Evaluation of Novel Resilience Schemes in Dynamic Optical Transport Networks*

Monika Jaeger[a], Ralf Huelsermann[a], Dominic A. Schupke[b], René Sedlak[c]

[a]T-Systems Nova GmbH, Technologiezentrum,
[b]Inst. of Communication Networks, Munich University of Technology
[c]Deutsche Telekom AG, Fachhochschule Leipzig, University of Applied Sciences

ABSTRACT

Today, Wavelength Division Multiplexing (WDM) transmission systems are deployed extensively in transport networks. They are used mainly for static point-to-point connections. With the availability of fast reconfigurable Optical Cross Connects (OXC) and the introduction of a control plane in the Optical Transport Network (OTN), optical channel based logical networks can be built for dynamic WDM networks.
Resilience in current transport networks is mainly based on static SONET/SDH dedicated and shared protection. Distributed control planes allow new, flexible protection mechanisms (e.g. GMPLS reroute and fast reroute).
To evaluate future distributed control concepts and new resilience schemes in transport networks, we have implemented a dynamic OTN simulation model.
Several case studies have been performed using different protection and restoration methods. Different failure scenarios (single or multiple link failures) were used. The paper evaluates the case studies in terms of scalability, recovery time criteria, capacity use (efficiency) and availability. It is shown that the new and flexible resilience schemes are a promising alternative to traditional statically preplanned protection in transport networks. Furthermore, they provide increased network availability in multiple failure cases.

Keywords: Resilience, Protection, Restoration, Availability, MPLS, GMPLS, ASON, ASTN, Optical Internetworking

I. INTRODUCTION

Currently optical transport networks are (semi-)permanent in the sense that provisioning of connections is done on a long-term basis. Most often, services are protected in the SONET/SDH layer with static protection mechanisms. Up to now, IP networks purely rely on slow but failure robust IP rerouting mechanisms. These will be enhanced in the future by MPLS restoration functions. Optical transport networks today are mostly based on static WDM system connections. With the introduction of fast reconfigurable optical switching nodes like Optical Add Drop Multiplexers (OADMs), Optical Cross Connects (OXCs), and wavelength based optical channel routing functions, the optical layer can dynamically provide optical channel services and virtual topologies to higher layers. In addition, the optical layer may be used for providing resilience functions. IP/MPLS-like distributed control planes for OTNs are defined in the standardization fora (IETF's GMPLS framework, ITU-T's ASON/ASTN) [4, 7, 5]. A control plane mainly consists of

* This work was done within the TransiNet project, supported by the Federal German Ministry of Education and Research [6].

[a] {Monika.Jaeger, Ralf.Huelsermann}@t-systems.com; T-Systems Nova GmbH, Tchnologiezentrum, Goslarer Ufer 35, D-10589 Berlin, Germany

[b] Schupke@ei.tum.de; Institute of Communication Networks, Munich University of Technology, Arcisstrasse 21, D-80290 Munich, Germany

[c] renesedlak@gmx.de; Deutsche Telekom AG, Fachhochschule Leipzig University of Applied Sciences, Gustav-Freitag-Strasse 43/45, D-04277 Leipzig, Germany

distributed routing and signaling functions needed for connection control [1]. With the availability of a control plane for the optical layer, fast and efficient MPLS-like restoration mechanisms based on optical channels can be introduced in OTNs. In the following, we investigate and evaluate new resilience schemes for future dynamic optical transport networks.

II. ROUTING IN OPTICAL NETWORKS

An optical channel is a wavelength based end-to-end connection through the optical layer of an OTN. There are different methods for calculating optical channel routes in optical networks. Other than in shortest path IP-routing schemes, in optical networks it is necessary to ensure that a chosen path provides enough resources, i.e. free wavelengths on all links. We call the shortest path with sufficient resources at the time of the setup request the 'shortest available path'.

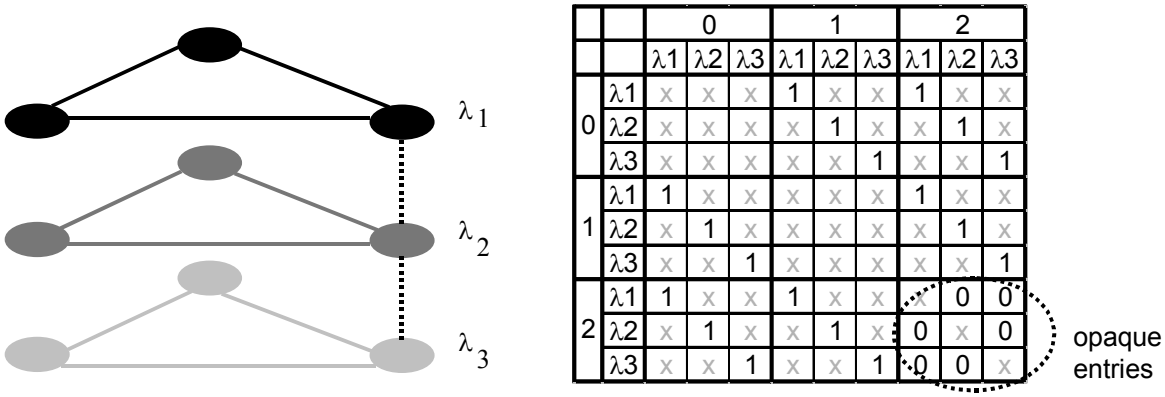
IP-routing protocols use distributed routing mechanisms, i.e. each packet will be routed hop-by-hop through the network, where the routers along the route only choose the best next hop. In optical networks, resource information has to be distributed in addition to topology information. Due to the above described resource availability requirement on 'shortest available paths' and due to the difference that wavelength switched optical networks are connection-oriented networks as opposed to packet-oriented IP networks, the distribution of routing decisions is not as simple as in packet based networks. In our simulation models we therefore use explicit source routing. Each router in the network has to have the same knowledge about the current network state, and the routers at the source compute the complete routes through the network to the destination, originating from itself. The most simple way to model consistent topology databases distributed over all routers is to implement a unique central resource database, to which all routers have simultaneous access. With this approach the problem of inconsistent databases is negligible.

