Self-Protecting Multipaths (SPM): Efficient Resilience for Transport Networks

Michael Menth

University of Würzburg, Institute of Computer Science, Germany
menth@informatik.uni-wuerzburg.de

Abstract. The self-protecting multipath (SPM) is a simple and efficient end-to-end protection switching mechanism for transport networks. It distributes the traffic of a demand between two nodes according to a specific load balancing function over several disjoint paths and redistributes it if one of them fails. The load balancing functions can be optimized so that backup capacity in the network is optimally shared by multiple demands in various failure scenarios. As a result, resilience against all link and node failures can be achieved with only little extra capacity and in capacitated networks more protected traffic can be carried with the SPM than with other resilience mechanisms. The SPM is rather simple which facilitates its deployment in practice. This chapter explains the SPM in detail, distinguishes it from other, similar mechanisms, shows how the load balancing functions can be optimized, and illustrates the superior performance of the SPM.

1 Structure and Operation

The self-protecting multipath (SPM) has been first published in [1]. It carries a traffic demand d between two routers in a network and protects the transmission against network failures. The path layout $\mathbf{P_d} = (\mathbf{p_d^0}, ..., \mathbf{p_d^{k_d-1}})$ of the SPM for a demand d consists of k_d disjoint parallel paths $\mathbf{p_d^i}$ that are explicitly established between two routers as depicted in Figure 1. The traffic is distributed over them according to a load balancing function $\mathbf{l_d^f}$ that indicates the traffic fraction that should be carried over each of them. If paths fail, the source node sees a pattern $\mathbf{f_d}$ of failed and working paths in the SPM for demand d and redistributes the traffic over the working paths according to another SPM-specific load balancing function $\mathbf{l_d^f}$ that depends on the observed failure pattern $\mathbf{f_d}$. Thus, the SPM redistributes traffic only when one of its partial paths is affected by a network failure. To detect a failure pattern $\mathbf{f_d}$, the source node must check whether each partial path within a SPM is working. This also includes partial paths that do not carry any traffic. They act as sensors in the network, give feedback about the network health, and can also trigger traffic shifts if they fail.

When the traffic matrix and the link capacities are given for a network, the routing and the load balancing functions of the SPM can be configured in an optimized way so that link utilizations are low under normal conditions and in failure scenarios. This

This work was funded by Siemens AG, Munich, and by the Deutsche Forschungsgemeinschaft (DFG) under grant TR257/18-2. The authors alone are responsible for the content.

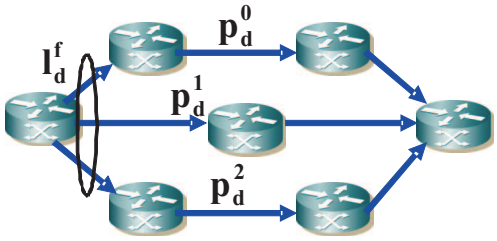


Fig. 1. The SPM distributes the traffic of a demand d over k_d disjoint paths $\mathbf{P_d} = (\mathbf{p_d^0}, ..., \mathbf{p_d^{k_d-1}})$ according to a load balancing function $\mathbf{l_d^f}$ which depends on the pattern $\mathbf{f_d}$ of failed and working paths.

requires that the transmission capacity of the links can be shared by different paths. Similarly, joint capacity provisioning and SPM configuration can minimize the required backup capacity in networks where links still need to be provisioned with capacity. To quantify and compare "backup efficiency", we use the maximum link utilization in capacitated networks and the required backup capacity normalized by the primary capacity in uncapacitated networks.

The SPM can be implemented by any connection-oriented communication technology that allows to establish disjoint partial paths. Backup efficiency can be realized only when transmission capacity can be shared among different paths. Multiprotocol Label Switching (MPLS) technology has has theses features. Therefore, it is interesting to implement the SPM in MPLS. The disjoint paths can be set up as label switched paths (LSPs) between a pair of routers, and the head-end router distributes the traffic over these LSPs according to a load balancing function $\mathbf{l_d^f}$. As an alternative, the SPM may also be implemented in Carrier Ethernet technology.

1.1 Basic SPM

The basic SPM uses load balancing functions $\mathbf{l_d^f}$ that partition traffic rates arbitrarily. However, this cannot be easily achieved in practice. Packets of a single flow should be forwarded over the same interface to avoid out-of-order delivery at the destination. Therefore, simple packet-based round-robin mechanisms or extensions of them cannot be used. Instead, hash-based load balancing algorithms guarantee that packets of the same flow are forwarded over the same interface [2]. These algorithms achieve a desired split ratio only in the long run with possibly significant deviations at particular instances. Therefore, it is rather hard to realize a desired traffic distribution with sufficient accuracy on a short time scale.

1.2 Integer SPM (iSPM)

The integer SPM (iSPM) constrains the load balancing function $\mathbf{l_d^f}$ to values 0 and 1, i.e., the traffic between two routers is carried only over a single partial path. Hence, the load balancing function $\mathbf{l_d^f}$ becomes a path selection function. In contrast to the basic

SPM, the iSPM does not need complex load balancing algorithms. Nevertheless, the iSPM has about the same backup efficiency as the basic SPM, especially in networks with a small or moderate node degree [3].

1.3 Failure-Specific SPM (fSPM)

The failure-specific SPM (fSPM) is another obvious extension of the basic SPM. Its source node uses a load balancing function that requires the knowledge of failed elements on the paths instead of the failure pattern $\mathbf{f_d}$ only. Thus, the source node requires a different load balancing function for every possible combination of link and node failures that affects the multipath structure of the SPM and relies on the fact that this information can be quickly provided to the source node under failure conditions. Hence, the fSPM is significantly more complex than the basic SPM or the iSPM. However, the fSPM can hardly increase the backup efficiency of the basic SPM [4].

2 Comparison with Other Resilience Mechanisms

We compare the SPM with various other resilience mechanisms that are applicable in similar environments as the SPM or that have a similar structure [5].

2.1 Resilience Mechanisms for Similar Environments

The SPM is a resilience mechanism for packet-switched communication networks that allow capacity sharing among arbitrary flows on their links. We give a brief overview of some other mechanisms that are applicable for the same environment.

