Konrad-Zuse-Zentrum
für Informationstechnik Berlin

Takustraße 7
D-14195 Berlin-Dahlem
Germany

RALF HÜLSERMANN
MONIKA JÄGER
ARIE M.C.A. KOSTER
SEBASTIAN ORLOWSKI
ROLAND WESSÄLY
ADRIAN ZYMOLKA

Availability and Cost Based Evaluation of Demand-wise Shared Protection

ZIB-Report 06–15 (March 2006)

Availability and Cost Based Evaluation of Demand-wise Shared Protection

Ralf Hülsermann[1], Monika Jäger[1], Arie M. C. A. Koster[2], Sebastian Orlowski[2], Roland Wessäly[3], Adrian Zymolka[2]

[1] T-Systems Enterprise Services GmbH, Goslarer Ufer 35, D-10589 Berlin, e-mail: {ralf.huelsermann, monika.jaeger}@t-systems.com
[2] Zuse Institute Berlin (ZIB), Takustr. 7, D-14195 Berlin, e-mail: {koster, orlowski, zymolka}@zib.de
[3] atesio GmbH, Sophie-Taeuber-Arp-Weg 27, D-12205 Berlin, e-mail: wessaely@atesio.de

Abstract

In this paper, we investigate the connection availabilities for the new protection scheme Demand-wise Shared Protection (DSP) and describe an appropriate approach for their computation. The exemplary case study on two realistic network scenarios shows that in most cases the availabilities for DSP are comparable with that for 1+1 path protection and better than in case of shared path protection.

1 Introduction

Network and service availability is one of the major requirements of modern telecommunication networks. A service or a connection gets unavailable as soon as one of the dedicated network components becomes unavailable, e.g., by a failure or defect. Several protection and restoration mechanisms make use of redundant network backup capacity to ensure service connectivity in case of network element or network link failures. Network complexity, cost of network configuration, recovery times, and the level of network availability are important issues for network providers when choosing an appropriate resilience mechanism.

Dedicated protection mechanisms like SDH 1+1 protection are widely deployed in present transport networks. These concepts can be easily handled with the use of centralized network management systems, ensure fast service recovery times, and provide a high level of service availability. On the other hand, they require a huge amount of redundant network capacity, making the resulting network configuration rather expensive. Shared protection mechanisms are able to share network backup resources between connections with disjoint working paths and can help to reduce the network costs. Thereby, the complexity of network operation and the service recovery time increase as the backup path establishment has to happen after the failure occurrence. Furthermore, the service availability in case of multiple network element failures decreases as concurrent access to shared backup resources occurs in specific failure scenarios.

In [8] and [12], two different models for the new survivability concept Demand-wise Shared Protection (DSP) have been introduced. DSP can be applied to connection-oriented services in different network layers and network technologies (MPLS, SDH, Ethernet, DWDM) and has the potential to combine the main advantages of dedicated and shared protection:

- good bandwidth efficiency and reduced network cost
- fast service recovery
- low configuration / operation complexity
- assurance of service recovery for all single failures
- high service availability in case of multiple failures

The main purpose of this paper is to compare the cost efficiency and the service availability for different versions of DSP, 1+1 path protection, and shared path protection. In section 4, we show that DSP can reduce the network cost on average by about 10% whilst the network availability for protected connections is in the same range as in case of 1+1 protection.

This paper is organized as follows. In section 2, we describe the functionality of the different resilience mechanisms under investigation and summarize their characteristics. In section 3, we present the used analytic methods and algorithms to calculate the service availabilities for each resilience strategy. A computational comparison of the cost and bandwidth requirements as well as of the network availability of the different concepts is described in section 4. Our conclusions are summarized in section 5.

2 Protection Mechanisms

In this section, the three resilience concepts used in the case study are defined: dedicated path protection, shared path protection, and Demand-wise Shared Protection (DSP). Furthermore, the applied methods for

routing paths and assigning network capacity are briefly described. Finally, a short discussion of the properties and a qualitative comparison of the survivability concepts are given.
In the sequel, a demand refers to a requirement for a number of connections d to be established between two nodes in the network of which d^* has to be protected against single network failures. For each demand, the connections can be routed independently from each other.