With the availability of topology information the routers are enabled to construct network graphs. The commonly used algorithm to compute shortest paths in graphs is the Dijkstra Algorithm. There are several alternatives when to calculate paths. First, using a pre-calculation the router calculates routes to a limited set of destinations or to all possible destinations during the initialization phase. In case of an incoming connection request the router has to check only, whether there are resources available along the pre-calculated route. If not, the connection gets blocked. This method reduces the processor load during the working phase, because the processing intensive route calculation has been done before. On the other hand, this scheme does not take alternative available routes based on the current network state into account. If the route calculation occurs online after the connection request has arrived, it is possible to manipulate the network graph with current resource information.

A modification of the route pre-calculation is the computing of more than one route between two nodes. In this case a set of routes can be checked online for free resources. There are several algorithms for computing k-shortest paths in the literature [3].

We consider two types of OXCs: first, so-called opaque OXCs with an electrical switching backplane, and second, transparent OXCs which switch signals in the optical layer. In the latter, there is no opto-electronic conversion and the signals are switched continuing on the same wavelengths. Thus, routes in transparent all-optical networks have to satisfy the Routing and Wavelength Assignment (RWA) constraints, where available paths must be wavelength continuing. The transparency length of all-optical connections is limited through degradation effects. However, throughout this paper we assume all transparent optical channel connections are shorter than the maximum transparent path length.

We call optical networks with opaque switching nodes opaque networks and optical networks with transparent switching nodes transparent networks. One method to compute routes in all three types of optical networks is the layered-graph scheme [Figure 1]. Every layer reflects a certain wavelength. A link is represented by all edges (wavelengths) lying on top of each other in the graph. At opaque nodes additionally vertical edges are inserted, connecting the layers and, thus, enabling wavelength conversion. The size of the resulting adjacency matrix [Figure 1] scales quadratically with the number of wavelengths and nodes (every new link/node increases the size of the topology by the order of # of wavelengths), but allows to obtain the wavelength specific shortest available path on all links within one calculation step, since the topology distinguishes different wavelengths, i.e. wavelength-specific routes are found. Currently, we set the costs for the vertical edges indicating wavelength conversion to zero. In future studies we will test if non-zero costs can help to reduce wavelength conversion costs.



		0			1			2		
		λ1	λ2	λ3	λ1	λ2	λ3	λ1	λ2	λ3
0	λ1	x	x	x	1	x	x	1	x	x
	λ2	x	x	x	x	1	x	x	1	x
	λ3	x	x	x	x	x	1	x	x	1
1	λ1	1	x	x	x	x	x	1	x	x
	λ2	x	1	x	x	x	x	x	1	x
	λ3	x	x	1	x	x	x	x	x	1
2	λ1	1	x	x	1	x	x	x	0	0
	λ2	x	1	x	x	1	x	0	x	0
	λ3	x	x	1	x	x	1	0	0	x

Figure 1: Principle of the layered graph model

Calculation of Disjoint Routes

For the pre-calculation of protection connections we have to compute link or node disjoint routes for a span or for end-to-end paths. We can do this in two steps by calculating the working (shortest) path first and calculate the backup (shortest disjoint) path then. The total length of working and backup path is not necessarily the minimum. Additionally, in some cases the two-step algorithm blocks by the working path all possible backup paths [Figure 2]. The shortest cycle algorithm avoids these disadvantages. This algorithm makes use of a modified Dijkstra Algorithm [2], which can handle negative edge weights and computes the shortest cycle between two given nodes [Figure 2]. The shorter branch of the cycle will get the working path, the longer one the backup path.

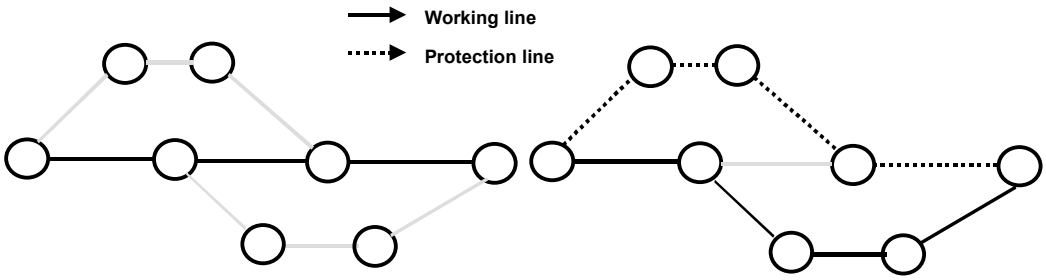


Figure 2: Difference between the two-step and the one-step algorithm

III. OVERVIEW OF RESILIENCE SCHEMES FOR DYNAMIC OPTICAL TRANSPORT NETWORKS

1. Protection & Restoration Today

Throughout the literature the terms protection and restoration are used in slightly different meanings. Protection makes use of pre-assigned capacity between nodes. This includes the pre-calculation of the protection path and the pre-planning of resources. There is 1+1 protection, where the signal is transported over both a working and a protection path simultaneously. In 1:1 protection, working and protection paths are set up at connection setup time, but after a failure, the signal has to be switched from the working to the protection path. In M:N shared protection, the protection capacity is assigned to the specific protection path after the failure. In this paper we use the term protection as the mechanism which sets up both working and backup path at connection setup time (1:1 protection). By this all backup resources are pre-assigned. Due to this pre-assignment all protected connections are fully protected in case of single link failures.

