}}$-SPR
LL	0.436	2.089	2.059
LR	10.890	12.966	13.018
RR	21.035	23.321	23.426
DF	0.508	2.164	2.134

To average the lost traffic over all double failure scenarios DF, we assume that link and router failures are independent of each other and that the probabilities for single link and router failures are 10^{-4} and 10^{-6} [16], respectively. We summarize the resulting probabilities for the different sets of failure scenarios in Table 2.

Table 2: Probability of specific failure scenarios in the Labnet03 network.

failure set	probabilty
$\emptyset$	0.9947
L	$0.5272 \cdot 10^{-2}$
R	$1.9894 \cdot 10^{-5}$
LL	$1.3710 \cdot 10^{-5}$
LR	$1.0545 \cdot 10^{-7}$
RR	$1.8899 \cdot 10^{-10}$
DF	$1.3680 \cdot 10^{-5}$

In Table 1 we realize that the overall lost traffic for all double failure scenarios DF is clearly dominated by the overall lost traffic in case of double link failures LL

because the probability of LL dominates the one of all other sets of failure scenarios. Therefore, we consider the option to provide more bandwidth and to protect the network against congestion due to double link failures, too. The impact of double failures in such networks is investigated in the next section.

4 Networks with Resilience against Single Link and Router Failures and Double Link Failures

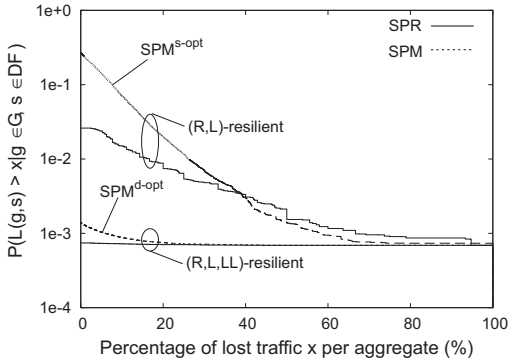
We first quantify the capacity savings by the optimized SPM for networks that are resilient against single failures and double link failures and then examine the impact of unprotected double failures in these networks.

4.1 Capacity Savings by the Optimized SPM

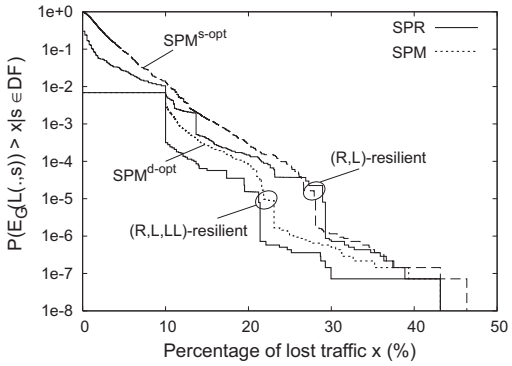
Table 3 shows the amount of required backup capacity for SPR and different versions of the SPM for different degrees of resiliency in the Labnet03 for a homogeneous traffic matrix. The networks are provided with so much capacity that congestion cannot occur in the protected failure scenarios. We consider three different versions of the SPM: optimized routing for single failures with and without the traffic rerouting option ($SPM^{s\text{-}opt}$-SPR, $SPM^{s\text{-}opt}$-INTR) and optimized routing for single link and router failures including the respective set of double ($SPM^{d\text{-}opt}$) with SPR rerouting as default. All three variants of the SPM require significantly less capacity than SPR. In particular, SPR requires 183% backup capacity while $SPM^{d\text{-}opt}$ requires only 92% to protect L, R, and LL failures. In contrast, SPR can protect only L and R failures with 92% backup capacity. The protection of all single and double failures (L, R, LL, LR, RR) requires another 50%–60% more capacity than the protection of L, R, and LL. The optimization of the load balancing function for double failures reduces the required backup capacity of the SPM by about 25% compared with its optimization for single failures only.

4.2 Impact of Double Failures in Networks with Resilience against Single Link and Router Failures and Double Link Failures

Our intention is to add resilience against double link failures to minimize the lost traffic due to congestion in case of general double link or router failures (LL, LR, RR). In contrast to the last section, we consider now the lost traffic averaged over all double failure scenarios.



(a) Complementary distribution function of the congestion strength of all aggregates (disconnected = 100% congested).



(b) Complementary distribution function of the percentage of lost traffic in the network.

Figure 4: Impact of double failures on the traffic loss for SPR and $SPM^{d\text{-}opt}$ in the Labnet03 network dimensioned for resilience against single link and router failures and double link failures.

Figure 4(a) shows the CCDF of the lost traffic per aggregate for all aggregates $g \in \mathcal{G}$ and double failure scenarios $s \in$ DF. An aggregate is disconnected with the same rather low probability for SPR and SPM for both dimensioning approaches. Therefore, the curves converge to that probability for a traffic loss of 100%. The probability to lose a certain amount of traffic differs by up to two orders of magnitude in networks resilient against single failures only (L, R) and in networks also resilient against double link failures (L, R, LL). In networks also resilient against double link failures (L, R, LL), hardly any traffic is lost due to congestion which can be seen from the fact that the curves hardly exceed the horizontal line. With single failure resilience only, the impact of the routing method is clearly visible for small amounts of lost traffic, but it is rather negligible

Table 3: Capacity requirements and backup capacity for different resilience and routing options together with the corresponding lost traffic in the presence double failure scenarios.

