Dual Failure Protection in Multilayer Networks based on Overlay or Augmented Model

Robert G. Prinz[1], *Student Member, IEEE*, Achim Autenrieth[2], *Member, IEEE*, Dominic A. Schupke[2], *Member, IEEE*

[1]Munich University of Technology, Institute of Communication Networks, Arcisstr 21, 80333 Munich
[2]Siemens, Corporate Technology, Information and Communication, Otto-Hahn-Ring 6, 81739 Munich
E-mail: prinz@tum.de, {achim.autenrieth, dominic.schupke}@siemens.com

***Abstract* –In this paper we present and compare different multilayer protection mechanisms which enable the client to protect its connections against dual failures in the server layer. In multilayer networks based on overlay or augmented model, the client is not aware of the routing information of the server layer. Therefore, some resilience mechanisms need new functions that have to be provided by the User Network Interface (UNI). Based on generic building blocks for surviving dual failures we propose four multilayer protection models. We extend our existing simulation software for analyzing resilience options and evaluate the selected operation scenarios.**

I. Introduction

The introduction of automated connection control in optical transport networks using ASON (Automatically Switched Optical Networks) [1] or GMPLS (Generalized Multi-Protocol Label Switching) [2] together with the standardization of interfaces like UNI (User Network Interface) and NNI (Network Network Interface) will allow establishing connections immediately on customer demand. A network operator (e.g., an IP/MPLS network operator) as customer can adapt the capacity of the network to the actual load pattern. It is also possible that this network operator does not even own the transport network infrastructure, but dynamically leases it based on online offers of competing suppliers.

The challenge is to automate the bandwidth adaptation process of the client network with the target of a stable, cost-efficient and dynamic network. In this paper, we focus on how the client network can provide highly available services. For these services, resilience mechanisms have to respond not only to single failures, but also to dual failures. The problem is that the client does not know anything about the routing and diversity of the lightpaths in the server layer. Previous literature considers dual failure recovery in the scope of single layers [3][4][5]. An introduction to multilayer resilience is given in [6], and a multilayer traffic engineering scheme using dynamic restoration is presented in [7]. In this paper the resilience concepts against double failures and for multiple layers are used in combination with the dynamic multilayer routing strategy published in [8] to achieve a high restorability against double failures in multilayer network.

The paper is organized as follows. Section II summarizes the multilayer architecture. Section III identifies building blocks from which we can provide multilayer protection. In Section IV we propose a set of multilayer models for protection against multiple failures. Section V describes our simulation architecture to evaluate these models. For several case studies, specified in Section VI, we show results in Section VII. In Section VIII, we draw conclusions and give an outlook.

II. Multilayer Architecture

In this paper, we assume a two-layer network model. The client layer is connected via UNIs to the OTN network (see Figure 1). The control planes of both layers exchange no information (overlay model) or only sparse information (augmented model) about the current routing and resource usage.

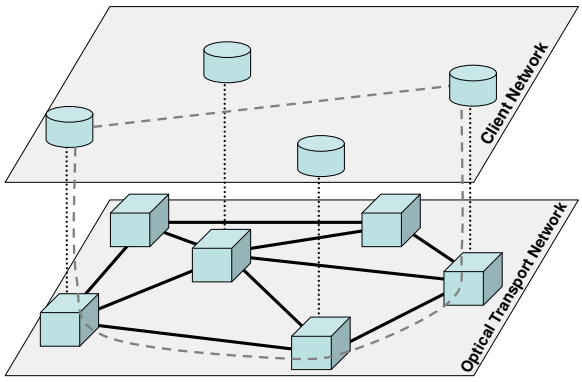

Figure 1 - Network Architecture

The client layer can request new link capacities on demand from the OTN-provider dynamically, using the UNI. Thus, the main concept of the client is to adjust the link resources automatically and cost-efficiently depending on the current demand.

In [8] a multilayer routing strategy is presented with dynamic link resource adaptation. For this work, we extend this model to provide resilience against multiple failures.

III. BUILDING BLOCKS

We identify three types of building blocks, which help us to develop different multilayer protection schemes.