We denote by the term restoration that any capacity available between two nodes is used to recover from a failure. Not until a failure has occurred, a backup path will be searched and, if found, the resources for the path will be assigned in the network. This method is simple, since it can be implemented as a re-setup of the path, but it can not be predicted easily (unless providing a huge amount of spare capacity) whether all services can be restored in different failure cases.
We define recovery time as the time it takes for the connectivity to be restored upon a failure for a data flow from ingress to egress point through the optical network. This time period includes all network activities necessary to restore the connectivity, e.g. failure notification and signaling, route calculation, and switching procedures. The total recovery time ranges between ≈50 ms in protected SDH/SONET networks and more than 40 s in IP networks with fault notification through exceeding the router dead counter.

2. Dedicated Path-Protection (1+1 / 1:1)

Dedicated path protection is mostly used in today's ring based SONET/SDH networks. In 1:1 protection, failures have to be detected and signaled, which is done with SONET/SDH alarms, before the data transmission will be locally switched over to the backup path. As can be easily seen, in ring networks at least 100% of the working capacity is necessary for the backup paths. The working paths take the shorter path in the ring and the backup paths take the longer path in the opposite direction of the ring. The same effect happens in mesh networks, but in general, the difference between working and backup path length is less significant. Future transport networks are expected to be less ring based but rather mesh topologies. In meshed networks, with little differences, dedicated path protection approaches are also possible. During connection setup two link and/or node disjoint paths are calculated [Figure 3]. The shorter route is chosen for the working path, and the longer route for the backup path. Figure 3 shows that in mesh networks it is possible to share backup resources between different connections. Due to the fact that SONET/SDH networks are (semi-)static networks, it is possible to optimize the usage of shared backup resources. Very efficient methods for planning shared backup resources, like the shared backup tree concept described in [19], can save about 30% capacity compared to a scenario without sharing. The disadvantage of such methods is that the optimization allows no online-calculation. The optimization methods are post-processing methods, optimizing the actual network state. In dynamic

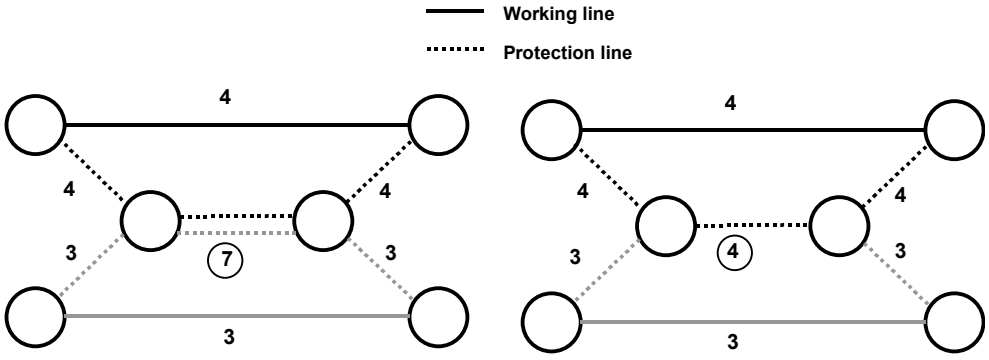


Figure 3: Difference between dedicated and shared protection in mesh topologies

optical networks we consider very short duration times of the connections, i.e. the networks state will change continuously. So, with post-processing methods the backup routes must be changed also continuously, which will reach in an undesirable effort to compute the backup routes. In contrast online calculation means, that during setup an optimal configuration of the backup path will be found, which will not change during the lifetime of the connection. We expect, that this will be a good compromise between the processing effort and the backup route optimization (see Section 3). In a failure case, the failure has to be detected and signaled, which can be done with SONET/SDH alarms, and the data transmission has to be switched over to the backup path.

3. Shared Backup Path Concept

There are several proposals for shared protection approaches for dynamic optical networks. We have implemented in our model a shared protection method usable for dynamic networks [11, 12]. This approach is an online-calculation where the working path is routed along the available shortest path, and the backup path is found on the link-disjoint route on which the highest backup sharing is possible. The concept provides 100% protection guarantee in case of

single link failures. The information needed by the nodes to compute the working and the backup path is restricted to the usage of each wavelength on each link, whether they are used as backup or working resource or whether they are free.

4. *p*-Cycles

p-Cycles can be regarded as pre-configured protection cycles in a mesh network. References [14,15] have shown that *p*-cycles can be efficiently applied to optical networks for link protection. Figure 4 (a) depicts a network with one link *p*-cycle. The *p*-cycle is able to protect on-cycle links as shown in Figure 4 (b). Furthermore, a *p*-cycle is able to protect straddling links. A straddling link is an off-cycle link having *p*-cycle nodes as endpoints. In the case of a straddling link failure, a *p*-cycle can simultaneously protect two working paths on the straddling link by providing the two alternative paths around the *p*-cycle as shown in Figure 4 (c)-(d).