2.1 1+1 Dedicated Path Protection

To ensure service connectivity in case of single network element failures, two link- or node disjoint paths (depending on planning requirements) are set up for 1+1 dedicated path protection. The signal is broadcasted over both the working and the backup path simultaneously. In case of a failure, the receiving terminal performs the protection switch between the two signals based purely on local information about the signal quality.
Figure 1 depicts an example configuration of two demands protected by 1+1 protection. Both demands, F-N and F-H, are routed along two node-disjoint paths. It is obvious that in minimum twice the amount of network capacity is needed to transport the traffic demand as in the unprotected case. Dedicated protection is able to survive any single failure scenario and provides a high level of connection availability in case of multiple network element failures. The service recovery time is very fast, typically in the range of 50ms as only local switching at the receiver site is needed which can be done automatically. Dedicated path protection is quite simple in network operation. The configuration and setup can be done via the network management system. Once the service is in operation, the two paths need not be touched any more [1].

2.2 Shared Path Protection

If working paths are fully disjoint, sharing of backup resources is possible. Depending on the network topology, the traffic demand, and the applied network planning and optimization strategy, resource reductions of more than 30% are possible [4][9].
In Figure 2, the demand between F and H uses the working path F-H and the backup path F-L-H. The demand between F and N is routed along working path F-N and backup path F-L-N. Since the demands have just to be protected against single link or node failures, sharing of backup capacity is possible on link F-L. In the failure-free state, the signal is send over the working path only. A failure along the working path has to be notified and signaled. Due to sharing resources, the cross-connection of the backup path has to be done after occurrence of a failure. By this, the service recovery time is much longer than in case of dedicated protection. Shared path protection ensures connection availability in case of any failure scenario which was considered in the planning phase (i.e., single link or node failures). In case of multiple failure scenarios, the service availability is reduced compared to dedicated protection as concurrent access to shared backup capacity occurs if connections with common backup resources are affected simultaneously. Moreover, shared path protection is more complex in network operation than dedicated protection. Some kind of signaling is needed for failure notification and backup path implementation. Once the failure is repaired, the connection should usually be switched back on the working path, or the backup resources have to be planned and assigned newly.

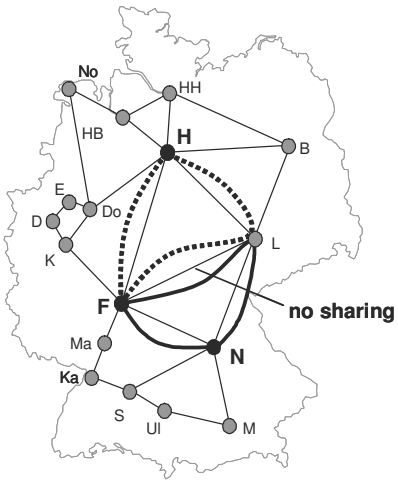

Figure 1: Example of a path configuration for 1+1 dedicated path protection

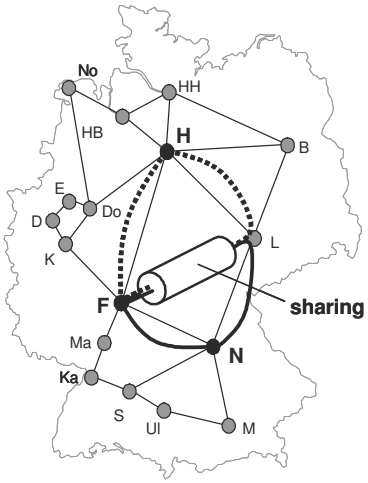

Figure 2: Example of a path configuration for shared path protection

2.3 Demand-wise Shared Protection

From a network operator's point of view, a survivable routing must just fulfill two basic requirements: For each demand,

- the working traffic has to be satisfied in the failure-free network state, and
- in any considered failure state, the specified fraction of the demand must survive.

With DSP, a number of paths is pre-established for each demand such that the above requirements hold. This number is at least the required demand value to enable routing in the failure-free network state and might involve additional connections for providing protection. Moreover, the concept bases on a routing scheme called diversification [3][13] which aims at spreading the complete routing of a demand over several different paths. The routing is carried out such that in each failure state at least the specified portion of the paths survives. DSP does not dedicate paths to be exclusively for working or backup traffic.