The first building block type represents the possibilities how to handle double failures. Considering highly available connections, we assume that each connection should always use a 1+1/1:1 protection to survive all single failures. To survive additionally double failures we consider three cases:

- Introducing a 1+1+1 protection with three pairwise disjointly routed paths (see Figure 2a)
- Using a reprovisioning after a first failure is on the working or on the backup path (see Figure 2b)
- Using a restoration mechanism after working and protection path are affected by failures. (see Figure 2c)

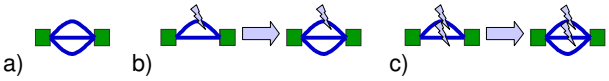

Figure 2 - Double Failure protection schemes,
a) 1+1+1 protection, b) 1+1+reprovisioning after first failure. c) 1+1 protection with restoration after second failure

The second building block type decides in which domain the signal is doubled (1+1 protection) or switched (1:1 shared protection). If this is done in the electrical domain (Figure 3 left), two interfaces are required between the electrical (client) and the optical layer. Otherwise, if this is done in the optical domain (Figure 3 middle and right), only one interface is necessary. This reduces costs but introduces a new single point of failure. This is acceptable if the interface between the electrical and optical domain has a very high availability (inside a well-protected building)..

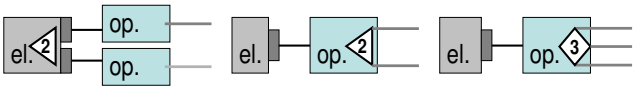

Figure 3 - Signal doubling in the electrical domain (left) and in the optical domain (middle) and signal tripling in the optical domain (right).

The multilayer model defines the third building block. It distinguishes if either protected client links (e.g., using server layer path protection) or client path protection is used. In case of protected client links (see Figure 4 left), the protection can be provided in the client layer as well as in the optical layer. In contrast, client path protection must be controlled by the client layer. For this purpose, the client control plane needs information about the disjointness of its client links.

IV. MULTILAYER PROTECTION MODELS

In the following four subsections, we present different multilayer protection mechanisms, which can survive dual server link failures. Therefore, we use the building blocks defined in the previous section.

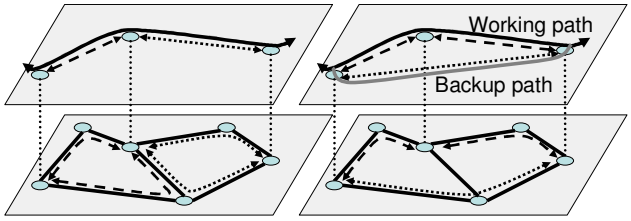

Figure 4 – Protected client links (left) and client path protection (right).

A. *Client link protected by OTN*

This most straightforward mechanism is a single layer protection in the OTN layer without any multilayer interactions. Each client link is represented by three pairwise disjointly routed server paths (see Figure 5). If one or two of these paths are affected by failures, the client link is still available. This mechanism can guarantee to survive dual server link failures if three pairwise disjoint paths with enough capacity can be found for every client link (otherwise it will be blocked). This very fast protection mechanism will occupy many resources even in the failure free status.

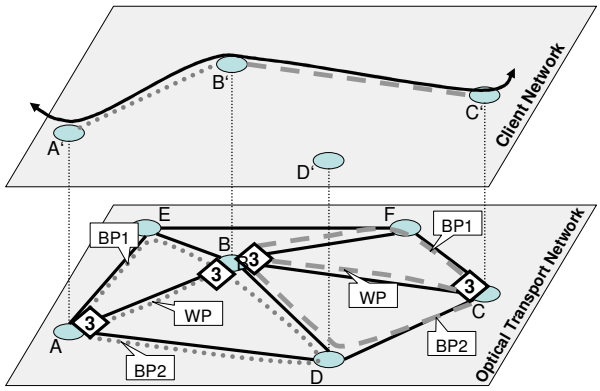

Figure 5 - Client link protected by OTN

In Figure 5 the client link protection by OTN is shown as an example. The client connection runs from node A' via B' to C'. The two virtual client links A'-B' and B'-C' are each protected in the server layer by tripling the signal. This is indicated in the figure using the symbol ③. Each virtual client link is transported by a working path (WP) and two disjointly routed backup paths (BP1 and BP2) in the OTN-layer. In case of shared protection, the resources of both second backup paths can be shared on fiber BD.

For instance, the working path (WP) A-B of the client link A'-B' is protected by the backup path 1 (BP1) from A via E to B, and backup path 2 (BP2) is running from A via D to B. For link protection in the server layer, either 1+1+ protection, 1:1:1, or 1+1:1 protection is possible. However, as the calculation of the shareable protection links is very complex for 1:1:1 scenario, we propose a 1+1:1 protection. For instance, the two BP2 in Figure 5 can share the resources on link B-D.

B. Client link protected by OTN with client path restoration after second failure

In contrast to the mechanism of the previous subsection in this case the client link is protected against single server layer link failures only. If a second failure disconnects a client link, the client layer will request a new client link on demand (not necessarily the same link again) to restore the affected traffic of the client layer (see Figure 6). This behavior leads to relative long outage times in case of dual server link failures. In networks with dynamic traffic and limited resources in the OTN layer a 100% protection against dual server link failures cannot be guaranteed.