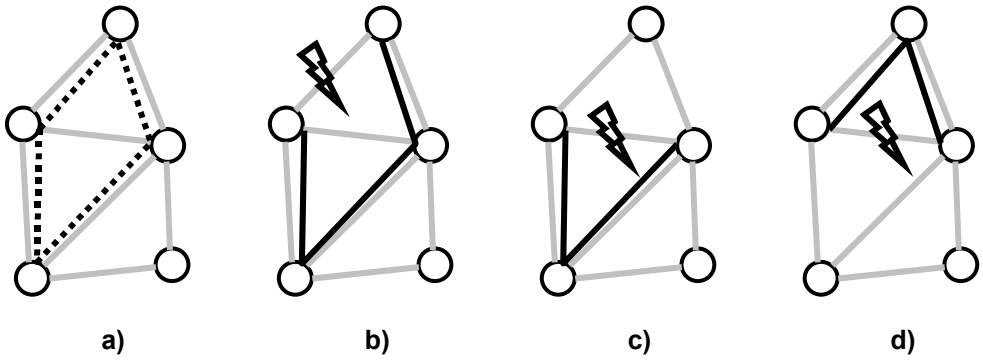


Figure 4: Link protection with *p*-cycles

In the following we consider virtual *p*-cycles, where the individual cycles are re-configurable by a network management [14,15,16] or by distributed self-organization [13,18]. The network configuration process of *p*-cycles in an existing network can be sketched as follows. First, a given demand for connections is routed through the network, so that the links reserve (working) capacity for the demands. The spare capacity of the links is the remaining available capacity. Then the *p*-cycles are formed in the spare capacity of the network. The set of link *p*-cycles is chosen such that for every link the working connections are protected by *p*-cycles of corresponding capacity. The routing of the demands has to be adapted, if a protecting set of *p*-cycles cannot be found.
p-Cycles have the outstanding property that protection switching decisions can be made quickly, since only the nodes neighboring the failure need to perform any real-time actions. Convergence times in the order of some 10 ms comparable to SONET/SDH line-switched rings can be achieved.
Therefore, *p*-cycles can be deployed efficiently using non-real-time configuration (centralized network management system or distributed self-organization) while the (distributed, node-internally processed) reaction to failures is very quick.
Each *p*-cycle represents a protection domain which is able to fully protect a single link within its domain. Multiple failures can be survived if the individual failures are in different domains. Thus, multiple *p*-cycles in a network can be used to decrease the probability of unrecoverable services during multiple failures.

5. MPLS Resilience Schemes

The Generalized Multiprotocol Label Switching (GMPLS) framework of the IETF [7] extends the Multiporotocol Label Switching (MPLS) concept for other layers than the IP layer, such as a TDM layer or the optical layer. Primarily the MPLS-Stack was designed to give the IP layer a more connection-oriented behaviour. IP-packets should no longer be routed hop-by-hop based on their IP addresses, but rather on virtual paths. To do this, MPLS creates a so-called Label Switched Path (LSP) between an ingress and an egress node. The creation and routing of the LSPs can be done statically by the network management or dynamically through routing and signalling protocols. It is possible to reserve bandwidth for LSPs on the links. The mapping between data packets and the transport on a specific LSP is based on Forwarding Equivalence Classes (FECs). Criteria for such FECs can be, e.g. IP addresses (source or destination) or protocol types. When an IP packet arrives at an ingress router, the router checks whether the packet belongs to a specific FEC. If this is the case, the router marks the packet with a specific label of the related LSP and forwards the packet to

the next Label Switched Router (LSR). Once a packet is labeled, all forwarding operations are label based. Then, the LSRs only have to look for the outgoing interface and the new outgoing label. The egress LSR picks the label and forwards the packet out of the MPLS domain.
It is possible to port the control plane principle of MPLS, with modifications, to other layers like the optical layer. The IETF is working on the standardization of the GMPLS framework. Mapping of the most significant properties of MPLS into the optical domain is done as follows:

Electrical MPLS:

- Electrical LSPs → virtual channels
- Assignment of label to LSP (virtual channel): Label Information Base (LIB)
- No data sent on LSP, no bandwidth used (reservation is possible) -> not used capacity available to other data flows on the same link

Optical Domain MPLS (also called Multiprotocol Lambda Switching):

- LSPs based on wavelengths paths → real optical channels
- Wavelengths = labels
- LSP reservation → dedicated optical channel, capacity cannot be used by other data flow on the same link

Electrical MPLS is a packet switched, virtual connection oriented technique which by the latter allows to provide quality or grade of service and several resilience schemes. In IP networks without MPLS the only mechanism in use is IP rerouting, where network element failures are handled as topology changes, which result in routing table updates. This scheme is very robust but also very slow (recovery times >> 1s).
MPLS resilience is based on protection and restoration of LSPs [8, 9]. In the following we will describe in detail the selection of different MPLS resilience schemes.

Local (link/span) Protection & Restoration

The main idea behind this scheme [Figure 5] is to calculate backup paths at nodes close adjacent to the failed links/spans. The advantage is that failure detection and switching procedures are locally restricted, and so the recovery time can be very short. Local protection in this case means that the two routers at the edges of the failed link/span switch over to a pre-calculated (and possibly reserved) backup path. In case of local restoration, the backup path between the two adjacent nodes has to be found after the failure had occurred. Sharing of backup resources between two different links/spans is possible.