IP Routing and Rerouting In intra-domain IP networks, routing follows the least-cost paths according to administrative link costs. They are the shortest paths with respect to this cost metric. The hop count metric sets all link costs to 1 and leads to the shortest paths in terms of hop count. In case of a failure, distributed routing algorithms find the next shortest paths and connectivity is restored after some time (in the order of seconds). Thus, restoration is used, i.e., backup paths are not established a priori but only when needed. The SPM is intended to react clearly faster (in the order of 100 ms), and its failover time depends mainly on the failure detection time.

Several least-cost paths possibly exist for a source and destination pair. Single shortest path (SSP) routing chooses just one of them for data forwarding while equal-cost multipath (ECMP) routing splits traffic equally over all interfaces that are part of a shortest path to the destination. Equal-cost paths are not necessarily disjoint, but may consist of partial paths that fork and join several times.

The path layout of IP routing can be controlled only indirectly by assigning appropriate link costs to links. Modifying the cost of a single link possibly changes layout of paths between several source and destination pairs. Given the topology, the link capacities, and the traffic matrix of a network, the link costs can be optimized so that the maximum utilization of all links in the network is minimized both under failure-free conditions [6] and for a limited set of failure scenarios [7, 8]. Optimization can also be performed using other objective functions besides the maximum link utilization [9].

End-to-End Protection Using Explicit Primary and Backup Paths In connection-oriented networks, a disjoint backup path can protect the transmission of traffic on a primary path. This is called end-to-end protection. The disjoint primary and backup paths are established at the time of the connection setup. The source node detects whether the primary path fails and then switches the traffic from the primary to the backup path. This principle called protection switching requires that a failure on the primary path is detected and reported to the head-end node, and works quite fast. End-to-end protection is a wide-spread principle and is applied, e.g., in MPLS networks.

The SPM also implements end-to-end protection. However, its partial paths are not explicit primary and backup paths. They are rather equal since all of them can basically carry traffic in failure-free and in failure scenarios which is determined by the load balancing function. Moreover, the primary/backup path concept deviates traffic from the primary path to the backup path only when the primary path fails while the SPM may also redirect traffic when one of its paths fails that does not carry any traffic. The primary/backup path mechanism can be optimized by choosing an appropriate layout for the primary and backup paths. The SPM has additional degrees of freedom: the path layout for multiple paths and the load balancing functions for different failure patterns can be chosen. This makes the SPM more flexible than the mere primary/backup path concept.

MPLS Fast Reroute MPLS fast reroute (MPLS-FRR) provides faster protection in MPLS networks than end-to-end protection [10]. FRR techniques in general achieve fast protection since nodes detecting a failure immediately switch traffic to backup paths instead of notifying the source node. This requires backup paths starting at every node along an LSP. Two options exist: facility backup [11] and one-to-one backup [12]. Facility backup installs local bypass LSPs around links and nodes to implement link and node protection. One-to-one backup is LSP-oriented and installs detour LSPs starting at every node of an LSP and ending at its tail-end router. To reduce the number of connection states in the routers, the detour LSPs can be merged at some merge point when they share the same downstream paths.

IP Fast Reroute The end-to-end protection and MPLS-FRR techniques are based on the connection concept. Therefore, they are not applicable in connectionless IP networks. To achieve faster protection than IP restoration, IP fast reroute (IP-FRR) provides local backup paths [13]. If a next hop fails in an IP network, loop-free alternates (LFAs) [14, 15] deviate traffic to alternative neighbor nodes that can route the traffic to the destination without using the failed node. Such alternative nodes do not always exist and, thus, LFAs cannot achieve protection of all link or node failures. In the not-via mechanism [16], a special address is used to tunnel a packet that encounters a next-hop failure on its path and guides it to the next-next-hop where the packet is decapsulated. As a result, the backup path layout of not-via addresses is similar to the facility backup option for node protection in MPLS-FRR. More approaches exist [17–19], but they are currently not being standardized so that it is not likely to see them deployed in the near future.

Other Mechanisms The authors of [20] propose a set of optimum primary and backup paths. Their assumption is that any node is informed about failed elements in the network and can activate failure-specific backup paths that do not need to be disjoint. This is quite complex since it requires fast dissemination of exact failure information through the network during outages and source nodes possibly need to switch traffic although none of its paths has failed. In contrast, the SPM switches its traffic to other partial paths only if its source node detects that at least one of its partial paths is broken. Segment protection [21] protects subpaths by backup paths and presents thereby a hybrid between link protection and end-to-end protection.

2.2 Resilience Mechanisms with Similar Structures

There are various other mechanisms for resilience and traffic engineering that take advantage of explicit multipath structures [5]. To avoid confusion with them, we present them and explain differences to the SPM.

Demand-Wise Shared Protection Demand-wise shared protection (DSP) is a survivability concept initially proposed in [22] for optical networks. A demand is the entirety of flows between two nodes. Bandwidth for a specific demand is reserved on several paths in the network. It is dedicated to particular flows and part of it is reserved for backup purposes. If one of the paths fails, the flows are redirected over other paths belonging to the same demand. The backup bandwidth is shared only among the flows of the same demand. In contrast, the SPM takes advantage of capacity sharing among flows with different source or destination nodes.

Protection Cycles Protection cycles (p-cycles) [23] have been originally proposed for ring-based optical networks where the transmission direction can be reconfigured within milliseconds. Thus, they are suitable for physical layer protection scheme, e.g., WDM or SONET networks, but they can also be adapted to be used in other technologies.

Figure 2 explains the idea of p-cycles. If an on-cycle link fails, protection is achieved by operating the cycle in the opposite direction. If a straddling link or path fails, its traffic can be rerouted over both parts of the cycle. Hence, p-cycles provide local protection. This requires fast signalling so that backup resources can be signalled on demand. Backup resources are not dedicated to specific connections in advance. Therefore, backup capacity sharing among different connections is possible. The p-cycles can be configured so that protection with only little backup capacity can be achieved. While p-cycles require cycle-oriented resource management, the SPM does not need to follow such rules.