In the upper part of Figure 6 each client link is routed in the OTN layer on 1+1 protected paths (⧋). In case of a client link failure due to a double failure in the OTN-layer, the client layer tries to reroute the affected client traffic on alternative links. If not enough resources are available in the client network, the client layer can request additional (protected) links from the server layer. In the figure, the virtual client link A'-D' is added.

To reduce additional impact on the services we propose in this case a non-revertive operation of the restoration mechanism after the second failure. As a consequence, we propose a stub release of unused links. E.g., if no other demand is traversing the link A'-B' in Figure 6, this link can be released after the restoration.

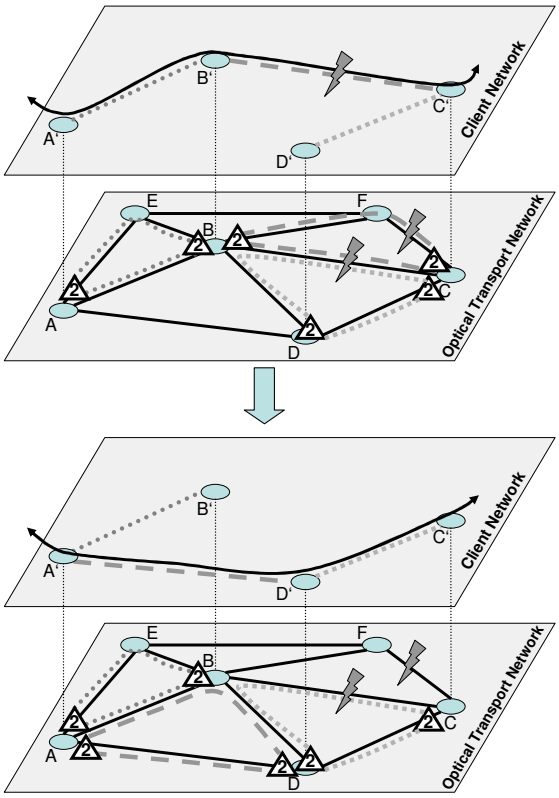

Figure 6 - Client link protected by OTN with redial after second failure

Non-revertive restoration can cause slow deterioration of the network state, since it moves services to longer paths. A periodic mechanism re-optimizing the network can resolve this deterioration. If no other client traffic is running over link A'-B', this link can be released to reduce costs.

C. Client link protected by OTN with additional client-layer path protection after first failure

Now, we aim to avoid the service outage time that the previous mechanism can exhibit after dual server link failures. In the following mechanism, the client will be notified from the OTN after a first failure. With the notify message the client is informed which client links are now unprotected. The server layer generates an identifier for the remaining lightpath of every affected client link and attaches them to the notify message.

The client then tries to find protection paths for all connections routed on the vulnerable client links, by using the unaffected client links. If enough resources are not available, the client can setup new auxiliary client links.

With the identifiers of the remaining lightpaths, the client can setup an unprotected new client link, which is disjoint to these ligthpaths in the server layer. A client protection path can use only an auxiliary client link if it is disjointly routed to all vulnerable links of the corresponding working path in the server layer.

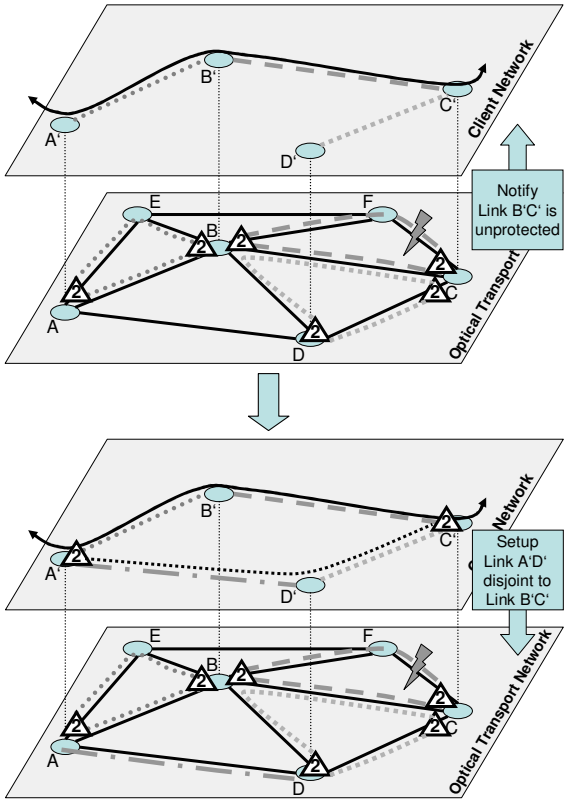

Figure 7 - Client link protected by OTN with additional client-layer protection after first failure

Figure 7 illustrates this case. Each client link (A'-B', B'-C, and C'-D') is routed in the OTN layer on 1+1 protected paths. In case of an OTN-link failure the client is notified via the UNI interface (upper part).