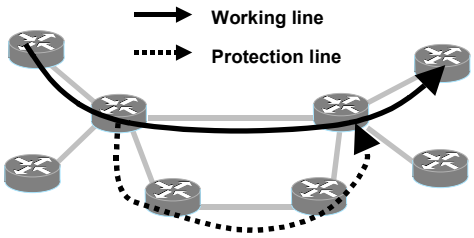


Figure 5: MPLS local protection & restoration

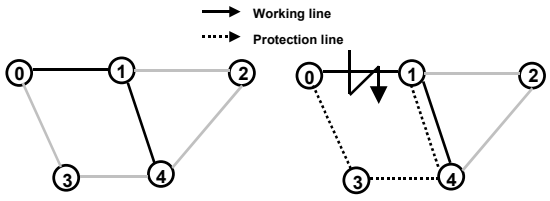


Figure 6: Quasi loop in locally protected mesh topologies

Using this scheme in meshed topologies can result in undesirable effects in some cases [Figure 6]. The topology shown is a sector from the topology, used for evaluating different resilience schemes by simulation (see Chapter IV). Due to the protection of the failed link 0-1 by the backup path 0-3-4-1 the path goes unnecessarily forth and back the link 1↔4 (a quasi-loop). Consider another failure of the link 1-4 which is protected by the backup path 1-2-4, then we obtain such a quasi-loop for two paths. The effect results in waste consumption of network resources and in additional transmission delay. Furthermore due to the double usage of resources (=wavelengths) on a link by one path it is not possible to use this scheme for bi-directional connections in transparent single fiber topologies. If only one fiber per link is installed, every wavelength on a link can be reserved only once.

MPLS Fast Reroute

A critical point in the local protection / restoration framework of MPLS is its limited scalability. For every LSP in the MPLS network it is necessary to set up a protection path for every span. This results in a number of backup LSPs which is equal to the number of LSPs multiplied by the number of spans. In terms of local restoration the edge routers of a failed span have to set up as many backup LSPs as they carry primary LSPs.
For increased scalability, a concept named fast reroute has been proposed. The idea behind this scheme is to set up only a single backup LSP and to tunnel all affected LSPs through this backup tunnel by mapping labels appropriately in the LIB [Figure 7].
Due to the consistency of labels and resources (wavelengths) in optical networks this principle can not be used in the optical domain. However, a single optical tunnel LSP could be used to protect all electrical LSPs on a wavelength.

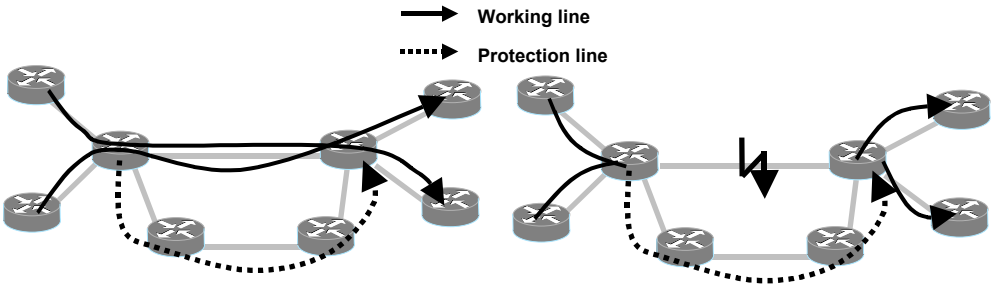


Figure 7: Principle of MPLS Fast Reroute

End to End (path) Protection/Restoration

This approach is similar to the transfer from SDH/SONET ring protection mechanisms to mesh topologies described above. A backup path for the whole end to end connection is computed. In case of protection we have a pre-calculation at connection setup, in case of restoration the path computation takes place after the failure occurred [Figure 8]. Due to the fact that in case of path protection with MPLS the only thing to do is to calculate the backup route and to arrange the label mapping in the LIB. Sharing of backup resources is easily possible. To ensure protection guarantee the backup bandwidth required in the worst case failure case has to be kept ready. It is possible to reserve extra bandwidth for sensitive LSPs In optical networks a pre-reserved backup path means allocated wavelengths. Here other resource sharing mechanisms are necessary (see Section 3).

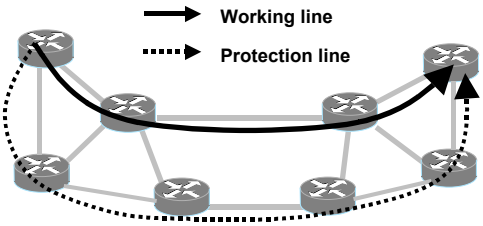


Figure 8: Principle of MPLS end-to-end protection/restoration

IV. EVALUATION OF SELECTED RESILIENCE SCHEMES

1. Validation of scalability and convergence time of MPLS resilience mechanisms

We see three main criteria, on which different resilience strategies can be evaluated. The first criterion is the scalability, which depends on the complexity of actions necessary to guarantee and restore the connectivity for a connection. It also depends on how the number of actions scales with the size of topologies or traffic matrices. The second criterion is the recovery time and the third the resource efficiency.

We give some evaluation results on the differences in scalability in [Table 1] and convergence time criteria in [Table 2] for the above described MPLS-like resilience schemes. In the following section we evaluate the capacity efficiency of selected mechanisms validated by analytical simulations. As can be seen the scalability of link protection is critical, while path protection and fast reroute scale in a linear way. Link and path restoration schemes, having the best scalability, need the longest recovery time, whereas link protection, having problems with scaling, is extremely fast.