TeXCP TeXCP [24] is rather a dynamic traffic engineering mechanism than a protection mechanism. It distributes traffic over a multipath structure consisting of single paths between source and destination. A load balancing algorithm adjusts the traffic distribution over the paths according to feedback from probes sent along the paths. The objective of this method is to minimize the maximum link utilization in the network. The

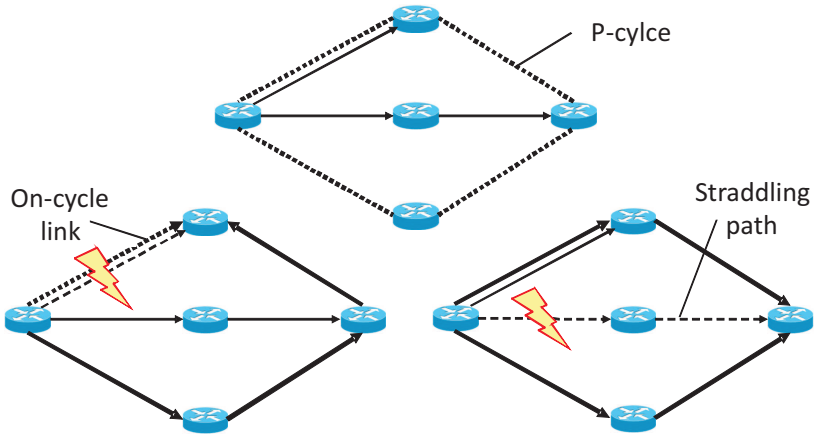


Fig. 2. Protection by p-cycles for on-cycle links and straddling paths.

multipath structure consists of not necessarily disjoint paths and can be implemented, e.g., by MPLS. In contrast, the SPM has pre-configured load balancing functions and can redistribute traffic quickly in case of a failure.

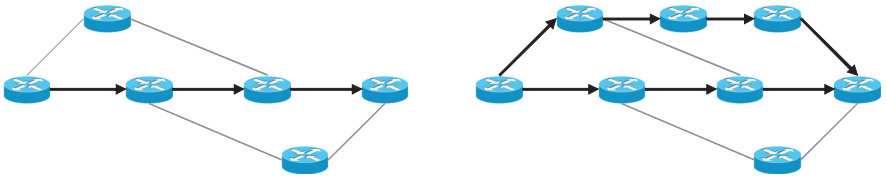
3 Optimized Configuration of the SPM

The optimization of a resilience mechanism improves its configuration so that it works well for a limited set of protected failure scenarios $\mathcal{S}$, e.g. all single link and node failures. There are various optimization goals. For capacitated networks, the maximum utilization of all links in all protected failure scenarios $\mathcal{S}$ should be minimized for a given traffic matrix and link capacities. For network planning, when links are not yet provisioned, the overall link capacities required to carry the traffic under failure-free conditions and in all protected failure scenarios should be minimized. The overall link capacity is just one example and other objectives like installation costs can be of more interest.

The configuration of the SPM comprises both the path layout and the load balancing functions that depend on the pattern of failed and working paths. Their joint optimization is possible, but it is computationally not feasible for medium-size or large networks. Therefore, we present a linear program for the optimization of the load balancing functions which can be applied if the path layout of the SPM is already given. We first explain how an appropriate path layout can be obtained for an SPM, then formalize the structure of the SPM, and eventually explain how the load balancing functions for the basic SPM can be optimized for various objectives using linear programs. The section closes with some remarks about optimization of iSPM and fSPM.

3.1 Path Layout

The SPM consists of disjoint paths so that the remaining paths are still working if a single path fails due to the failure of a single network element. A very intuitive method to find link- or node-disjoint paths in a network is based on the shortest path algorithm. The disjoint paths are obtained iteratively: once a shortest path between a pair of nodes is found, its links and interior nodes are removed from the topology. When no additional path can be found, the algorithm stops. This simple approach cannot always find disjoint paths (see Figure 3(a)) although a disjoint paths solution exist, or it may not always find the shortest disjoint paths (see Figure 3(b)). Therefore, disjoint-shortest paths algorithms should be used. A good overview can be found in Bhandari's book [25]. The k-disjoint shortest paths algorithm finds up to k shortest paths if so many are available in the network. Setting k to a smaller value yields fewer disjoint shortest paths with possibly shorter path lengths.



(a) A disjoint path cannot be found.

(b) The length of the shortest disjoint paths is increased.

Fig. 3. Impact of the wrong selection of the first shortest path.

3.2 Modelling SPMs for Linear Programs

We formulate linear programs for the optimization of the load balancing functions. To that end, we present some general notation and conventions for the description of network concepts, failure scenarios, and load balancing functions.

General Notation Let $\mathbb{X}$ be a set of elements, then $\mathbb{X}^n$ is the set of all n-dimensional vectors and $\mathbb{X}^{n\times m}$ is the set of all $n \times m$-matrices with components taken from $\mathbb{X}$. Vectors $\mathbf{x} \in \mathbb{X}^n$ and matrices $\mathbf{X} \in \mathbb{X}^{n\times m}$ are written bold and their components are written as

$$\mathbf{x} = \begin{pmatrix} x_0 \\ \vdots \\ x_{n-1} \end{pmatrix} \text{ and } \mathbf{X} = \begin{pmatrix} x_{0,0} & \cdots & x_{0,m-1} \\ \vdots & & \vdots \\ x_{n-1,0} & \cdots & x_{n-1,m-1} \end{pmatrix}.$$

The scalar multiplication $c\cdot\mathbf{v}$ and the transpose operator $^\top$ are defined as usual. The scalar product of two n-dimensional vectors $\mathbf{u}$ and $\mathbf{v}$ is written with the help of matrix multiplication $\mathbf{u}^\top\mathbf{v} = \sum_{i=0}^{n-1} u_i \cdot v_i$. Binary operators $\circ \in \{+, -, \cdot\}$ are applied

component-wise, i.e., $\mathbf{u} \circ \mathbf{v} = (u_0 \circ v_0, \ldots, u_{n-1} \circ v_{n-1})^\top$. The same holds for relational operators $\circ \in \{<, \leq, =, \geq, >\}$, i.e. $\mathbf{u} \circ \mathbf{v}$ is true if $\forall\ 0 \leq i < n\colon u_i \circ v_i$ holds. For simplicity reasons we define special vectors $\mathbf{0} = (0, \ldots, 0)^\top$ and $\mathbf{1} = (1, \ldots, 1)^\top$ with context-specific dimensions.