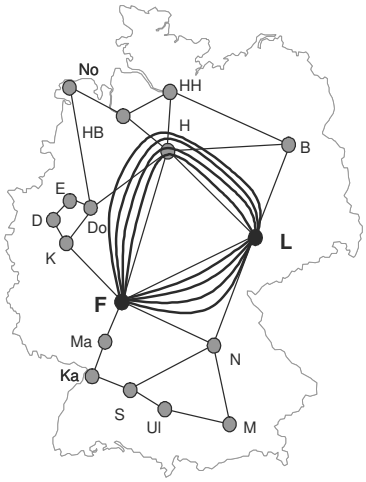

Figure 3: Example of a 1+1 routing with 8 paths

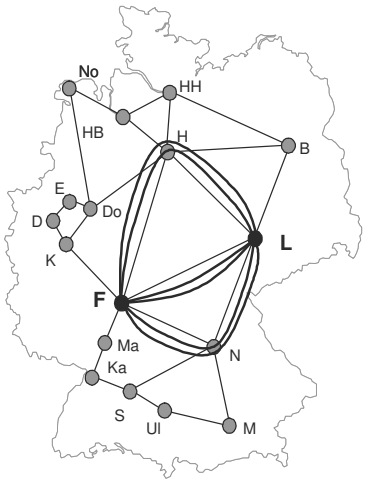

Figure 4: Example of a DSP routing with 6 paths

A comparison of a 1+1 routing and an admissible DSP configuration is depicted in Figure 3 and Figure 4 where four demand units have to be routed between F and L with full protection against single link or node failures. Figure 3 shows a 1+1 protection routing, leading to a total of eight paths (e.g. lightpaths in WDM or VC-n paths in SDH) and an occupied network capacity of 12 [capacity-units·hops]. Figure 4 illustrates a possible DSP routing with six paths and a necessary network capacity of 10. At least four paths survive a single link failure or outage of a transit-node.

In a first version of DSP [8], the number of paths to establish in total for a demand is pre-determined based on connectivity arguments and given as an input value to the network optimization. Two cases have been considered: (i) exploration of the maximum node-connectivity between every pair of nodes (*maxconn*), which minimizes the total number of paths to establish, and (ii) exploration of the node-connectivity two between every pair of nodes (*2conn*), which requires more paths, but enables shorter routes to choose. Both variants form special cases of the extended DSP variant [12]. In this general case, the two basic requirements are explicitly formulated as linear inequalities. This way, both the total number of paths to be established and their routing are part of the optimization (and thus can be determined to best benefit from the entire network's perspective).

2.4 Discussion

DSP combines advantages of dedicated and shared path protection with each other. Backup capacity is *dedicated* to each particular demand, but *shared* within the demand. This way of capacity sharing can reduce the total network capacity and network cost compared to purely dedicated protection. However, the sharing possibilities are restricted compared to shared path protection since capacity is only shared between working paths of the same demand. Thus, the capacity requirements of DSP are bounded from above by 1+1 dedicated path protection and from below by shared path protection. Furthermore, DSP shares capacity always in an end-to-end manner which allows to pre-establish and cross-connect all paths in advance. As a consequence, paths need not to be set up in case of a failure. Thus, the recovery times are faster and the operational effort complexity is smaller than in case of shared path protection. Only a failure detection and backward signalization is needed before the traffic can be detoured to the surviving paths of the demand. Hence, DSP performs just local switching at the end nodes. As with dedicated protection, the interdependencies between working and backup path are limited to individual demands which helps to improve the network scalability. DSP is designed to guarantee service availability for any specified fraction of demand in any considered failure state. It can easily be extended to take also multiple failures into account. However, for reasons of comparison, we apply it for

protection against single link and node failures. Nevertheless, in case of multiple network-element failures, the network availability is expected to be higher than in case of shared path protection as concurrent access of different demands to shared backup resources will not happen.