Scalability critical issues

	# of required precalculated backup LSP's
path/link restoration	0
path protection	# of LSP's
link protection	# of LSP's • # of Links
fast reroute	# of Links

Table 1: Differences in scalability of MPLS resilience schemes

Necessary recovery time critical actions

	failure		Backup Path	
	detection	signaling	calculation	signaling
path restoration	x	x	x	x (end to end)
link restoration	x	x	x	x (local)
path protection	x	x		
link protection	x			
fast reroute	x			

Table 2: Differences in recovery time critical actions of MPLS resilience schemes

2. Quantitative Evaluation of Resource Efficiency

To obtain quantitative results about the resource efficiency of different resilience schemes in optical networks, we analyzed a selection of the resilience mechanisms described above. These schemes are:

1. End-to-end dedicated path protection (without backup resource sharing)
2. End-to-end shared path protection
3. Dedicated link protection
4. The *p*-cycle approach

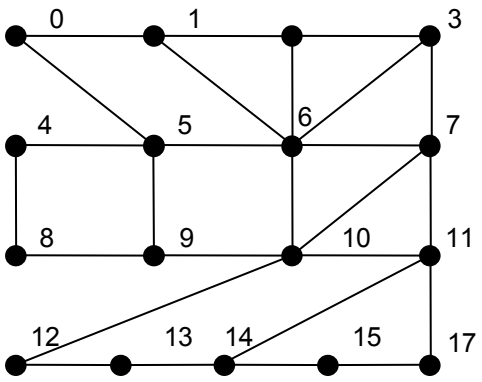


Figure 9: Analyzed network topology

name of the node

name of the node	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
0			2								2						
1			1				1										
2				1		1	3	2	1	1	1				1		1
3							2	2			1	1					1
4						1			1	1							
5							4	3	1	4	3						
6								3	1	4	5	2			1		
7										3	3	1			1	1	1
8										2	1				1		
9											5				1		
10												1	1	1	2	2	2
11															1		1
12														1	1		
13															1		1
14																1	1
15																	1
16																	

Table 3: Used traffic matrix (granularity = units of wavelengths à STM-16)

All schemes were simulated based on the same mesh topology as depicted in [
Figure 9] with the same demand matrix of [Table 3]. This mesh topology represents a hypothetical German national optical network topology. The traffic matrix was derived from a population model, differentiating telephone, IP and other data traffic. The connection switching was assumed to be a) fully opaque and b) fully transparent. Multiple demands for one connection were routed diversely, i.e. demands equal n were routed using n independent connections

with demand equal one. The wavelength selection was done using the first-fit principle: starting with the lowest wavelength going up to the highest, the first available wavelength is to be chosen. Furthermore we suppose that only one fiber per link is installed, so that every wavelength is supported only once on each link. During the first set of simulations, the additionally needed capacity for guaranteeing 100% availability in case of single link failures was calculated and compared to the capacity needed for a network without protection. The next simulation case analyzes the availability of the network in case of double failures. Here, the simulations were executed on the network topologies dimensioned following the first case study (spare capacity dimensioning for full coverage of single link failures).

Dimensioning for Single Link Failures

The aim of this case study was to compute the needed spare capacity for each mechanism. All working paths were routed along the shortest path. Figure 11 shows the ratio of additionally needed backup capacity for the analyzed mechanisms in the opaque network. It is easy to see that today's mostly used dedicated path protection scheme (1+1) needs about 170 % of the working capacity for protection. With the proposed new approaches this amount of capacity can be decreased substantially. For the path restoration scheme we assumed that every connection will be restored on the shortest path in the new topology after the link failure. However, this condition is not necessary. Due to the possibility of restoration to find all alternative paths after a failure case, it is possible that the spare resources can be further decreased [10] and all single link failures still can be restored. However, a too restricted dimensioning of the capacity can result in switched connections, which can not be restored in failure case.
The shared protection approach provides the same single failure protection guarantee as the 1:1 case but saves about 34 % capacity compared to the dedicated protection case. For the link protection case, where resource efficiency is not as good as in the path restoration process, but better than in the 1+1 approach, we have analyzed the quasi-loop effect described above. The difference in resource usage of the scenario with quasi loops allowed, and the scenario, where quasi loops are deleted in a post-processing, is marginal. There is a very small number of connections creating such quasi loops when using link protection in this topology.
As can be seen in Figure 11, the *p*-cycle approach performs the best and needs less than 100% of the working capacity in this scenario. It should be noted that the performance of the *p*-cycles is best, since an optimal configuration of the *p*-cycles in the spare capacity is performed. This is not done, e.g., for the shared backup path protection where the backup paths remain as initially routed (depending on the order of connection setup requests) and are thus not re-optimized after each working path setup. Although the spare capacity configuration of *p*-cycles (e.g. reconfiguration upon new

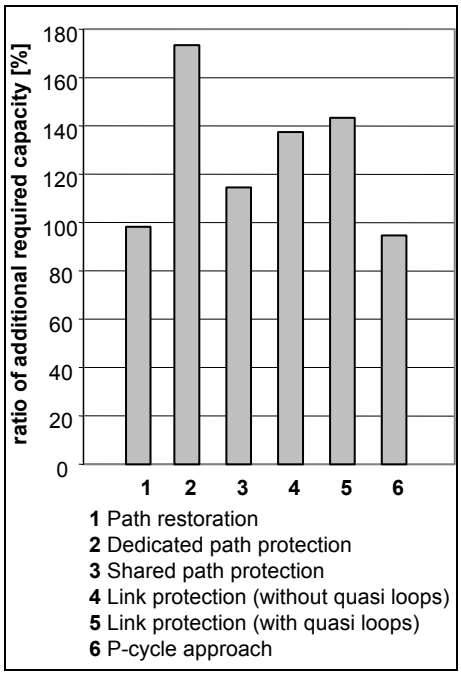


Figure 11: Comparison of the rate of additional required spare capacity in an opaque network