Network Concepts A network $\mathcal{N} = (\mathcal{V}, \mathcal{E})$ consists of $n = |\mathcal{V}|$ nodes and $m = |\mathcal{E}|$ unidirectional links. The links are numbered $0 \leq i < m$ and represented as unit vectors $\mathbf{e_i} \in \{0,1\}^m$, i.e., $(e_i)_j = 1$ if $i = j$, and $(e_i)_j = 0$ if $i \neq j$ with $0 \leq j < m$. We denote the traffic aggregate between routers $\mathbf{v_i} \in \mathcal{V}$ and $\mathbf{v_j} \in \mathcal{V}$ by the demand $d = (i, j)$ and the set of all demands by $\mathcal{D} = \{d = (i, j) : 0 \leq i, j < n \text{ and } i \neq j\}$. The traffic rate associated with each demand $d \in \mathcal{D}$ is $c(d)$ and is given by the traffic matrix.

A single path $\mathbf{p}$ between two distinct nodes is a set of contiguous links represented by a link vector $\mathbf{p} \in \{0,1\}^m$. The path layout of an SPM for demand d is a multipath $\mathbf{P_d}$ that consists of k_d single paths $\mathbf{p_d^i}$ for $0 \leq i < k_d$. They are link- and possibly also node-disjoint except for their source and destination nodes. The multipath is represented by a vector of single paths $\mathbf{P_d} = (\mathbf{p_d^0}, ..., \mathbf{p_d^{k_d-1}})$. Thus, a multipath is described by a matrix $\mathbf{P_d} \in \{0,1\}^{m \times k_d}$.

Failure Scenarios A failure scenario s is given by a set of failed links and nodes. The set of protected scenarios $\mathcal{S}$ contains all outage cases for which the SPM should protect the traffic from being lost and also the failure-free scenario $\emptyset$. The failure indication function $\phi(\mathbf{p}, s)$ yields 1 if a path $\mathbf{p}$ is affected by a failure scenario s; otherwise, it yields 0. The failure pattern of a multipath $\mathbf{P_d}$ is the vector $\mathbf{f_d(s)} = \Big(\phi(\mathbf{p_d^0}, \mathbf{s}), ..., \phi(\mathbf{p_d^{k_d-1}}, \mathbf{s})\Big)^\top$ and indicates the failed single paths in failure scenario s. Thus, with a failure pattern of $\mathbf{f_d} = \mathbf{0}$, all paths are working while for $\mathbf{f_d} = \mathbf{1}$ connectivity cannot be maintained by the SPM.

Normally, all demands $d \in \mathcal{D}$ are active. If routers fail, some demands disappear which leads to a traffic reduction that is expressed by the failure scenario specific set of aggregates $\mathcal{D}_s$.

- *No Traffic Reduction (NTR):* We assume hypothetically that failed routers lose only their transport capability for transit flows but they are still able to generate or receive traffic. Therefore, we have $\mathcal{D}_s = \mathcal{D}$.
- *Source Traffic Reduction (STR):* If a certain router fails, all demands with this source node disappear.
- *Full Traffic Reduction (FTR):* We assume that demands with failed source *or* destination are stalled.

Load Balancing Functions For each demand $d \in \mathcal{D}$ there is one SPM, and each SPM has a load balancing function to distribute the traffic of its demand d over its k_d disjoint paths. If certain paths fail, which is indicated by the failure pattern $\mathbf{f_d(s)}$, the load balancing function shifts the traffic to the remaining working paths. Thus, the SPM needs a load balancing function $\mathbf{l_d^f}$ for each failure pattern $\mathbf{f_d} \in \{0,1\}^{k_d}$. It should be optimized for all failure patterns $\mathcal{F}_d^{\mathcal{S}} = \{\mathbf{f_d(s)} : s \in \mathcal{S}\}$ that occur in the protected failure

scenarios $s \in \mathcal{S}$. Since the load balancing function $\mathbf{l_d^f} \in (\mathbb{R}_0^+)^{k_d}$ describes a distribution, it must obey

$$\mathbf{1}^\top \mathbf{l_d^f} = 1. \tag{1}$$

Furthermore, failed paths must not be used, i.e.

$$\mathbf{f_d}^\top \mathbf{l_d^f} = 0. \tag{2}$$

3.3 Optimization of Load Balancing Functions for Capacitated Networks

We present a linear program to optimize the load balancing functions for all SPMs in a network so that the maximum utilization ρ_{max} of all links in all protected failure scenarios $s \in \mathcal{S}$ is minimized [26]. The assumption is that all link capacities and the traffic matrix are given and that the path layout $\mathbf{P_d}, d \in \mathcal{D}$ is also provided for all SPMs.

The bandwidths are denoted by a vector $\mathbf{b} \in (\mathbb{R}_0^+)^m$ which carries a capacity value for each link. Similarly, the vector indicating the traffic rates on all links, which are induced by a specific SPM $\mathbf{P_d}$, a load balancing function $\mathbf{l_d^f}$, and a specific failure pattern $\mathbf{f} \in \mathcal{F}_d^{\mathcal{S}}$, is calculated by $\mathbf{P_d} \cdot \mathbf{l_d^f} \cdot c(d)$.

In packet switched networks, resources are not physically bound to traffic aggregates. If traffic is rerouted due to an outage, the released resources can be immediately reused for the transport of other traffic. Under this assumption, the capacity constraints are

$$\forall s \in \mathcal{S} : \sum_{d \in \mathcal{D}_s} \mathbf{P_d} \cdot \mathbf{l_d^{f_d(s)}} \cdot c(d) \leq \mathbf{b} \cdot \rho_{max} \tag{3}$$

and must be met for all protected failure scenario $s \in \mathcal{S}$. The scalar ρ_{max} is the value of the maximum link utilization and needs to be minimized. Thus, the objective function is

$$\rho_{max} \rightarrow \min . \tag{4}$$

The free variables to be set are $\mathbf{l_d^f} \in (\mathbb{R}_0^+)^{k_d}, d \in \mathcal{D}, \mathbf{f} \in \mathcal{F}_d^{\mathcal{S}}$ and the maximum link utilization ρ_{max} itself. The following constraints must be respected in the optimization process to obtain valid load balancing functions and to avoid overload on the links.