The client can then request the setup of a new unprotected client link to establish a client layer protection path while the client working path is unprotected.

In this case a revertive operation is proposed, as the client layer protection path is established before a secondary failure occurs. The client layer has to be notified, when the original link is again protected. Then the client protection path can be released, and subsequently any unused virtual links unused can also be released.

As in the previous mechanism, it cannot be guaranteed to protect the client traffic fully against dual server link failures, if dynamic traffic is assumed and the OTN layer resources are limited.

D. Client path protection enabled by SRLG information provided by the OTN

The last mechanism is a pure client connection protection. The OTN does not provide any resilience scheme. Each virtual client link, which represents a path through the server layer, gets a shared risk link group (SRLG) identifier by a UNI-function. This identifier allows the client network to find out which client links are routed disjointly in the server layer. The client can request new client links which are routed disjointly to existing client links in the server layer by attaching their SRLG identifiers to the setup message. In the failure-free state, the connections are protected with 1:1 protection, which is reprovisioned after a first failure.

Due to the finer granularity of the client connections, we expect that this mechanism will have the smallest capacity usage compared to the mechanisms presented in the subsections before. The SRLG identifiers are sparse information of the routing in the server layer, thus this mechanism can be used in augmented model multilayer architectures. However, again, it cannot be guaranteed to protect the client traffic fully against dual server link failures, if dynamic traffic is assumed and the OTN layer resources are limited.

In the example of Figure 8, each client connection is protected in the client layer (1:1 protection with reprovisioning after the first link failure). For this, the OTN provides information about the disjointness with SRLG identifiers. In the example, the SRLG identifiers are the product of the SRLG identifiers of the used server links. Each server link has a unique identifier. Two client links are routed disjointly in the server layer, if their identifiers have no common divisor greater than one.

In this case, a stub release of the original client path stubs and the unused client links is proposed to free network resources during the failure situation. If the client layer is informed about the repair of the failed link, a revertive operation may be used.

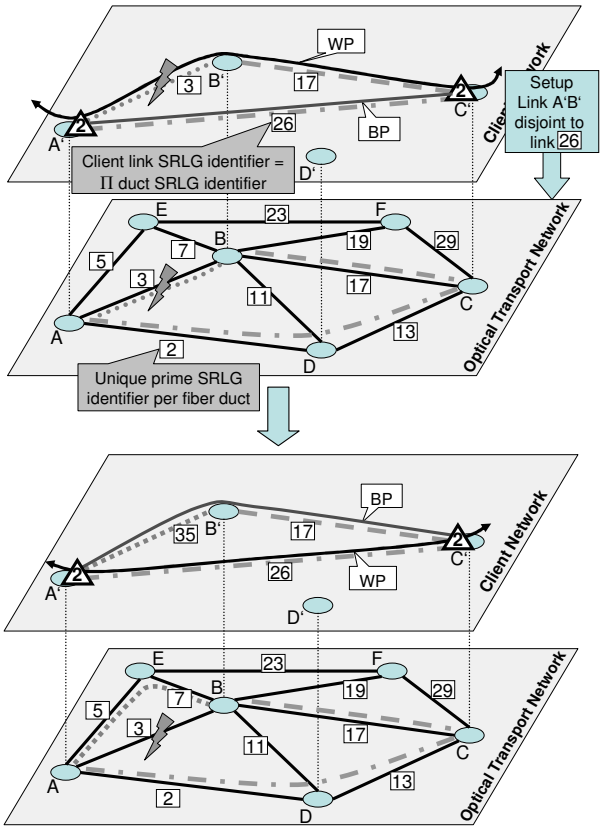

Figure 8 -. Client link protected by OTN with additional client-layer protection after first failure

E. Overview of Multilayer Protection Models

Table I gives an overview over the proposed multilayer protection models and their characteristics. Using the simulation environment presented in the next section, we investigated these models with the case studies introduced in Section VI.

TABLE I – MULTILAYER PROTECTION MODELS

Model	First failure	Second failure	Proactive (second failure)	Reactive (second failure)	Double Failure Restorability	Stub-release
A	dedicated optical path protection	dedicated / shared optical protection path	in failure free state		100%	-
B	dedicated optical path protection	restoration		After second failure	<= 100%	Yes
C	dedicated optical path protection	dedicated client protection path	after first failure		<= 100%	No
D	dedicated / shared client path protection	dedicated / shared client path protection	after first failure		<= 100%	Yes

V. Simulation Software

To compare the presented multilayer protection mechanisms we extend the simulation software used in [8]. An overview of the software architecture is shown in Figure 9. The software is written in C++, using a multilayer graph library (GRAPH), an event based simulation library (CNCL) and an optimization library (ILOG CPLEX Concert).