3 Connection Availability

3.1 Availability Related Measures

The availability of a path is determined by the availability of the used network components. Such components might be hardware like physical transmission links, interface cards, multiplexers, or switching nodes, as well as the control software of cross-connects or the network management system. The cycle of normal operation, element outage, element repair, and element recovery can be described by the *Mean Time Between Failure (MTBF)* (i.e. the average time between two occurrences of a failure in a discrete network element) and the *Mean Time To Repair (MTTR)* (i.e. the average time between element outage and element recovery).
The availability q of a network element is defined as the ratio of uptime and MTBF:

$$q = \frac{MTBF - MTTR}{MTBF}$$

The unavailability p of a network component indicates when the component is not available. It is defined as the complement of the availability:

$$p = 1 - q$$

In practice, a common alternative to *MTBF* is *Failures in Time (FIT)*, where the relation is given by

$$MTBF[h] = 10^9 / FIT$$

and MTBF is measured in hours. For optical transmission links, it is common to consider the *Cable-Cuts (CC)*, indicating the average cable length suffering from 1 cable-cut a year. See Section 4.1 for the numbers used in our case study.

3.2 Availability of 1+1 Dedicated Path Protection

The availabilities of network components are considered to be independent. Hence, the availability of a path can be calculated as the product of the availabilities of it's components:

$$q = q_{N_1} \cdot q_{L_1} \cdot q_{N_2} \cdot q_{L_2} \cdot q_{N_3} \cdot \ldots \cdot q_{N_k} \cdot q_{L_k} \cdot q_{N_{k+1}}$$

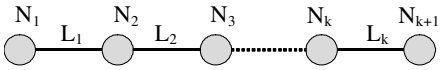

Figure 5: Serial configuration of components

If a connection is routed along several node-disjoint paths, the connection is available if one of the parallel paths is available. Stated otherwise, it is unavailable if all paths are unavailable. The unavailability of the parallel path configuration is defined as the product of the unavailabilities of the individual paths (without the end-nodes):

$$p_{parallel} = p_1 \cdot p_2 \cdot \cdots \cdot p_n$$

and

$$q_{AB} = q_A \cdot (1 - p_1 \cdot p_2 \cdot p_n) \cdot q_B$$

with A and B the end-nodes of the connection.

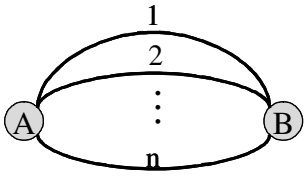

Figure 6: Parallel configuration of paths

3.3 Availability of Shared Path Protection

A simultaneous failure along working and backup path has to be taken into account when calculating the availability of shared path protection:

$$p_{ded} = p_w p_b$$

Additionally, a penalty for potential access-conflicts has to be considered. As mentioned above, such conflicts will happen for failing of working paths which have common backup resources. To quantify this penalty, we apply the method described in [7]. Under the assumption of independent failure events and binomially distributed failure number in a backup path sharing group (i.e., all working paths which use a specific common backup resource), the penalty can be approximated with:

$$p_{\text{penalty}} = p_w q_b \left(1 - q_w^{n_g - 1}\right) \cdot \left[1 - \frac{1}{2 + (n_g - 2)\, p_w}\right]$$

where n_g indicates the size of the backup path sharing group.
The sum of p_{ded} and the penalty is a lower bound for the unavailability of shared path protection since a potential reduction of the number of conflicts due to specific failure scenarios is not taken into account.

3.4 Availability of Demand-Wise Shared Protection

The calculation of the connection availability of DSP uses a straightforward methodology which is based on the calculation of conditional probabilities. The DSP routing for a specific demand forms a separate de-

mand-flow-graph which can be analyzed independently from the remaining parts of the network. A failure scenario is specified by the components that are up and those that are down in the demand-flow-graph. For each failure scenario i, the probability P_i the scenario arises is defined as the product of the availability of the components which are up and running, and of the unavailabilities of the components which are failing:

$$P_i = \prod_{j \in E_{down}} p_j \prod_{k \in E_{up}} q_k$$

where E_{down} includes all failed elements and E_{up} includes all elements which are in normal operation.

A demand of size d can be divided into two portions: The protected portion d^* which has to survive any single element failure and the unprotected portion $d-d^*$ which is not protected against failures. We calculate a separate availability for both portions.