- **(C0)**: Equation (1) assures that the load balancing function is a distribution.
- **(C1)**: Equation (2) assures that failed paths are not used.
- **(C2)**: Equation (3) assures that the bandwidth suffices to carry the traffic in all protected failure scenarios.

These constraints constitute a linear program that can be efficiently solved for networks with up to about 100 nodes.

3.4 Joint Optimization of Load Balancing Functions and Link Capacities

We present a linear program for the joint optimization of the load balancing functions for all SPMs and the link capacities in a network. Its objective is to minimize the overall network capacity required to carry the traffic in all protected failure scenarios $s \in \mathcal{S}$

[27]. The assumption is that only the network topology and the traffic matrix are given and that links are not yet capacitated. Furthermore, the path layout $\mathbf{P_d}, d \in \mathcal{D}$ is also provided for all SPMs.

The link capacities $\mathbf{b}$ must be set in such a way that Equation (3) is met when setting the value for the maximum link utilization ρ_{max} to a fixed desired value. The objective function is the minimization of the overall bandwidth:

$$\mathbf{1}^\top \mathbf{b} \rightarrow \min . \tag{5}$$

Thus, the free variables to be set are $\mathbf{l_d^f} \in (\mathbb{R}_0^+)^{k_d}, d \in \mathcal{D}, \mathbf{f} \in \mathcal{F}_d^{\mathcal{S}}$ and the link bandwidth vector $\mathbf{b}$. Again, the constraints **C0 – C2** must be met whereby ρ_{max} is set to a fixed desired value. Also this linear program can be efficiently solved for networks with up to about 100 nodes.

3.5 Optimization of the iSPM

The integer SPM (iSPM) is a special case of the basic SPM where the load balancing functions can take only the values 0 and 1 instead of any real values between 0 and 1. If the solution of the linear programs presented above is limited to integer solutions, they are significantly more complex to solve so that optimization using linear programs is not feasible for real-world problem instances. An efficient heuristic algorithm for the optimization of the load balancing functions in capacitated networks has been presented in [3]. Its evaluation has shown that networks with up to 200 nodes can be easily optimized and the backup efficiency of the iSPM is only little worse than the one of the basic SPM. Especially in networks with an average node degree up to 5 the backup efficiency of the iSPM optimized with this heuristic is at most 5% worse than the one of the basic SPM.

3.6 Optimization of the fSPM

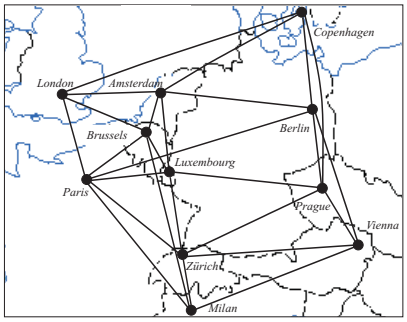
The failure-specific SPM (fSPM) is an extension of the basic SPM. The difference between them is that the load balancing functions of the fSPM $\mathbf{l_d^s}$ depend on the exact failure scenario s on the affected partial paths instead of the failure pattern $\mathbf{f_d}$ observed by the source node of the basic SPM. The linear programs presented above can be easily adapted to optimize the load balancing functions of the fSPM. This has been done in [4]. Although the number of load balancing functions $\mathbf{l_d^s}, d \in \mathcal{D}, s \in \mathcal{S}, \mathbf{f_d}(\mathbf{s}) \neq \mathbf{0}$ for the fSPM is much larger than the number of load balancing functions $\mathbf{l_d^f}, d \in \mathcal{D}, f \in \mathcal{F}_d^{\mathcal{S}}$ for the basic SPM, its evaluation has shown that the computation time required for the solution of the linear program has increased only by little; it took only 16% longer than for the basic SPM in the investigated cases. However, the improvement in backup efficiency is negligible so that fSPM is not an interesting option for implementation in practice due to its increased operational complexity.

4 Performance Results

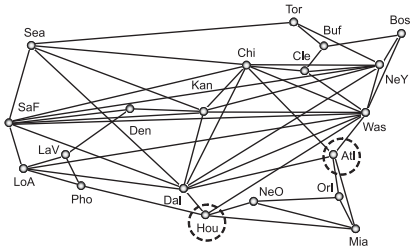
The SPM requires only very little backup capacity to protect single link and node failures [27]. In capacitated networks, significantly more protected traffic can be transmitted than with conventional single shortest path (SSP) routing [26]. This backup

efficiency of the SPM depends on the underlying network structure. When networks are tightly provisioned for protected single failures $\mathcal{S}$, the minimized backup capacity might not suffice to accommodate backup traffic from unprotected multi-failure scenarios $s \notin \mathcal{S}$ [28]. However, this also holds for other routing and resilience mechanisms when the network is capacitated only for rerouted traffic resulting from a limited set of protected single failures $s \in \mathcal{S}$. These findings are illustrated in the following.

We apply the SPM to networks with different characteristics to investigate their backup efficiency. The networks under study are the COST239 which has been used in the COST239 project [29] and the Labnet network which has been used in the KING project [30]. Their topologies are depicted in Figures 4(a) and 4(b). In the following studies, the COST239 network is associated with a traffic matrix proportional to the city cites [30] and the Labnet is accompanied with a homogeneous traffic matrix. The networks are assumed to have equal link capacities.



(a) The COST239 network has 11 nodes and 52 links; it has a highly resilient structure due to the large average node degree δ_{avg}.



(b) The Labnet has 20 nodes and 106 links; the simultaneous failure of Hou and Atl effects a separation of the network into two disconnected islands.

Fig. 4. Topologies of networks under study.

