Impact of Unprotected Multi-Failures in Resilient SPM Networks: a Capacity Dimensioning Approach

Michael Menth, Ruediger Martin, and Ulrich Spoerlein
Department of Distributed Systems, Institute of Computer Science, University of Würzburg, Germany
Email: {menth,martin,spoerlein}@informatik.uni-wuerzburg.de

***Abstract*— Restoration or protection switching mechanisms protect traffic in packet-switched networks against local outages by deviating it around the failure location. This assures connectivity, but sufficient backup capacity is also needed to maintain quality of service (QoS) for the duration of the outage. To that end, sufficient capacity must be provided on the links so that the network can survive a set of protected failure scenarios without congestion due to redirected traffic. The self-protecting multipath (SPM) is a protection switching mechanism for which the required backup capacity can be minimized by linear optimization methods. However, unprotected multi-failures may lead to congestion in such "resilient networks" since backup capacity may be missing. In this paper, we quantify and compare the impact of unprotected double failures on the QoS for the optimized SPM, single shortest path routing (SSP), and equal-cost multipath (ECMP) routing.**

I. Introduction

Protection switching methods are used to deviate affected traffic quickly in case of network failures. They are usually embedded in a connection-oriented network architecture. For instance, a primary path may be protected by a disjoint backup path such that if one network element of the primary path fails, the source router can quickly redirect the traffic to the backup paths. The backup paths require backup capacity to carry the deviated traffic in failure cases. In packet-switched networks, several backup paths can share this capacity if they are activated in different failure scenarios. This reduces the required backup capacity and thereby the entire capital expenses for the network. The self-protecting multipath (SPM) [1] is a protection switching algorithm whose structure consists of several disjoint paths from source to destination over which the traffic is distributed according to a load balancing function. If one of the paths fails, the traffic is redistributed over the working paths according to another pre-computed load balancing function.

If the routing and the rerouting of the traffic is known for a set of protected failure scenarios $\mathcal{S}$, links in a network can be provisioned with so much capacity that overload on backup paths due to redirected traffic is avoided. We do that for standard single shortest path (SSP) and equal-cost multipath (ECMP) routing, i.e., their cost metric is based on the hop count. For the SPM, we calculate optimized load balancing functions for the working and the failure scenarios such that the sharing of backup capacities is maximized and that the overall capacity requirements of the network are minimized. Such "resilient networks" provide full protection only against failures considered in $\mathcal{S}$. As SPM networks require substantially less capacity than SSP or ECMP networks, the motivating question for our investigation is: do SPM networks encounter more severe QoS violations than SSP/ECMP networks if unprotected failures occur? Thus, we study the connectivity and the potentially lost traffic of all traffic aggregates due to unprotected multi-failures and contrast them for networks that are dimensioned to protect all single link and router failures with SPM, SSP, or ECMP routing.

The paper is structured as follows. Section II explains the SPM and summarizes the results regarding the backup capacity minimization. Section III analyzes the impact of unplanned double failures on the connectivity and the lost traffic for SPM, SSP, and ECMP routing when the network is provisioned to survive all single failure scenarios without QoS degradation. Finally, we summarize this work and draw our conclusions in Section IV.

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

II. Restoration and Protection Switching

In this section we give a short overview on various resilience mechanisms and summarize results regarding the backup capacity minimization of the SPM.

A. Restoration Mechanisms

Restoration mechanisms take actions only after a network failure. They try to find new routes or set up explicit backup paths when the traffic cannot be forwarded anymore due to link or node failures. The disadvantage of such methods is obvious: they are slow. The re-convergence of the IP routing algorithm is a very simple and robust restoration mechanism [2], [3]. It routes the traffic along least-cost paths which are found by distributed routing algorithms as long as the network is physically connected. The cost of a path is determined by the sum of the virtual costs of its links that are normally set to one (hop count metric). Single shortest path (SSP) routing forwards the traffic only over a single shortest path. If several next hops exist that lead to least cost path to the destination, the one with the lowest node ID is chosen to make the single path deterministic. In contrast, equal-cost multipath (ECMP routing distributes the traffic rate equally to all such next hops and forwards the traffic along a multipath structure.