For each failure scenario i, the number of surviving paths $n_{sp}(i)$ is counted. The product of the failure scenario probability and the surviving fraction of the demand is added to the availability $q_{d,i}$ of this demand:

$$q_{d,protected} = \sum_i P_i min\left(n_{sp}(i), d^*\right)$$

$$q_{d,unprotected} = \sum_i P_i max\left(0, min\left(n_{sp}(i) - d^*, d - d^*\right)\right)$$

The formula for calculating the availability for dedicated protection is a special case of this general methodology. The total number of scenarios is given by 2^k, where k is the number of network components in the demand-flow-graph. This number can be reduced by application of the formulae for components in series with the same demand-flow.

We have implemented this methodology by use of a recursive algorithm. This algorithm considers any failure scenario in the demand-flow-graph by recursively assuming the elements to be failing or in normal operation.

Figure 7 depicts an exemplary demand–flow-graph. Consider a demand of value $d = 2$ between s and t. The share of the demand which has to be protected against single node or link failures is $d^* = 1$ and 3 paths are routed (Figure 7). Note, that this configuration is quite inefficient as 2 paths (in 1+1 routing) would be sufficient, but it is adequate to illustrate the algorithm.

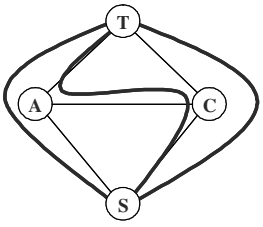

Figure 7: Demand-flow-graph

Assume each link and node in the graph has an individual failure probability which we denote as p_n for nodes and p_{nm} for links. Now, the availability for DSP is computed recursively as follows: For each element (i.e. link or node in the demand graph) consider both cases:

- Element x fails with probability p_x:
  mark the element and all traversing paths as failed and consider the remaining instance.
- Element x works with probability $(1-p_x)$:
  assume this element will not fail anymore (i.e., is fixed) in further considerations.

In both cases, the remaining instance is reduced by the possible failure of an element (which is either failed or fixed and thus cannot fail). Instead, we get a probability factor for the availability in the remaining instance. This is recursively iterated until we know how many paths survive any arising scenario.

For explanation, consider link AT. If it fails, only path T-C-S will survive if the links SC and CT as well as the node C will not fail which happens with the probability $(1-p_{SC})(1-p_C)(1-p_{CT})$. Hence, 1 path will survive with the probability $p_{AT}(1-p_{SC})(1-p_C)(1-p_{CT})$. In any further considerations we fix link AT. Here, we get the probability factor $(1-p_{AT})$ for all following terms.

Next we consider link AC. If it fails, again path T-C-S survives with probability $(1-p_{SC})(1-p_C)(1-p_{CT})$. But further, also path T-A-S will survive with probability $(1-p_A)(1-p_{AS})$. We end up with the term

$$\underbrace{(1-p_{AT})}_{\substack{AT \text{ is} \\ \text{fixed}}} \underbrace{p_{AC}}_{\substack{AC \text{ is} \\ \text{failed}}} \Big\langle \underbrace{(1-p_{SC})(1-p_C)(1-p_{CT})}_{\text{path } T\text{-}C\text{-}S \text{ survives}} \cdot \underbrace{1}_{n_{SP}(1)} + \underbrace{(1-p_A)(1-p_{SA})}_{\substack{\text{path } T\text{-}A\text{-}S \\ \text{survives}}} \cdot \underbrace{1}_{n_{SP}(2)} \Big\rangle$$

In total, we get the following formula for the protected portion of the demand:

$$\begin{aligned}
&P_{AT}(1-P_{SC})(1-P_C)(1-P_{CT})\cdot 1 + \\
&(1-P_{AT})(P_A(1-P_{SC})(1-P_C)(1-P_{CT})\cdot 1 + \\
&\quad (1-P_A)(P_{SC}(1-P_{SA})\cdot 1 + \\
&\quad\quad (1-P_{SC})(P_C(1-P_{SA})\cdot 1 + \\
&\quad\quad\quad (1-P_C)(P_{SA}((1-P_{AC})(1-P_{CT})\cdot 1 + P_{CT}(1-P_{AC})\cdot 1 + P_{AC}(1-P_{CT})\cdot 1) + \\
&\quad\quad\quad\quad (1-P_{SA})(P_{AC}((1-P_{CT})\cdot 1 + P_{CT}\cdot 1) + \\
&\quad\quad\quad\quad\quad (1-P_{AC})P_{CT}\cdot 1 + (1-P_{CT})\cdot 1)))))
\end{aligned}$$