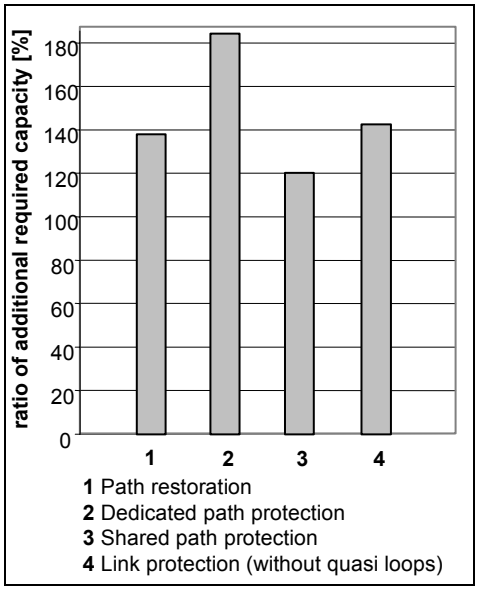


Figure 10: Comparison of the rate of additional required spare capacity in a transparent network

demands) is non-disrupting for the working capacity, other options are also available [16].

In the transparent network scenario we need to install more capacity even for the working paths, than in the opaque network scenario (217 wavelengths vs. 166 wavelengths). All demands are still routed along the same paths (shortest path), i.e. the number of wavelengths in use is the same, but to satisfy the RWA-problem more wavelengths must be installed on each link, even if some of them will not be used. The same effect occurs with the backup paths. So the absolute amount of capacity to be installed is higher than in opaque networks.
Figure 10 shows the percentage of additionally needed capacity. For the shared path protection and the link protection scheme we computed nearly the same ratio between working/backup capacity as in the opaque scenario, but the path restoration consumes much more capacity than in the opaque scenario. This effect is explained by the fact that, due to the shortest path routing in restoration, sharing of wavelengths only happens accidentally. The RWA constraint in transparent networks restricts this sharing compared to opaque networks substantially. In dedicated protection schemes, no sharing takes place in both network cases, whereas in shared protection schemes, sharing possibilities are explicitly sought, leading to less difference in the working/backup capacity ratio between opaque and transparent networks. We do not consider *p*-cycles for the transparent network scenario, since in our approach the cycles are found after routing and coloring (working) paths and, thus, are too dependent on the wavelengths assigned to the paths.

Availability in case of double failures

The probability of multiple fiber duct failures in large optical networks can become significant. According to [17], for the analyzed topology the mean time of multiple failures per year can be obtained with the formulas (1) to (3) and the assumption of a Mean Time Between Failures (MTBF) of 1750000 h per km and a Mean Time To Repair (MTTR) of 48 h. This results in a time of nearly 40 h for the mean presence of double failures per year in that network.

$$A = \left(\frac{MTBF}{MTBF + MTTR} \right)^{l} \qquad \text{(A – availability of the fiber with length l)} \qquad (1)$$

$$P = 1 - \prod_i A_i - \sum_i (1 - A_i) \prod_{j \neq i} A_j \qquad \text{(P – probability of double failures)} \qquad (2)$$

$$T = 365 \frac{d}{y} d \cdot 24 \frac{h}{d} \cdot P \qquad \text{(T – mean time of double failures in hours/year)} \qquad (3)$$

The purpose of a second investigation is to obtain the availability of the network, which is dimensioned to survive single link failures, in case of double failures with the analyzed resilience schemes. For every two-span-failure the lost (not restorable) connections are counted and over all two-span-failure cases finally averaged. Figure 13 and Figure 14 show, that the ratio of the lost calls for all mechanisms is very low. For the high value of lost calls for the *p*-cycle approach we note that a worst case analysis is performed as explained as follows. If connections on the two failed spans (obtained by the combination) are protected by the same *p*-cycle, we count one connection as lost, since the *p*-cycle protection may be already used for restoring the other one. For all two-span-failures the lost connections are counted and finally averaged. This is an upper bound calculation, since a single *p*-cycle can often protect failed connections sharing the same *p*-cycle, as long as the backup connections do not use the same part of the *p*-cycle. Furthermore, two failures on the same path and on the same *p*-cycle may be counted as a failed connection, although the path can survive. As an enhancement to survive multiple failures, after the first failure new *p*-cycles can be successfully calculated and installed which can be used for the restoration of the second failure [16].

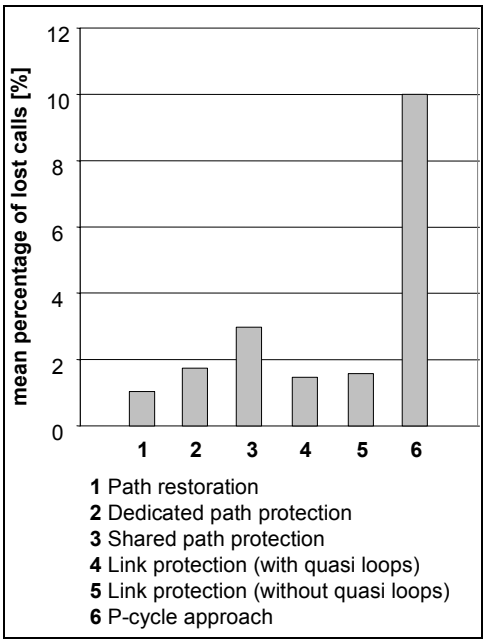


Figure 13: Mean percentage of lost calls in case of double failures in an opaque network