B. Protection Switching Mechanisms

A good overview on protection switching is given in [4].

1) End-to-End Protection with 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 head end router of a broken primary path to the corresponding backup path. This is called end-to-end (e2e) protection. It is faster than restoration, but the signalling of the failure to the head end router takes time and traffic being already on the way is lost.

2) Fast Reroute Mechanisms: MPLS fast reroute (FRR) tackles the problem of lost traffic in case of e2e protection. Backup paths towards the destination are set up not only at the head end router of the primary path but also at almost every intermediate node of the path [5]. Then, a backup path is immediately available if the path breaks at some location. FRR mechanisms also exist for IP networks. Several solutions are being discussed, but a preferred method is not yet established [6]–[8].

3) Self-Protecting Multipath: The self-protecting multipath (SPM) [1] is a special e2e protection switching mechanism. Its path layout consists of disjoint paths and the traffic is distributed over all of them according to a load balancing function (see Figure 1). If a single path fails, the traffic is redistributed over the remaining working paths according to another load balancing function. Thus, a separate load balancing is required for every pattern of failed and working paths. The path layout for the SPM is calculated preferably by the k-disjoint-shortest-path algorithm [9] to maximize its number of disjoint paths and the load balancing function can be optimized by non-integer linear programs [10].

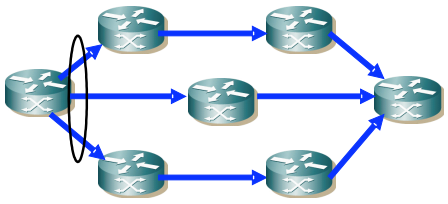


Fig. 1. The SPM distributes the traffic over disjoint paths according to a load balancing function which depends on the pattern of failed and working paths.

C. Routing Optimization for Network Dimensioning

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 to a different required capacity for the links. Using the maximum of the capacities for a link that result from a set of protected failure scenarios $\mathcal{S}$ leads to a 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 a routing or resilience mechanism X in a non-resilient network by $C_X^{\emptyset}$ and $C_X^{\mathcal{S}}$ is the required capacity in a resilient network to protect all failure scenarios in $\mathcal{S}$. As shortest path routing requires the least network capacity to forward the traffic in the failure-free scenario, we take SSP routing as the baseline for our comparison and define the relative required backup capacity by $\frac{C_X^{\mathcal{S}} - C_{SSP}^{\emptyset}}{C_{SSP}^{\emptyset}} \cdot 100\%$. In packet-switched networks, backup resources are shared among different aggregates in different failure scenarios. This backup capacity sharing can intentionally be used to minimize the required backup capacity and, thereby, the overall expenses for the network.

In [10], we optimized the load balancing function of the SPM to reduce the required backup capacity. We studied 240 different random networks constructed according to the algorithm in [11] which allows to rigidly control the network size n, the average node degree δ_{avg}, and the maximum deviation of individual node degrees from that average δ_{dev}^{max}. For the sake of simplicity, we assumed homogenous traffic matrices, i.e., all nodes exchange the same amount of traffic, and dimensioned the network in such a way that it is resilient to all single link and single node failures.

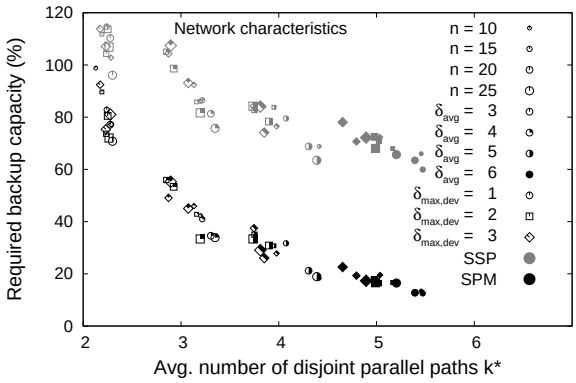


Fig. 2. Backup capacity for 240 random networks with resilience against single link and single node failures.