When calculating the availability of the unprotected share of the demand we have only take into account those failure scenarios with $n_{sp} > d^*$:

$$\begin{aligned}
&(1-P_{AT})(0 + \\
&\quad (1-P_A)(0 + \\
&\quad\quad (1-P_{SC})(0 + \\
&\quad\quad\quad (1-P_C)(0 + \\
&\quad\quad\quad\quad (1-P_{SA})(P_{AC}(1-P_{CT})\cdot 1 + \\
&\quad\quad\quad\quad\quad (1-P_{AC})P_{CT}\cdot 1 + (1-P_{CT})\cdot 1)))))) \\
&= (1-P_{AT})((1-P_A)((1-P_{SC})((1-P_C)((1-P_{SA})(P_{AC}(1-P_{CT})\cdot 1 + (1-P_{AC})P_{CT}\cdot 1 + (1-P_{CT})\cdot 1)))))
\end{aligned}$$

Finally, note that the very same method gives also the correct result for 1+1 routings. For this, just consider the same demand graph without link AC and without path T-A-C-S.

4 Case Study

For evaluation of the connection availability of DSP and comparison with dedicated and shared path protection, we have applied the survivability mechanisms to two different network scenarios.

The DSP routings are adopted from the computational study presented in [5]. The solutions are obtained with the help of an integer linear programming approach for minimizing the total network cost. We have used two different approaches to calculate routings for dedicated protection. The first approach calculates routings for unprotected and protected traffic demands also by use of an integer linear programming formulation, whose results have been presented in [5], too. The second method calculates the Shortest Cycle [2] between the end-nodes of a connection for the protected portion of the demand, and the Shortest Path [2] for the unprotected portion of the demand, both based on hop-count and physical path length. The application of heuristics for network planning is widely deployed in commercial network planning tools like [10]. For the case of shared path protection, we have used an heuristic approach which routes like in dedicated path protection. Along the backup path, as much capacity as possible is shared between demands with node-disjoint working paths.

4.1 Network scenarios

The network scenarios *NSFNET* and *Germany* originate from the reference network scenarios presented in [6]. Table 1 summarizes some characteristics of the topologies and the traffic demands. The network designs and the total network costs have been computed with an optical equipment cost model, see [8] for details.

network scenario	number of nodes	number of links	mean nodal degree	total traffic demand (bi-directional)
NSFNET	14	21	3	686
Germany	17	26	3.06	2710

Table 1: Description of used network scenarios

For every network instance, we consider three scenarios: 50% (*halfprotected*), 75% (*mostprotected*) and 100% (*fullprotected*) protection of all traffic demands. For comparison reasons, we have also considered the case where none of the traffic demands have to be protected (*unprotected*). Fractional survivability requirements are rounded up as to guarantee that at least the percentage of the traffic survives and to require protection for entire lightpaths/VC-n paths only.

The used availability numbers for optical network equipment (Table 2) are based on the availability model presented in [11].

The availability of the connection end-nodes is assumed to be 1, a common simplification applied in other studies of this kind [7][11] as well. In case of protected connections, the end-nodes are serially switched in line with the parallel working and protection paths. Hence, the availability of the end-nodes will dominate the connection availability, and the significance of the results is limited. In real networks, additional effort is undertaken to protect connections against failures of the end-nodes, like the connection of the customer with two separate network edge-nodes or the use of an optical channel protector (OCP).

equipment part	FIT	MTTR [hours]
WDM transponder	3.40E+03	9
WDM Mux/Demux	1.00E+04	9
OXC	1.00E+04	9
Cable (1km)	5.70E+02	24
OLA	1.00E+04	9

Table 2: Availability numbers of equipment

4.2 Results

Within all figures below, we use the following labelling (in the same order) to distinguish between the different protection schemes and the protected or the unprotected share of the demand:

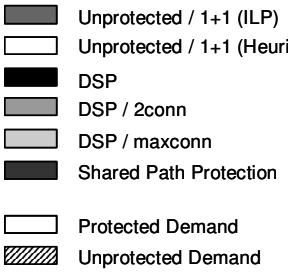

Figure 8 and Figure 9 show the mean end-to-end availability for the unprotected and the protected share of the demands. The comparison of the total network cost is presented in Figure 10 and Figure 11. To link the additional network costs for network backup capacity and the increases in connection availability when using any protection scheme, we have normalized the increase in availability (Δq) according to the increase of the costs ($\Delta cost$) compared to the unprotected case:

$$g = \frac{\Delta q}{\Delta cost}$$

This term is defined as the availability gain g. Figure 12 and Figure 13 depict the availability gain for all protection schemes and different levels of protection.

4.3 Discussion

We can observe that DSP provides nearly the same mean availability for the protected fraction of the demands as 1+1 protection. Compared to shared path protection, the mean availability for DSP is better in most cases. Comparing the three DSP variants, the highest level of availability was observed when using the *2conn* DSP variant. As mentioned in Section 2.3, *2conn* explores connectivity 2 between node-pairs which enable relative short routes to choose. Short routes are beneficial for availability, as link failures are dominant in our case study.