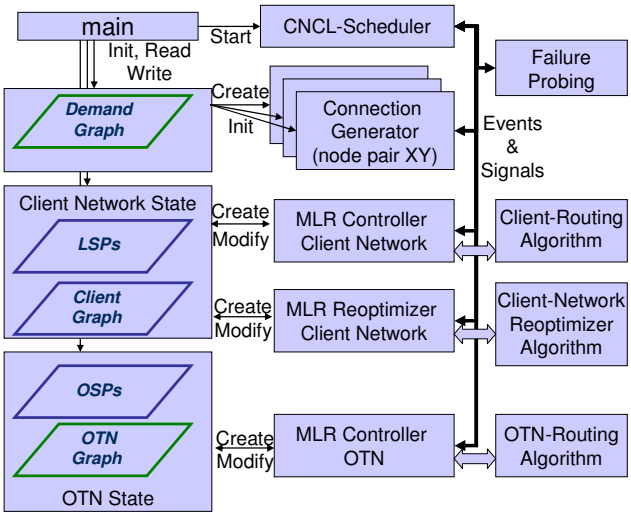

Figure 9 - Structure of our simulation software

All details about the network, e.g. current resources or current connections, are handled in the relating network state (Client Network State and OTN State). For every demand relation in the demand graph, a connection generator generates the corresponding client traffic. We assume connection oriented traffic in the client network (e.g GMPLS traffic). Modeling MPLS virtual private network (VPN) connections, the traffic is assumed to be Poisson distributed with negative exponential distributed service times. All bidirectional connections have the same bit rate b, the same mean service time s, and the same traffic scaling factor x. With the given traffic intensity A_{st} of a node pair st the mean inter arrival time i_{st} can be calculated with equation (1):

$$i_{st} = \frac{s}{x \cdot A_{st}} \tag{1}$$

Setting up or releasing client traffic as well as requesting new client resources is handled by the Multi-Layer Resilient (MLR) controller of the client network. To route the traffic in the client network, the controller uses a routing algorithm which is described in the next section.

To ensure that the client network will not run in inefficient resource consumption, we use a reoptimization as described in [8]. The reoptimization tries to improve the efficiency by rerouting the client traffic, defragmenting parallel client links, and releasing of unused resources. This process is invoked periodically and uses a mixed integer linear program (MILP).

The MLR controller of the OTN handles the bidirectional optical switched paths (OSPs) and routes them depending on the used OTN routing algorithm, which is again described for every case study in the next section. Every OSP has the same capacity, which is a multiple of the client connections bit rate.

To fairly analyze the different approaches of the previous section, we introduce a failure probing mechanism. The simulator makes in equidistant time intervals a snapshot of the current network states. These snapshots are then analyzed depending on the current case study (see next chapter) in a second process.

All the signals and events used in the simulation are managed by the CNCL-Scheduler. To ensure confident results, the simulator stops if the relative Bayes error of all the estimated mean values that are determined is smaller than an assigned value. For this we calculate for every time interval an average of every investigated value. The statistical evaluation of these values is then done by the Batch-Means method, which is included in the CNCL library (CNBatch-Means).

VI. Performed Case Studies

For our case studies we use the pan-European network from the COST239 project [9] (see Figure 10). We assume that all fibers have enough capacity, such that no blocking will occur.

The cost of a lightpath is the sum of the cost of the fibers traversed by it, which is here the fiber length. These values are shown in the upper right part of Table II. The lower left part of this table displays the used traffic intensity values for generating the bidirectional connections.

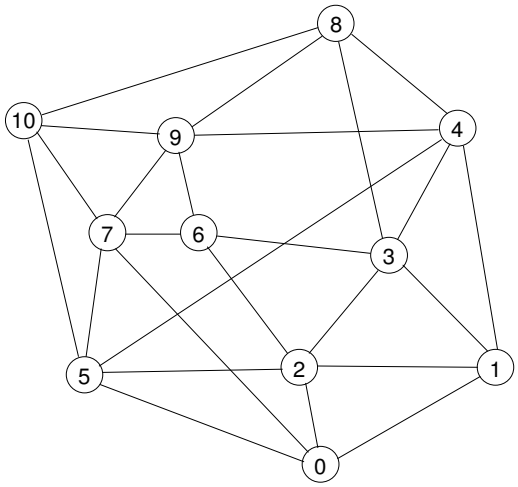

Figure 10 - COST239 Network

TABLE II - BIDIRECTIONAL DEMAND MATRIX (TRAFFIC INTENSITY) AND COST OF A WAVELENGTH IN THE OTN FIBERS.