Figure 2 illustrates the required backup capacity for the 240 random networks that were dimensioned for resilience against all single link and single router failures. We sampled 5 networks for each combination $(n, \delta_{avg}, \delta_{dev}^{max})$ and each point in the figure corresponds to the average values of these 5 networks. The x-axis shows the average number of disjoint paths in the networks and the y-axis shows the required backup capacity. The average number of disjoint parallel paths k^* of a network is strongly correlated with its average node degree δ_{avg} and the figure proves that the required backup capacity can be effectively reduced with an increasing number of parallel paths. In contrast, the network size has no significant impact. In [11] we have shown that SPP routing requires significantly more backup capacity to make the network resilient against the same failures. Therefore, the SPM seems as a promising protection switching approach. However, a critical question remains: are the capacity savings of the SPM compared to SSP routing at the expense of reduced resiliency against unprotected multi-failures?

III. RESULTS

In this section, we assess the impact of double failures on the amount of disconnected and congested aggregates and on the lost traffic by mathematical analysis. We compare these measures in networks using the rerouting of standard SSP, ECMP, and the optimized SPM as resilience mechanism. The networks are dimensioned in such a way that they have enough capacity to carry the traffic to support their traffic matrix in all single link and node failures.

A. Motivation and Test Network

We consider the Labnet03 for our initial studies. Its topology is given in Figure 3 and it is typical for North-American core networks. It comprises $n = 20$ nodes and $m = 53$ 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.

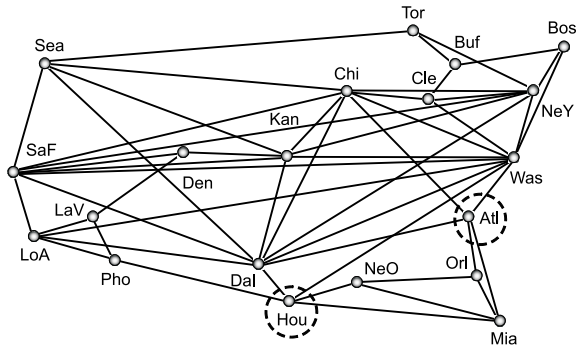


Fig. 3. Topology of the Labnet03: the simultaneous failure of Hou and Atl effects a separation of the network into two disconnected islands.

For a homogeneous traffic matrix, SSP requires 93% backup capacity to protect the network against congestion in all single link and node failures in addition to its required capacity in the failure-free case. For the heterogenous traffic matrix given in [11], SSP needs 87% percent more capacity. The optimized SPM reduces the required backup capacity down to 48% and 39%, respectively. This strong reduction of the backup capacity raises the question for the impact of multi-failures on the percentage of disconnected and congested aggregates as well as the lost traffic for the optimized SPM in comparison to SSP routing.

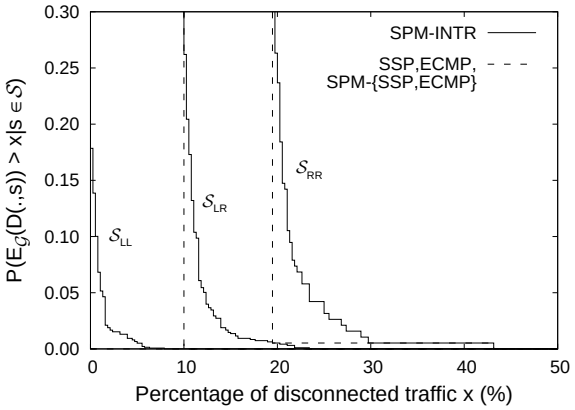
B. Percentage of Disconnected and Congested Aggregates

We study three different sets of double failure scenarios, separately. $\mathcal{S}_{LL}$ contains all double link failures, $\mathcal{S}_{LR}$ contains all simultaneous and independent link and router failures, and $\mathcal{S}_{RR}$ contains all double router failures. Of course, each router failure entails also the failure of its adjacent links. The failure scenario affects the connectivity and the path of each aggregate. An aggregate is disconnected if no path can be found by the routing. The disconnection of an aggregate depends on the special failure scenario s and the routing, but it is independent of the link bandwidths. SSP and ECMP always find a route through the network as long as it is physically connected. In contrast, the SPM uses explicit routes that are not automatically reorganized when they are broken. If the SPM has only two disjoint paths, the failure of an element in each of these paths disconnects the corresponding traffic aggregate. In such a situation, the connectivity is lost until the failure is repaired (SPM-INTR), or it is restored by changing the transport paradigm for this specific aggregate from the connection-oriented SPM to connectionless SSP or ECMP forwarding (SPM-SSP, SPM-ECMP).