Sets of protected failures		SPR	SPR$^{\text{s-opt}}$-INTR	SPM$^{\text{s-opt}}$-SPR	SPM$^{\text{d-opt}}$
$\emptyset$	Capacity requirement	816.00	822.00	822.00	-
	Backup capacity	0%	0%	0%	-
L,R	Capacity requirement	1578.00	1215.18	1215.18	-
	Backup capacity	93%	48%	48%	-
	Lost traffic in DF	0.508%	2.164%	2.131%	-
L,R,LL	Capacity requirement	2321.00	-	1793.18	1567.32
	Backup capacity	183%	-	119%	92%
	Lost traffic in DF	0.070%	-	0.072	0.074%
L,R,LL,LR,RR	Capacity requirement	2757.00	-	2222.71	2027.57
	Backup capacity	238%	-	172%	148%
	Lost traffic in DF	0.0003%	-	0.0003%	0.0003%

in the case of additional double failure resilience.

Figure 4(b) contrasts the CCDFs of the percentage of the overall lost traffic in case of double failures (DF) in the Labnet03 with a capacity dimensioned for resilience against single failures (L, R) and for additional double link failures (L, R, LL), respectively. Again, we see that the additional capacity decreases the probability for traffic loss by up to two orders of magnitude. Compared to that, the curves of the two different routing methods are quite close together.

We condense the information of the CCDFs into single numbers by averaging the lost traffic over all double failure scenarios in DF and summarize them in Table 3. Note that the probability for double failures in general (LL, LR, RR) is only $1.3815 \cdot 10^{-3}$% in the Labnet03. The percentage of lost traffic in case of double failures can be greatly reduced by adding capacity for double link failure scenarios (LL). It can be further reduced by adding even more capacity to avoid congestion in case of combined link and router failures (LR) and double router failures (RR). However, these failure types are quite unlikely and (L, R, LL)-resilience already leads to very little lost traffic. Therefore, there is a tradeoff between additional amount of required backup capacity (53-56%) and the saved traffic loss depending on the intended network service.

5 Conclusion

Resilient networks are provided with extra capacity to avoid congestion and lost traffic due to redirected traffic in failure scenarios. In networks with resilience against single failures, congestion occurs only in the presence of double failures. As double link failures are the most probable double failures, we compared in this work the following two resilience options: networks with resilience against single failures and networks with additional resilience against double link failures.

We considered two different routing mechanisms and tested them in the Labnet03 for the two resilience options: shortest path routing (SPR) and the self-protecting multipath (SPM) whose load balancing functions are optimized to minimize the required backup capacity. We showed that the optimized SPM requires for the same level of reliability significantly less capacity than SPR. In particular, the SPM can provide additional resilience against double link failures with the same capacity that is needed by SPR to provide resilience against single link and router failures.

In spite of the reduced amount of backup capacity, the lost traffic in the case of unprotected double failures is in the same order of magnitude for the SPM as for the SPR. This holds for both discussed resilience options. The additional resilience against double link failures almost eliminates the lost traffic due to congestion in the presence of double failures.

References

[1] 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.

[2] A. Autenrieth and A. Kirstädter, "Engineering End-to-End IP Resilience Using Resilience-Differentiated QoS," *IEEE Communications Magazine*, vol. 40, no. 1, pp. 50–57, Jan. 2002.

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

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

[5] 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, Oct. 2003, pp. 91 – 98.

[6] M. Menth, A. Reifert, and J. Milbrandt, “Self-Protecting Multipaths - A Simple and Resource-Efficient Protection Switching Mechanism for MPLS Networks,” in 3^{rd}*IFIP-TC6 Networking Conference (Networking)*, Athens, Greece, May 2004, pp. 526 – 537.

[7] 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, no. 2, pp. 207–221, Apr. 1998.

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

[9] 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.

[10] 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.

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

[12] M. Shand and S. Bryant, “IP Fast Reroute Framework,” http://www.ietf.org/internet-drafts/draft-ietf-rtgwg-ipfrr-framework-06.txt, Oct. 2006.

[13] S. Bryant and M. Shand, “IP Fast Reroute Using Notvia Addresses,” http://www.ietf.org/internet-drafts/draft-bryant-shand-ipfrr-notvia-addresses-00.txt, Mar. 2005.

[14] C. Hoogendoorn, K. Schrodi, M. Huber, C. Winkler, and J. Charzinski, “Towards Carrier-Grade Next Generation Networks,” in *International Conference on Communication Technology (ICCT)*, Beijing, China, April 2003.

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

[16] J.-P. Vasseur, M. Pickavet, and P. Demeester, *Network Recovery*, 1st ed. Morgan Kaufmann / Elsevier, 2004.