Node	0	1	2	3	4	5	6	7	8	9	10	Cost of a used wavelength on a fiber
0		820	320			820		930				
1	12.5		730	320	660							
2	15	15		565		600	350					
3	2.5	2.5	2.5		340		730		740			
4	5	7.5	7.5	2.5		1090			390	660		
5	27.5	22.5	27.5	5	22.5			300			450	
6	12.5	5	7.5	2.5	2.5	20		220		390		
7	2.5	2.5	2.5	2.5	2.5	5	2.5			210	390	
8	17.5	5	15	2.5	2.5	15	10	2.5		760	1310	
9	25	7.5	7.5	2.5	5	20	12.5	2.5	10		550	
10	2.5	2.5	2.5	2.5	2.5	7.5	2.5	2.5	2.5	2.5		
	Bidirectional demand matrix (traffic intensity)											

We consider a future scenario where a client network provider offers an on-demand Gigabit Ethernet service (1 Gbit/s). For this, the client uses GMPLS and leases resources from an OTN provider with a granularity of 10 Gbit/s. Thus, we assume that a client link can carry 10 client connections. The mean service time of a client connection is 30 days. The client network provider reoptimizes his network every 10 days.

To see the dependency of the client traffic we scale the traffic by a factor between 0.1 and 1. The simulation starts with an empty client network. To avoid transient conditions at the beginning of a simulation and to have steady-state conditions we start recording data for the statistical evaluation after an initialization period of 200 simulated days. We collect statistical data for following paramters:

- The leasing cost of the client network
- The number of leased client links
- The number of client connections
- The relative client network load
- The number of used wavelengths channels on every fiber duct

The simulation is stopped if the relative Bayes error of the mean values of these parameters is smaller than 5%.

To route a new client connection we use a Dijkstra algorithm which finds the path through the fully meshed client network with the smallest sum of cost *c'* of every used client link. The cost *c'* of a client link is dependent on its current state. We calculate the cost $c'_{i,np}$ of a client link with id *i* between node pair *np* by equation (2):

$$c'_{i,np} = \begin{cases} 0.1 \cdot c_{np} + (1 - l_i) & \text{if link } i \text{ between node pair } np \text{ has free capacity} \\ c_{np} & \text{if no link with free capacity exist between node pair } np \\ \infty & \text{otherwise} \end{cases} \quad (2)$$

The relative load l_i of the link with id *i* can have a value between 0 and 0.9. Hence, if there exist parallel links with free capacity between node pair *np*, the Dijkstra algorithm prefers with the term $(1-l_i)$ in equation (2), the link with the highest load. We use this to reduce the fragmentation of parallel links. The value c_{np} in equation (2) is the leasing cost of a client link between the node pair *np*. This leasing cost is dependent on the considered case study (see next section). If the path found by the Dijkstra algorithm uses non-existing or fully loaded links, we setup new client links there.

For our investigations we define 4 different case studies:

CASE1: Client link protected by OTN with a 1+1+1 protection (see section IV.A).

CASE2: Client link protected by OTN with a 1+1:1 protection with shared second backup paths (see section IV.A).

CASE3: Client link protected by OTN with 1+1 protection with restoration after a double failure (see section IV.B). Both networks use stub release.

CASE4: Client link protected by OTN with 1+1 protection with additional client-layer protection after first failure (see section 0). Both networks use no stub release.

The augmented model approach in Section IV.D is not included in the results and is for further investigation.

Depending on the performed case study, the OTN routing algorithm (see Figure 9) returns:

- in CASE1 the three shortest disjoint paths. The shortest one is used as the working path and the others are used as backup paths. The leasing cost of the related client link c_{np} is the total length of the tree paths.
- in CASE2 the three shortest disjoint paths. The shortest one is used as the working path, the next shortest as the first backup path and the third path is used as the second backup path, which is shared. The leasing cost of the related client link c_{np} is the sum of the working and the first backup path lengths.
- in CASE3 and CASE4 the two shortest disjoint paths. The shortest one is used as the working path and the other as backup path. The leasing cost of the related client link c_{np} is the total length of the two paths.

The current sharing capacity sc_f on a fiber *f* and, with it, the additional leasing cost *slc* for the client network in CASE2 are calculated as follows:

We test all double fiber duct failure scenarios. The current sharing capacity sc_f is the maximum number of used second backup paths on fiber *f*. The additional leasing cost *slc* for the client network is the sum of sc_f weighted with the

fiber length over all fibers. Every time the OTN state changes, the sharing capacity will be recalculated.