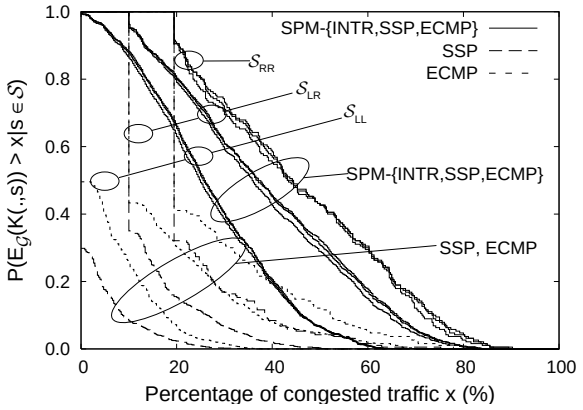
The function $D(g,s)$ yields zero if the aggregate $g \in \mathcal{G}$ is still connected in the failure scenario s, otherwise it yields one. The set $\mathcal{G}$ comprises all traffic aggregates in the network. The traffic rate of a single aggregate $g \in \mathcal{G}$ is given by $c(g)$. We calculate the percentage of the disconnected traffic $E_{\mathcal{G}}(D(.,s)) = \frac{\sum_{g\in\mathcal{G}} c(g)\cdot D(g,s)}{\sum_{g\in\mathcal{G}} c(g)}$ for each failure scenario $s \in \mathcal{S}$ rather than the percentage of the disconnected aggregates. However, this difference is not important in our study since we use homogeneous traffic matrices, i.e., the traffic rate between all border routers is the same. Based on these failure-specific percentages $E_{\mathcal{G}}(D(.,s))$, $s \in \mathcal{S}$, we derive the complementary distribution function (CDF) $P(E_{\mathcal{G}}(D(.,s)) > x | s \in \mathcal{S})$ of the percentage of disconnected traffic under the condition that the failure scenario s belongs to the set $\mathcal{S}$.

Figure 4(a) shows the CDF of the disconnected traffic for SSP, ECMP, and SPM. In case of the double link failures $\mathcal{S}_{LL}$, all aggregates remain connected for SSP and ECMP routing, as well as for SPM-SSP and SPM-ECMP, which leads to a straight vertical dashed line at $x = 0$. For the link and router failures $\mathcal{S}_{LR}$, the aggregates starting or ending at the failed router are disconnected, i.e., exactly $(n-1)\cdot(n-2)$ out of $n\cdot(n-1)$ aggregates remain connected for every $s \in \mathcal{S}_{LR}$. Therefore, we observe a straight vertical line at $\frac{380-342}{380} = 0.1$. When two routers fail ($\mathcal{S}_{RR}$), at most $(n-2)\cdot(n-3)$ out of $n\cdot(n-1)$ aggregates remain connected for every $s \in \mathcal{S}_{RR}$. 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 $|\mathcal{S}_{RR}| = 190$ yields a very low probability for the outage of such a large amount of traffic. We also performed this experiment with the heterogeneous traffic matrix from [11], but we only present the results for the homogeneous one since they are easier to understand. As mentioned before, the SPM leads more easily to disconnection than SSP or ECMP, and as a consequence, we introduced the variants SPM-INTR, SPM-SSP, and SPM-ECMP. The latter two lead to the same connectivity as SSP. Figure 4(a) shows that SPM-INTR leads to at most 12% more disconnected traffic compared to SSP for $\mathcal{S}_{LL}$, $\mathcal{S}_{LR}$, and $\mathcal{S}_{RR}$. However, in more than 95% of the considered failure scenarios, SPM disconnects only at most 2% more traffic than SSP or ECMP routing.