In addition, we study a large number of randomly constructed networks using the algorithm given in [30]. It allows to control the number of nodes n, the average node degree $\delta_{avg} = \frac{m}{n}$ where m is the number of unidirectional links, as well as the maximum deviation δ_{max}^{dev} of the node degree of a single node from the average node degree δ_{avg}. The construction algorithm is based on the Waxman model [31] so that close nodes are more likely to be connected than distant nodes. For these random networks we assume equal traffic matrices and equal link capacities.

In the remainder, the path layout of the SPMs is calculated using the k-disjoint-shortest-path algorithm [25] and at most $k = 5$ link- and node-disjoint paths between source and destination are tried to be found. Furthermore, the set of protected failure scenarios $\mathcal{S}$ comprises all single link and node failures. Hence, at most one partial path

of an SPM fails. The optimization methods assume the full traffic reduction (FTR) option when nodes fail (see Section 3.2).

4.1 Impact of Network Structure on Backup Efficiency

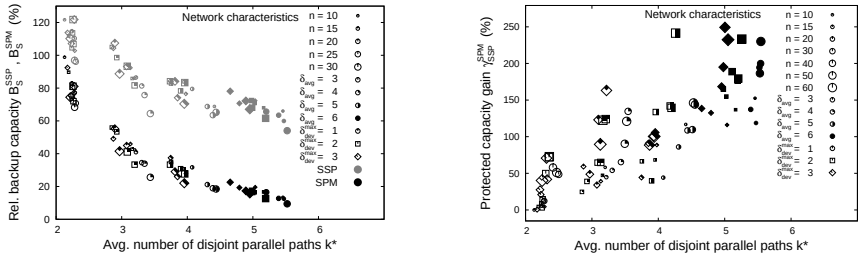
We consider the overall capacity $C_{\mathcal{S}}^{X}$ that is required to carry the traffic matrix with resilience mechanism X under all protected failure scenarios $\mathcal{S}$ (failure-free conditions, single link and node failures). We compare this capacity to the minimum capacity $C_{\emptyset}^{X}$ that is required to carry the traffic matrix under failure-free conditions. We use single shortest path (SSP) routing based on the hop-count metric for comparison since this yields the smallest value for $C_{\emptyset}^{SSP}$. We calculate the relative required backup capacity for SSP routing and rerouting by $B_{\mathcal{S}}^{SSP} = \frac{C_{\mathcal{S}}^{SSP} - C_{\emptyset}^{SSP}}{C_{\emptyset}^{SSP}}$ and obtain a value of 78% for the COST239 network.

Furthermore, we calculate the path layout for all SPMs in the COST239 network using the k-shortest paths algorithm. We jointly optimize the load balancing functions and the link capacities according to the method described in Section 3.4 while setting $\rho_{max} = 1$. As a result, the overall capacity $C_{\mathcal{S}}^{SPM}$ to carry the traffic without loss under all single link and node failures is minimized. We compute the relative required backup capacity by $B_{\mathcal{S}}^{SPM} = \frac{C_{\mathcal{S}}^{SPM} - C_{\emptyset}^{SSP}}{C_{\emptyset}^{SSP}}$ and obtain a value of 23% for the COST239 network. This is extremely little backup capacity compared to SSP routing and rerouting and shows the very good backup efficiency of the SPM.

We investigate the relative required backup capacity for SSP and SPM depending on network characteristics using a large number of randomly constructed networks. We vary the network size n, the average node degree δ_{avg}, the maximum deviation δ_{dev}^{max} of the nodes from the average node degree, and construct 5 sample networks for each configuration. We average for these 5 sample networks the average number of disjoint paths per node pair and also the relative backup capacity. These data are compiled in Figure 5(a). They show that the SPM requires clearly less backup capacity than SSP. The relative backup capacity significantly depends on the average number of disjoint parallel paths in the network. In contrast, the number of nodes n and the maximum deviation from the average node degree δ_{max}^{dev} have a rather small impact.

We consider the optimization of load balancing functions for capacitated networks. We minimize the maximum link utilization ρ_{max}^{SPM} for all single link and node failures for the basic SPM and calculate this value ρ_{max}^{SSP} also for SSP routing and rerouting. We define $\gamma_{SSP}^{SPM} = \frac{\rho_{max}^{SSP}}{\rho_{max}^{SPM}} - 1$ as the protected capacity gain by SPM compared to SSP. Applied to the COST239 network, we get $\gamma_{SSP}^{SPM} = 1.09$. Thus, the SPM can carry more than twice the traffic that SSP can handle with protection. This again reveals an excellent backup efficiency for the SPM.

We extend this study to sample networks in analogy to above, and Figure 5(b) shows its results. The protected capacity gain is always positive and increases clearly with the average number of disjoint parallel paths in the network. In larger networks it also tends to be larger than in smaller networks. Under certain conditions, the SPM can carry 250% more protected traffic than SSP. This can be explained as follows. The probability for a mismatch between the capacity of a link and its carried traffic under SSP routing



(a) Relative backup capacity in uncapacitated networks.

(b) Protected capacity gain in networks with equal link capacities.

Fig. 5. Backup efficiency in random networks: basic SPM vs. single shortest path IP routing and rerouting.

and rerouting increases with the network size. Therefore, the maximum link utilization ρ_{max}^{SSP} also increases. In contrast, the SPM steers traffic around bottleneck links and avoids large maximum link utilizations ρ_{max}^{SPM} which works well when the network has multiple disjoint paths.

In [32] we have compared the backup efficiency of the SPM and the following other resilience mechanisms:

- SSP: single shortest path routing
- optSSP: optimized SSP using the heuristic in [8]
- ECMP: equal-cost multpath routing
- optECMP: optimized ECMP using the heuristic in [8]
- PB: disjoint primary and backup path routing (obtained through simple 2-disjoint shortest paths calculation)
- optPB: optimized primary and backup path routing (obtained as a special case of the iSPM with only two partial paths per multipath)
- Bypass: standard MPLS-FRR facility backup
- impBypass: MPLS-FRR facility backup with the simple improvement presented in [11]
- Detour: standard MPLS-FRR one-to-one backup
- impDetour: MPLS-FRR one-to-one backup with the simple improvement presented in [12]

The SPM is clearly superior to all other resilience mechanisms with regard to backup efficiency. While optSSP, ECMP, optECMP, PB, optPB were more backup-efficient than SSP, impDetour, Detour, impBypass, and especially Bypass turned out to be less backup-efficient than SSP.