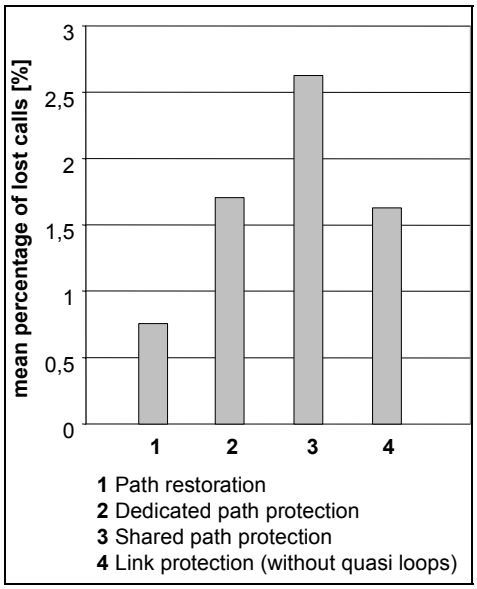


Figure 12: Mean percentage of lost calls in case of double failures in a transparent network

The path restoration scheme shows the best capability to survive double failures. This is easy to explain with the fact, that restoration is able to find any possible alternative path in the failed topology. For the protection schemes it is to be noticed in general, that the methods with the lowest capacity efficiency have the highest availability in case of double failures.

V. CONCLUSIONS

Starting with an overview of today's protection and restoration mechanisms we presented innovative resilience schemes, as proposed in the MPLS/GMPLS framework. The approaches have been evaluated with a focus on scalability, recovery time and capacity efficiency. In our studies we observe that there is not a single mechanism which fades out all the others. As far as capacity efficiency is concerned, in opaque networks the shared-protection approaches path restoration, shared path protection, and p-cycles need considerable less resources than link protection and dedicated protection. In transparent networks path restoration, shared path protection, and link protection have comparable efficiency, but outperform dedicated protection. The number of lost calls due to double-failures is for all protection and restoration mechanisms except for p-cycles less than 3% of all calls. In our first approximate calculations p-Cycles achieve a value of 10%, which is an upper bound. We expect that in future real life networks there will be a mix of different resilience schemes, depending on a service differentiation. The main traffic load should be protected using a restoration scheme, because it provides the highest capacity efficiency and so the lowest installation costs.

REFERENCES

1. D. Colle, M. Pickavet, P. Demeester, M. Jaeger, A. Gladisch, "IP-based Control Plane Architectures for Optical Networks" WAON2001 - 2nd International Workshop on All-Optical Networks, Zagreb, 2001.
2. R. Bhandari, “Survivable Networks, Algorithms for Diverse Routing”, Kluwer, Boston, 1999.
3. D. Eppstein, “Finding the k Shortest Paths” 35th IEEE Symp. Foundations of Computer Science., Santa Fe, pp. 154-165, 1994.
4. ITU-T Recommendation G.8080/Y.1304 V 1.0.
5. http://www.oiforum.com
6. http://www.transinet.de
7. E. Mannie et al., “Generalized Multi-Protocol Label Switching (GMPLS) Architecture”, http://search.ietf.org/internet-drafts/draft-ietf-ccamp-gmpls-architecture-02.txt, Work in Progress
8. V. Sharma et al., “Framework for MPLS-based Recovery”, http://search.ietf.org/internet-drafts/draft-ietf-mpls-recovery-frmwrk-03.txt, Work in Progress
9. E. Mannie et al., “Recovery (Protection and Restoration) Terminology for GMPLS”, http://search.ietf.org/internet-drafts/draft-mannie-gmpls-recovery-terminology-00.txt, Work in Progress
10. R. Huelsermann, M. Jaeger, R. Sedlak, “Simulation of Automatic Switched Optical Transport Networks”, 3. ITG Fachtagung Photonische Netze, Leipzig, April 2002.
11. R. Huelsermann, M.Jaeger, „Evaluation of a shared backup approach for optical transport networks”, accepted for ECOC 2002.
12. M. Sridharan et al, “Dynamic Routing with Partial Information in Mesh-Restorable Optical Networks”, ONDM 2002, Torino, February 2002.
13. W.D. Grover and D. Stamatelakis, “Cycle-oriented distributed preconfiguration: ring-like speed with mesh-like capacity for self-planning network restoration”, in Proc. of IEEE ICC, 1998.
14. W.D. Grover and D. Stamatelakis, “Bridging the ring-mesh dichotomy with *p*-cycles”, in Proc. of DRCN Workshop, 2000.
15. D.A. Schupke, C.G. Gruber, and A. Autenrieth, “Optimal Configuration of *p*-Cycles in WDM Networks”, in Proc. of IEEE ICC, 2002.
16. C.G. Gruber and D.A. Schupke, “Capacity-efficient Planning of Resilient Networks with p-Cycles”, in Proc. of Networks 2002, 10th International Telecommunication Network Strategy and Planning Symposium, Munich, Germany, 2002.
17. D.A. Schupke, A. Autenrieth, T.Fischer, “Survivability of Multiple Fibre Duct Failures”, in Proc. of III. DRCN Workshop, Budapest, 2001.
18. D. Stamatelakis and W.D. Grover, “OPNET Simulation of Self-organizing Restorable SONET Mesh Transport Networks”, in Proc. of OPNETWORKS, 1998.
19. D. Colle, “Design and Evolution of Data-centric Optical Networks”, PhD thesis, 2002, INTEC, University Gent, Belgium.