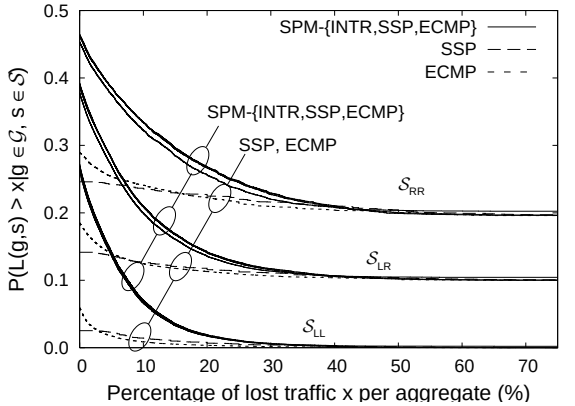
In case of a failure, traffic is redirected and may lead to congestion on backup paths if capacity is missing. If there



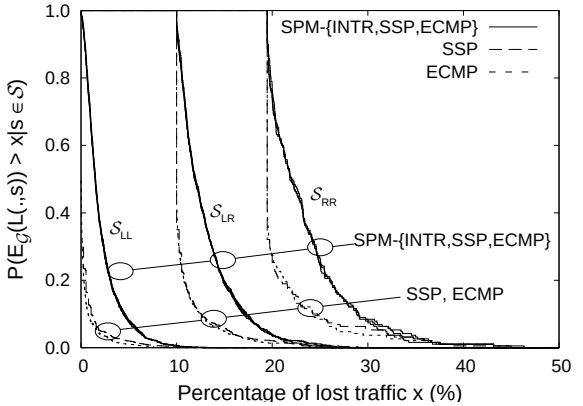
(a) Complementary distribution function of the percentage of disconnected traffic.



(b) Complementary distribution function of the percentage of congested traffic.



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



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

Fig. 4. Impact of double failures on the disconnection, congestion, and traffic loss for SSP, ECMP, and SPM-variants in the Labnet03 network.

is enough capacity, the function $K(g,s)$ yields 0, otherwise it yields 1. The x-axis of Figure 4(b) presents the percentage of the traffic that suffers from disconnection or congestion. The minimum of these values is limited by the disconnected traffic. Depending on the type of double failures, up to 30%, 50%, or 65% of the aggregates may be affected for SSP. ECMP uses more links than SSP and leads, therefore, to some more congested traffic. The SPM is more sensitive to double failures than SSP and ECMP in the sense that up to 65%, 80%, or 85% of the traffic suffers from connection loss or congestion. The three variants SPM-INTR, SPM-SSP, and SPM-ECMP yield very similar results. SPM-INTR has the least affected traffic because the disconnection of an aggregate affects only a single aggregate while the redirection might congest all aggregates on its backup path. Analogously to ECMP and SSP, SPM-ECMP leads to slightly more congestion than SPM-SSP.

C. Lost Traffic

We calculate for each aggregate $g \in \mathcal{G}$ and each considered failure scenario $s \in \mathcal{S}$ an upper bound $L(g,s)$ of the traffic that is lost due to disconnection or congestion. It is based on the percentage of missing capacity on the paths in multi-failure scenarios. Figure 4(c) shows the corresponding CDF $P(L(g,s) > x | g \in \mathcal{G}, s \in \mathcal{S})$, i.e., it shows the CDF of the percentage of lost traffic of *individual* aggregates in special failure scenarios. Again, we differentiate the three different sets of double failures $\mathcal{S}_{LL}$, $\mathcal{S}_{LR}$, and $\mathcal{S}_{RR}$. The percentage of disconnected aggregates in Figure 4(a) is a lower bound for the corresponding CDFs in Figure 4(c) because the disconnection of an aggregate leads to 100% traffic loss. Traffic redirection by SSP causes up to 25%–35% additional traffic loss but only in very rare cases. The SPM leads to a larger number of congested aggregates than SSP (cf. Figure 4(b)), but Figure 4(c) shows that the traffic loss is mostly rather small (<30%) if congestion occurs.