4.2 Traffic Loss due to Unprotected Multi-Failures

The SPM requires only little backup capacity to protect single link failures. If only little backup capacity is provided, some traffic is possibly lost in case of unprotected

multi-failures when there is insufficient backup capacity. This issue has been investigated in [28] and compared with SSP and ECMP routing and rerouting. The Labnet in Figure 4(b) was used for the analysis in [28] together with a homogeneous traffic matrix to facilitate the evaluation. Single link failures cannot partition the Labnet in two parts, but the simultaneous failures of nodes Hou and Atl effect a separation of the network into two disconnected islands.

The SPM has optimized load balancing functions for single path failures. If two paths fail, some interpolation between suitable load balancing functions should quickly yield a valid load balancing function for that case. 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).

Traffic loss can be due to overload because of rerouted flows and missing backup capacity (A); it can be due to node failures so that demands starting and ending in the failed nodes are lost (B); it can also be due to unavailable paths when a network is disconnected by failures (C). Sufficient backup capacity can minimize only the lost traffic due to (A). Link failures are more likely than router failures. Similarly, double link failures ($\mathcal{S}_{LL}$), link and router failures ($\mathcal{S}_{LR}$), and double router failures ($\mathcal{S}_{RR}$) have different probabilities and also different impact. Averaging over all of them obscures the impact of the different failure classes, therefore, they are analyzed and reported separately.

Table 1. 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

Double link failures can cause traffic loss only due to (A). Table 1 shows that double link failures lead to an average traffic loss of 0.436% and 0.315% for SSP and ECMP routing in the Labnet network when it was capacitated very tightly for single link and node failures only. The SPM leads to significantly more traffic loss in the order of 2% whereby the exact SPM variant has only little impact on the lost traffic. Link and router failures lead to lost traffic due to (A) and (B). They lead to 10% lost traffic due to (B). The remaining lost traffic is due to (A) which is caused by missing backup capacity. This is about 0.85% for SSP and ECMP while it is about 3% for the SPM. Double router failures lead to lost traffic due to (A), (B). About 19.47% lost traffic is due to (B). One out of 190 possible double router failures leads even to lost traffic due to (C) so that additional 11.84% traffic is lost in that particular case. Averaged over all double failures,

this increases the lost traffic only by 0.06% and has quite little impact. Hence, SSP and ECMP lose about 1.5% traffic due to missing capacity (A) while the SPM variants lose about 3.9% traffic due to missing capacity (A). When the results for the different double failure scenarios are weighted by their probabilities, SSP and ECMP lead to 0.5% and 0.39% lost traffic while the SPM mechanisms lead to about 2.1% lost traffic. Hence, the SPM leads to clearly more average traffic loss than SSP or ECMP routing and rerouting in case of double failures due to the minimized backup capacity. However, the traffic loss is not tremendously higher. These numbers were obtained from a rigid analysis assuming that capacity is provided very tightly. This is of course not realistic.

Although the average lost traffic due to missing capacity in case of double failures is rather small, providing enough capacity to avoid missing backup capacity for all double failures is quite expensive. Table 2 shows how much relative backup capacity is required for the same mechanisms as above to avoid traffic loss due to missing capacity for different sets of protected failure scenarios. Thereby, the SPM remains optimized for single failures and the backup capacity required for double failures is calculated for the different strategies (SPM-INTR, SPM-SSP, SPM-ECMP). The table shows that the protection against double failures requires significantly more backup capacity than for single failures. The capacity savings of the SPM compared to SSP and ECMP remain and even increase. In contrast to protection against single failures, the different SPM strategies (SPM-INTR, SPM-SSP, SPM-ECMP) require different backup capacity values when double failures are protected.

Table 2. Required network resources in capacity units and relative required backup capacity in percent for the resilience against different protected failure scenarios $\mathcal{S}$.

Sets of protected failures	SSP	ECMP	SPM-INTR	SPM-SSP	SPM-ECMP
$\mathcal{S}_L, \mathcal{S}_R$	93%	77%	48%	48%	48%
$\mathcal{S}_L, \mathcal{S}_R, \mathcal{S}_{LL}$	183%	143%	103%	119%	115%
$\mathcal{S}_L, \mathcal{S}_R, \mathcal{S}_{LL}, \mathcal{S}_{LR}, \mathcal{S}_{RR}$	238%	207%	117%	172%	168%

5 Summary

The SPM is a simple protection switching mechanism for connection-oriented, packet-switched networks. Therefore, it may be applied, e.g., in MPLS or Carrier Ethernet networks. The SPM sets up several disjoint paths and transmits traffic over them according to a load balancing function that depends on the set of failed paths. Optimization of the load balancing functions can minimize the required backup capacity dramatically or maximize the protected capacity in capacitated networks. Hence, the SPM is simple and provides fast fail-over at low cost. It is a compelling protection switching mechanism for future transport networks.

Acknowledgment

The author would like to thank Ulrich Spoerlein for his valuable inputs in preparing the manuscript as well as David Hock and Matthias Hartmann for proof-reading.