To compare the four case studies with respect to double failures we need a failure probing in CASE3 and CASE4. In these two cases the capacity requirements of the OTN network rises with a single failure in CASE4 and with a double failure in CASE3. As double failures are rare events, and in order to evaluate all possible failure scenarios, in the simulator the failures are not generated by a random process, but by systematically generating all possible failure scenarios after given periodic time intervals.

For this, the simulator makes every seven simulated days a snapshot of the current client network and of the OTN. With these snapshots, a second process calculates the current capacity requirements to the OTN depending on the case study:

- In CASE3, we minimize for every double failure scenario the resulting leasing cost with a MILP.
- In CASE4, we minimize for every single failure scenario the resulting leasing cost with a MILP.

To limit the computing time of the optimizations we restrict the solution by defining only a limited set of suitable paths for the solution.

VII. Discussion of Results

In the following, we exemplify the kind of results the simulator can produce and draw several first conclusions comparing the case studies.

Figure 11 depicts the mean leasing costs over the traffic scaling factor for CASE1 to 4. For CASE3 and CASE4, failure probing is deactivated here. In all cases, the cost increases linearly with the traffic, as expected from the cost model

CASE1 has the highest cost, because of the extensive protection capacity need in the OTN. CASE2 performs better by making use of OTN capacity sharing. Costs are approximately 80% of the CASE1 costs.

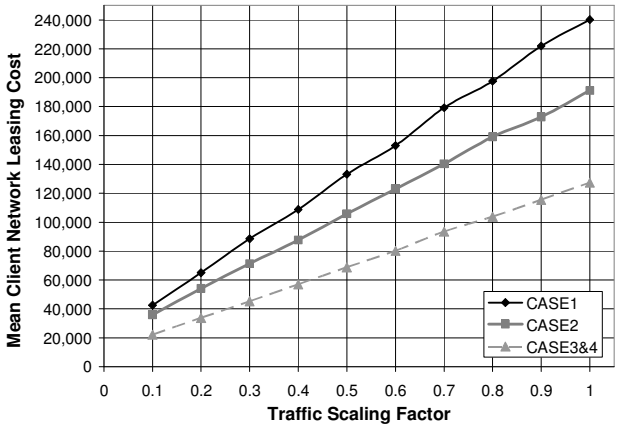

Figure 11 - Mean leasing costs over traffic scaling factor

The cost for CASE3&4 is about half of CASE1, however, without considering failure events. Hence, the CASE3&4 curve in Figure 11 represents the base cost, and cost for protecting capacity has to be added in failure events. Therefore, an immediate advantage of CASE3&4 is that the client network operator needs only to demand more OTN capacity when failure events occur. The cost for protecting capacity becomes apparent only during client-affecting failures, and not implicitly from the beginning of a demanded OTN service to its end (as in CASE1&2). At the same time, costs stay at low levels during normal operation for CASE3&4.

Figure 12 shows the relative load in the client network as function of the traffic scaling factor. As the client requests capacity from the OTN as needed, the client network capacity varies, thus, the load is not only dependent on the traffic, but also on the capacity. We see in Figure 12 that the client reaches high load values of 60% to 90%, thus always utilizing the (dynamic) capacity to a great degree. All cases follow this desired behavior. The small variations among them can be explained by different cost values between the node pairs, e.g., while the cost for node pair A-B is higher than for C-D for CASE2, the cost relation can be vice versa for CASE3. Thus, the client's overall route selection, that bases on these cost values, can be different in the set of cases.

Furthermore, the figure shows that with higher traffic volume the load becomes also higher, which is due to the economy-of-scale effect that is still valid for (dynamic) capacity. Note that if the client installed as much static capacity as needed in the 100% traffic scaling scale, the load would be much lower for the lower scaling values.

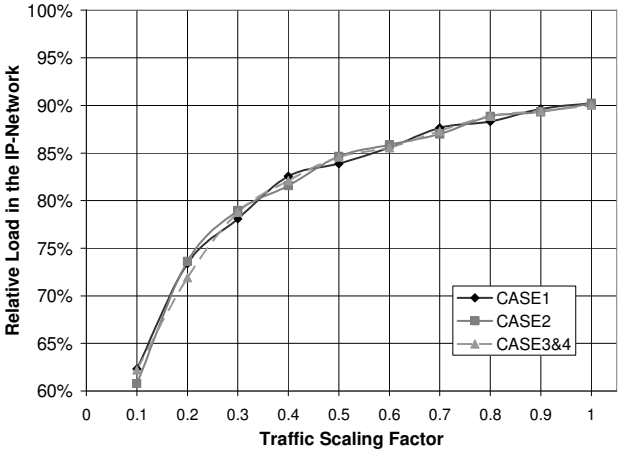

Figure 12 - Relative load in the client network over traffic scaling factor

During the simulations, we also measured the maximum occurring number of wavelengths needed per fiber. The sum over all fibers of these maxima is depicted in Figure 13. Hence, if the OTN operator installs the depicted capacity values, the OTN incurs no blocking events in the corresponding simulation run. Without failure probing, all