Figure 4(d) shows the CDF of the percentage $E_{\mathcal{G}}(L(.,s))$ of the overall lost traffic for a special failure scenario s which is averaged over all aggregates $g \in \mathcal{G}$ while Figure 4(c) shows the lost traffic of individual aggregates. The most probable average traffic loss of SSP, ECMP, and SPM ranges between 0–10%, 10–25%, and 19–43% depending on the considered sets of failure scenario $\mathcal{S}_{LL}$, $\mathcal{S}_{LR}$, or $\mathcal{S}_{RR}$, respectively. The important finding is that the lost traffic for SPM does not exceed the one

for SSP by far. The mean values averaged over all scenarios within a specific set of double failure scenarios are given in Table I. For SPM about 2% more traffic is lost in $\mathcal{S}_{LL}$, $\mathcal{S}_{LR}$, or $\mathcal{S}_{RR}$ than for SSP or ECMP routing.

TABLE I
LOST TRAFFIC DUE TO DOUBLE FAILURES IN %.

failure set	SSP	ECMP	SPM-INTR	SPM-SSP	SPM-ECMP
$\mathcal{S}_{LL}$	0.436	0.315	2.089	2.059	2.021
$\mathcal{S}_{LR}$	10.890	10.807	12.966	13.018	12.968
$\mathcal{S}_{RR}$	21.035	20.965	23.321	23.426	23.356
$\mathcal{S}_{all}$	0.508	0.388	2.164	2.134	2.096

D. Overall Impact of Double Failures

Link failures occur with a probability in the order of 10^{-4} while router failures occur with a probability in the order of 10^{-6} [12]. If we consider all double failure scenarios $\mathcal{S}_{all} = \mathcal{S}_{LL} \cup \mathcal{S}_{LR} \cup \mathcal{S}_{RR}$ weighted by their probabilities, the impact of the double link failures dominates. As a consequence, the performance curves for $\mathcal{S}_{all}$ hardly differ from $\mathcal{S}_{LL}$. This is also visible in Table I where the average loss for $\mathcal{S}_{all}$ is very similar to the one for $\mathcal{S}_{LL}$.

After all, double failures may lead to disconnection of aggregates. If the physical connectivity is not compromised by the failure, SSP and ECMP routing always retains the connectivity while the SPM can lose connection, but this happens only in rare scenarios. Then, forwarding the traffic of the affected aggregate according to SSP or ECMP (SPM-SSP, SPM-ECMP) solves the problem. Double failures lead to congested links. This affects aggregates more often for SPM than for SSP or ECMP for two reasons. In networks with SPM, aggregates have more links within their paths than in networks with SSP and networks dimensioned for the optimized SPM have less backup capacity than networks dimensioned for standard SSP or ECMP routing.

However, the average traffic loss for double failures is very low (0.5%–2%) for SSP, ECMP, and for SPM. Considering the fact that double failures occur with a probability of $\binom{53}{2} \cdot 10^{-4} \cdot 10^{-4} + \binom{53}{1} \cdot \binom{20}{1} \cdot 10^{-4} \cdot 10^{-6} + \binom{20}{2} \cdot 10^{-6} \cdot 10^{-6} = 1.39 \cdot 10^{-5}$, this leads to a traffic loss of $2.78 \cdot 10^{-5}$%. Single router failures occur with a probability of $\binom{20}{1} \cdot 10^{-6}$ and lead to the loss of 10% of the traffic, thus, an overall traffic loss of $2 \cdot 10^{-4}$% is observed. This value can be improved only by more reliable exchange points and possibly redundant exchange structures. However, as long as nodes have an unavailability of 10^{-6} or higher, the slightly increased traffic loss of SPM vs. SSP is irrelevant.