References

1. Menth, M., Reifert, A., Milbrandt, J.: 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) 526 – 537
2. Martin, R., Menth, M., Hemmkeppler, M.: 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 (October 2006)
3. Martin, R., Menth, M., Spoerlein, U.: Integer SPM: Intelligent Path Selection for Resilient Networks. In: IFIP-TC6 Networking Conference (Networking), Atlanta, GA, USA (May 2007)
4. Menth, M., Martin, R., Spoerlein, U.: Failure-Specific Self-Protecting Multipaths – Increased Capacity Savings or Overengineering? In: International Workshop on Design of Reliable Communication Networks (DRCN), La Rochelle, France (October 2007)
5. Menth, M., Martin, R., Koster, A.M.C.A., Orlowski, S.: Overview of Resilience Mechanisms Based on Multipath Structures. In: International Workshop on Design of Reliable Communication Networks (DRCN), La Rochelle, France (October 2007)
6. Fortz, B., Thorup, M.: Internet Traffic Engineering by Optimizing OSPF Weights. In: IEEE Infocom, Tel-Aviv, Israel (2000) 519–528
7. Fortz, B., Thorup, M.: Robust Optimization of OSPF/IS-IS Weights. In: International Network Optimization Conference (INOC), Paris, France (October 2003) 225–230
8. Menth, M., Hartmann, M., Martin, R.: Robust IP Link Costs for Multilayer Resilience. In: IFIP-TC6 Networking Conference (Networking), Atlanta, GA, USA (May 2007)
9. Hartmann, M., Hock, D., Schwartz, C., Menth, M.: Objective Functions for Optimization for Resilient and Non-Resilient IP Routing. In: 7^{th} International Workshop on Design of Reliable Communication Networks (DRCN), Washington, D.C., USA (October 2009)
10. Pan, P., Swallow, G., Atlas, A.: RFC4090: Fast Reroute Extensions to RSVP-TE for LSP Tunnels (May 2005)
11. Martin, R., Menth, M., Canbolat, K.: 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) 329 – 338
12. Martin, R., Menth, M., Canbolat, K.: 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 (October 2006)
13. Rai, S., Mukherjee, B., Deshpande, O.: IP Resilience within an Autonomous System: Current Approaches, Challenges, and Future Directions. IEEE Communications Magazine **43**(10) (October 2005) 142–149
14. Atlas, A., Zinin, A.: RFC5286: Basic Specification for IP Fast Reroute: Loop-Free Alternates (September 2008)
15. Martin, R., Menth, M., Hartmann, M., Cicic, T., Kvalbein, A.: Loop-Free Alternates and Not-Via Addresses: A Proper Combination for IP Fast Reroute? accepted for Computer Networks (2009)

16. Bryant, S., Previdi, S., Shand, M.: IP Fast Reroute Using Not-via Addresses. http://tools.ietf.org/id/draft-ietf-rtgwg-ipfrr-notvia-addresses-04.txt (July 2009)
17. Nelakuditi, S., Lee, S., Yu, Y., Zhang, Z.L., Chuah, C.N.: Fast Local Rerouting for Handling Transient Link Failures. IEEE/ACM Transactions on Networking **15**(2) (April 2007) 359–372
18. Menth, M., Martin, R.: Network Resilience through Multi-Topology Routing. In: 5^{th} International Workshop on Design of Reliable Communication Networks (DRCN), Island of Ischia (Naples), Italy (October 2005) 271 – 277
19. Cicic, T., Hansen, A.F., Kvalbein, A., Hartmann, M., Martin, R., Menth, M.: Relaxed Multiple Routing Configurations for IP Fast Reroute. In: IEEE Network Operations and Management Symposium (NOMS), Salvador de Bahia, Brazil (April 2008)
20. Murakami, K., Kim, H.S.: Optimal Capacity and Flow Assignment for Self–Healing ATM Networks Based on Line and End-to-End Restoration. IEEE/ACM Transactions on Networking **6**(2) (April 1998) 207–221
21. Ou, C.S., Rai, S., Mukherjee, B.: Extension of Segment Protection for Bandwidth Efficiency and Differentiated Quality of Protection in Optical/MPLS Networks. Optical Switching and Networking: A Computer Networks Journal **1**(1) (January 2005) 19 – 33
22. Koster, A.M.C.A., Zymolka, A., Jäger, M., Hülsermann, R.: Demand-Wise Shared Protection for Meshed Optical Networks. Journal of Network and Systems Management **13**(1) (2005) 35–55
23. Grover, W.D., Stamatelakis, D.: Cycle-Oriented Distributed Preconfiguration: Ring-Like Speed with Mesh-Like Capacity for Self-Planning Network Restoration. In: IEEE International Conference on Communications (ICC). (Jun 1998) 537–543
24. Kandula, S., Katabi, D., Davie, B., Charny, A.: Walking the Tightrope: Responsive Yet Stable Traffic Engineering. In: ACM SIGCOMM, Philadelphia, PA, USA (August 2005)
25. Bhandari, R.: Survivable Networks: Algorithms for Diverse Routing. Kluwer Academic Publishers, Norwell, MA, USA (1999)
26. Menth, M., Martin, R., Spoerlein, U.: Optimization of the Self-Protecting Multipath for Deployment in Legacy Networks. In: IEEE International Conference on Communications (ICC), Glasgow, Scotland, UK (June 2007)
27. Menth, M., Martin, R., Spoerlein, U.: Network Dimensioning for the Self-Protecting Multipath: A Performance Study. In: IEEE International Conference on Communications (ICC), Istanbul, Turkey (June 2006)
28. Menth, M., Martin, R., Spoerlein, U.: Impact of Unprotected Multi-Failures in Resilient SPM Networks: a Capacity Dimensioning Approach. In: IEEE Globecom, San Francisco, California, USA (November 2006)
29. Batchelor, P., Daino, B., Heinzmann, P., Hjelme, D., Inkret, R., Jäger, H., Joindot, M., Kuchar, A., Le Coquil, E., Leuthold, P., de Marchis, G., Matera, F., Mikac, B., Nolting, H.P., Späth, J., Tillerot, F., Van Caenegem, B., Wauters, N., Weinert, C.: Study on the Implementation of Optical Transparent Transport Networks in the European Environment - Results of the Research Project COST 239. Photonic Network Communications **2**(1) (2000) 15–32
30. Menth, M.: Efficient Admission Control and Routing in Resilient Communication Networks. PhD thesis, University of Würzburg, Faculty of Computer Science (July 2004)
31. Waxman, B.M.: Routing of Multipoint Connections. IEEE Journal on Selected Areas in Communications **6**(9) (1988) 1617–1622
32. Menth, M., Martin, R., Hartmann, M., Spoerlein, U.: Efficiency of Routing and Resilience Mechanisms in Packet-Switched Communication Networks. accepted for European Transactions on Telecommunications (ETT) (2009)