cases qualitatively follow the cost curves in Figure 11. With failure probing, however, CASE3&4 are in the region of CASE2. Thus, the operator sees the same maximum capacity here. If, under the no-blocking paradigm, the operator has to invest in the same capacity for CASE2-4, other criteria (as operational simplicity) matter when selecting among the architectures underlying these three cases.

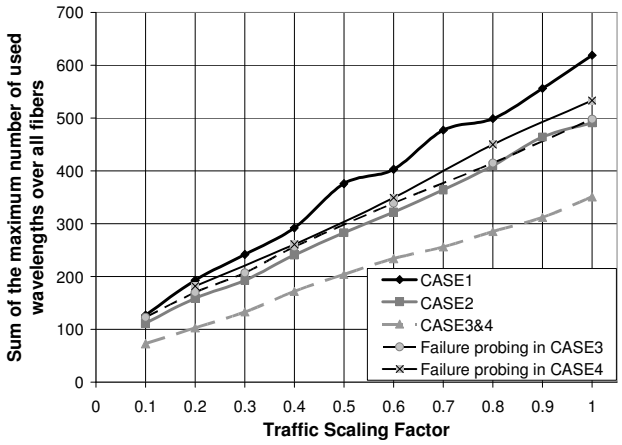

Figure 13 - Sum of the maximum number of used wavelengths over all fibers

VIII. CONCLUSION

In this paper we propose and discuss novel multilayer protection schemes surviving dual server layer failures based on overlay and augmented model architectures. Using simulation, we compare them to the straight forward approach of deploying 1+1+1 protection and 1+1:1 shared protection in the OTN. In a failure-free situation, the cost of the 1+1+1 reference scenario is about double the cost of the proposed mechanisms. Using on-demand protection paths to provide resilience against double failures, the additional resources must only be provided (or leased) during the first failure or during double failure scenarios, depending on the double failure protection model. Although on-demand protection reaches about the same cost levels as 1+1:1 shared protection during dual failures, this cost only occurs while these (infrequent) failure situations occur. As the maximum capacity requirements of all models are in the same order, future investigations will be focused on the impact of the used method to the restoration times for the first and the second server layer failure.

REFERENCES

[1] *ITU-T Rec. G8080/Y.1304*, "Architecture for the Automatically switched Optical Network (ASON)," November 2001

[2] E. Mannie, "Generalized Multi-Protocol Label Switching (GMPLS) Architecture," *RFC3945*, October 2004

[3] W. D. Grover, "Mesh-based Survivable Networks: Options and Strategies for Optical, MPLS, SONET and ATM Networking," Prentice Hall, Upper Saddle River, 2003.

[4] Schupke, D.A.; Autenrieth, A.; Fischer, T., "Survivability of Multiple Fiber Duct Failures," *Third International Workshop on the Design of Reliable Communication Networks (DRCN)*, Budapest, Hungary, October 2001.

[5] D. A. Schupke and R. G. Prinz, "Capacity Efficiency and Restorability of Path Protection and Rerouting in WDM Networks Subject to Dual Failures," Photonic Network Communications, Journal, Kluwer Academic Publishers, 8(2):191-207, September 2004.

[6] P. Demeester, M. Gryseels, A. Autenrieth, et al., "Resilience in multilayer networks. IEEE Communications Magazine, 37(8):70–76, August 1999.

[7] B. Puype, Q. Yan, D. Colle, et al., "Resilient multilayer traffic engineering through dynamic path restoration - Survivable data-centric automatic switched optical networks," *Optical Network Design and Modelling (ONDM 2004)*, Gent, Belgium, 2-4 February 2004, pp. 327-342

[8] Prinz, R.G.; Iselt, A, "A Multilayer-Routing-Strategy with Dynamic Link Resource Adaptation," *Optical Network s & Technologies Conference (OpNeTec)*, Pisa, Italy, October 2004.

[9] P. Batchelor et al., "Ultra High capacity optical transmission networks: Final report of action COST239," in *Faculty of Electrical Engineering and Computing*, Zagreb, 1999.