E. Capacity Requirements to Protect Double Failures

At first sight, the values for the traffic loss in Table I suggest that only very little additional capacity is required to make the network resilient against congestion due to double failures, too. We calculate the required capacity for the Labnet03 network and for a homogeneous traffic matrix for different sets of protected failure scenarios: no protected failures, single link or node failures ($\mathcal{S}_L, \mathcal{S}_R$), single link or node failures and double link failures ($\mathcal{S}_L, \mathcal{S}_R, \mathcal{S}_{LL}$), and all single and double element failures ($\mathcal{S}_L, \mathcal{S}_R, \mathcal{S}_{LL}, \mathcal{S}_{LR}, \mathcal{S}_{RR}$). Table II shows that double link failures increase the capacity requirements by another 90% for SSP, 66% for ECMP, and by 55%, 71%, and 67% for the SPM variants compared to single element failures. Taking all single and double element failures into account, this leads to 145% more capacity for SSP, 130% more capacity for ECMP, and 69%, 124%, and 120% more capacity for the SPM variants. This very large increase is due to the fact that in many double failure scenarios only little or no traffic is lost, but in a very few ones up to 95% of the traffic is lost. The probability of these scenarios is so small that it is not visible in Figure 4(c). The table shows that it is less costly to upgrade SPM networks from single-failure resilience to double failure resilience than for SSP or ECMP networks. Note that the SPM was not re-optimized for the increased sets of protected failure scenarios which reveals potential to further reduce the required capacity. Rerouting traffic according to SSP or ECMP when SPM has lost connection leads also to a significant increase of required capacity (SPM-INTR vs. SPM-SSP, SPM-ECMP). Traffic distribution by ECMP compared to SSP decreases the capacity requirements. This holds both for mere SSP/ECMP routing as well as for SPM-SSP/SPM-ECMP.

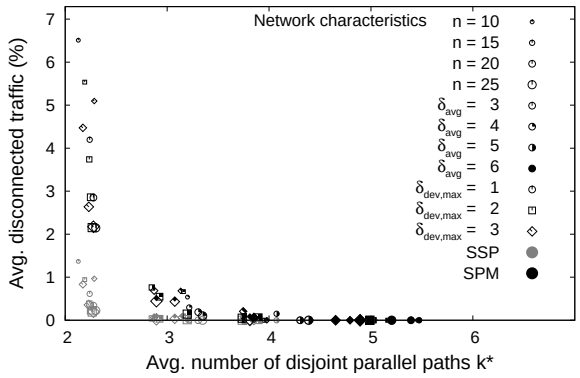
TABLE II
REQUIRED NETWORK RESOURCES IN CAPACITY UNITS AND RELATIVE REQUIRED BACKUP CAPACITY IN % FOR THE RESILIENCE AGAINST DIFFERENT PROTECTED FAILURE SETS.

sets of protected failures	SSP	ECMP	SPM-INTR	SPM-SSP	SPM-ECMP
without resilience	816.00	816.00	822.00	822.00	822.00
$\mathcal{S}_L, \mathcal{S}_R$	1578.00	1447.36	1215.18	1215.18	1215.18
	93%	77%	48%	48%	48%
$\mathcal{S}_L, \mathcal{S}_R, \mathcal{S}_{LL}$	2313.00	1986.54	1649.63	1793.18	1752.96
	183%	143%	103%	119%	115%
$\mathcal{S}_L, \mathcal{S}_R, \mathcal{S}_{LL}, \mathcal{S}_{LR}, \mathcal{S}_{RR}$	2757.00	2503.00	1772.57	2222.71	2189.33
	238%	207%	117%	172%	168%

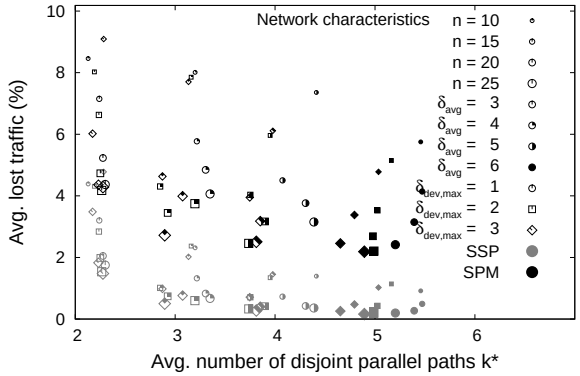
F. Disconnection and Traffic Loss in Random Networks

We evaluate the percentage of the disconnected traffic and of the lost traffic due to disconnection and congestion in the presence of double failures. We use the same random networks as in Figure 2 for our evaluation. Figure 5(a) shows that only networks with an average node degree of $\delta_{avg} = 3$ suffer from a severe disconnection. The disconnection is significantly larger in networks with SPM than in networks with SSP or ECMP and larger networks lead to less disconnected traffic. The percentage of disconnected traffic decreases clearly with the average number of disjoint parallel paths k^* per aggregate and is almost zero for networks with $\delta_{avg} = 4$.

Figure 5(b) shows the percentage of lost traffic. It is visibly larger than the disconnected traffic. Small networks tend to have more traffic loss than large ones and we see a clear decrease of the traffic loss with an increasing average number of disjoint parallel path k^* in the network. Again, the SPM causes more traffic loss than SSP, but this difference decreases with increasing network size.



(a) Percentage of disconnected traffic.



(b) Percentage of lost traffic due to disconnection and congestion.

Fig. 5. Performance measures for randomly constructed networks in the presence of unprotected double failures.

IV. Conclusion

The self-protecting multipath (SPM) is an e2e protection switching mechanism which reacts faster than restoration mechanisms based on the shortest path principle, e.g. single shortest path (SSP) or equal-cost multipath (ECMP) routing. When the network topology and the traffic matrix are given, the structure of the SPM can be efficiently optimized such that the required network capacity is minimized and no traffic is lost due to congestion for a set of protected failure scenarios $\mathcal{S}$. In well connected networks, SPM requires only 15–50% additional backup capacity to protect all single link and node failures while SSP or ECMP need 45–90% backup capacity. Failures that have not been considered in the capacity provisioning of the "resilient" network may lead to congestion and the motivating question for this work was: are the capacity savings of the SPM compared to SSP or ECMP at the expense of reduced resiliency against unprotected multi-failures?

Our studies in the Labnet03 network revealed that unprotected double failures lead on average to 2% more traffic loss in resilient SPM networks than in resilient SSP or ECMP networks. This holds for double link failures, double router failures and independent link and router failures. Taking into account unavailability values of 10^{-4} for links and 10^{-6} for routers, double link failures dominate other double failures such that SSP loses about 0.5% of the traffic while SPM loses about 2.2% of the traffic in the presence of double failures. Traffic loss occurs not only due to unprotected double failures but also due to disconnection of traffic by single router failures. This loss amounts to $2 \cdot 10^{-4}$% in the considered network example. In contrast, the lost traffic due to double failures is between $0.35 \cdot 10^{-5}$% and $1.39 \cdot 10^{-5}$%. Thus, the difference regarding the lost traffic between the SPM and SSP/ECMP is irrelevant as long as the reliability of the routers is not increased.

At first sight, 2% lost traffic suggests that about 2% more capacity is sufficient to improve the resiliency. However, we showed for our example network that the SPM requires 47% more capacity to avoid congestion due to double failures and SSP needs even another 75% more capacity. Thus, resiliency for double failures is expensive, and it is even more expensive for SSP than for SPM.

We considered the lost traffic due to disconnection and congestion due to double failures also in random networks and found out that the traffic in networks with an average node degree of $\delta_{avg} = 3$ or more suffers only little from disconnection, and that congestion in the presence of double failures is lower in well connected networks. We also observed that less traffic is lost in large networks than in small networks as the proportion of the traffic affected by the failure is smaller.

After all, networks dimensioned for the optimized SPM have only a slightly reduced resilience against unprotected double failures than networks dimensioned for hop count based SSP or ECMP routing, and SPM networks can be upgraded with less capacity to be resilient against congestion due to double failures.

References

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

[2] 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.

[3] 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.

[4] 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.

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

[6] M. Menth and R. Martin, "Network Resilience through Multi-Topology Routing," in *5th International Workshop on Design of Reliable Communication Networks (DRCN)*, Island of Ischia (Naples), Italy, Oct. 2005.

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

[8] A. Atlas and A. Zinin, "Basic Specification for IP Fast-Reroute: Loop-Free Alternates," http://www.ietf.org/internet-drafts/draft-ietf-rtgwg-ipfrr-spec-base-05.txt, July 2005.

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

[10] 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.

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

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