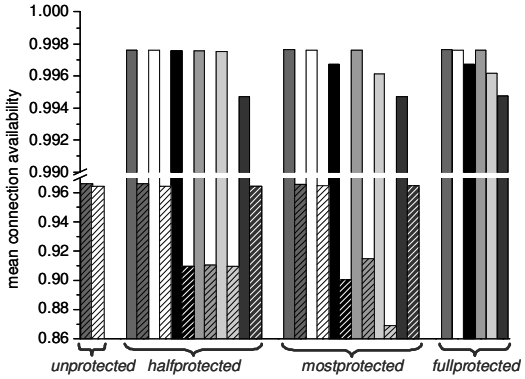

Figure 8: Connection availability for *NSFNET*

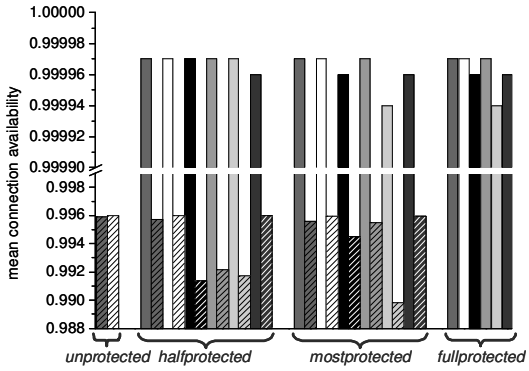

Figure 9: Connection availability for *Germany*

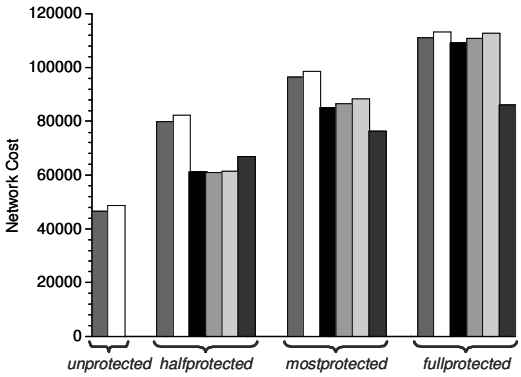

Figure 10: Total network cost for *NSFNET*

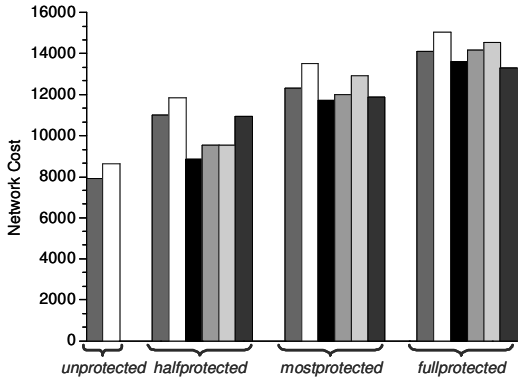

Figure 11: Total network cost for *Germany*

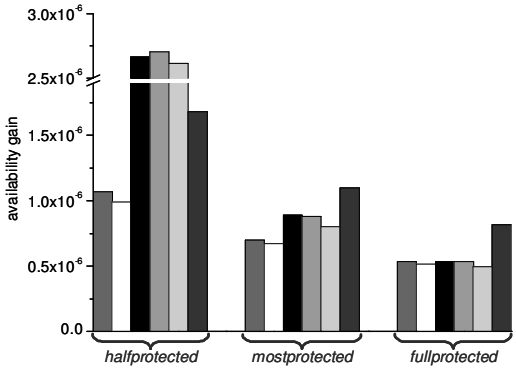

Figure 12: Availability gain for *NSFNET*

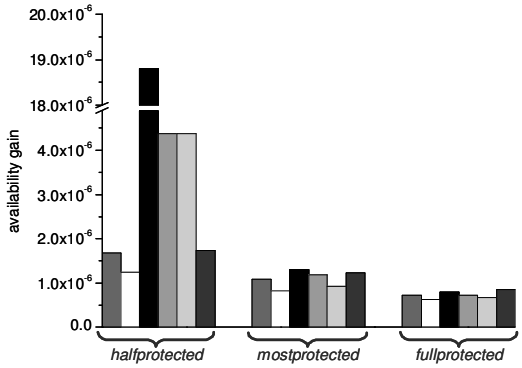

Figure 13: Availability gain for *Germany*

In case of *maxconn*, the maximum connectivity between node pairs is explored. Thus, the mean path length is increased compared to *2conn* which decreases the connection availability. Since the connectivity to be explored is not prescribed in DSP (and selectable between 2 and the maximum connectivity of the node-pair), the availability of the extended version DSP is in between these two basic variants.

The availability of the unprotected fraction of the demand is always lower in case of DSP compared to the other protection schemes. The reason for this is that in case of DSP unprotected traffic might be indirectly affected by failures if disrupted and protected traffic is switched over to paths used by unprotected traffic.
From the network cost comparison, we can observe that DSP is very effective for low protection levels

and loses gain as the protection level advances towards 100%. In all cases, DSP is a more cost-effective survivability concept than 1+1 protection. For *halfprotected*, the best solution by DSP is below the cost for the shared path protection heuristic solution. For *mostprotected* and *fullprotected*, sharing of backup resources between different demands (shared path protection) is more effective than sharing of resources within each demand (DSP). Finally, we can observe that the ILP approach for 1+1 protection is more cost-effective than routing of demands along Shortest Paths or Shortest Cycles, resp.

The comparison of the availability gain shows that DSP outperforms 1+1 protection for all protection levels. The highest effectiveness for DSP is observed in case of *halfprotected* demands (notice the break in the scales of the figures). For *mostprotected* and *fullprotected* demands, shared path protection has higher gain than DSP in the NSFNET scenario and is as effective as DSP in the Germany scenario. Its implementation however is more complicated.

5 Conclusions

Demand-wise Shared Protection combines advantages of dedicated protection and shared path protection. It provides fast recovery times, good capacity efficiency, and low operational effort.

This paper presented an analytical approach for computing the connection availability for DSP. The method can easily be implemented by use of a recursive algorithm.

It turned out that DSP provides nearly the same level of connection availability as dedicated protection for the protected connections. Compared to shared path protection, connection availability of DSP is better in most cases. When linking the mean availability and the additional network costs for backup capacity, we have observed that DSP is more effective than 1+1 protection, in particular if not 100% of all demands have to be protected. Compared to shared path protection, DSP provides a comparable efficiency while operational management is considerably simpler and recovery times are much faster.

6 Acknowledgement

The work reported in this paper has been supported by the European Commission through IST NOBEL and by the German Ministry of Education and Research (BMBF) within the EIBONE project under contract number 01BP567 for Zuse Institute Berlin and 01BP568 for atesio GmbH.

7 References

[1] M. Barry, S. Bodamer, J. Späth, M. Jäger, R. Hülsermann, "A Classification Model for Network Survivability Mechanisms", 5th ITG-Workshop on Photonic Networks 2004, pp.129-136.

[2] R. Bhandari, "Survivable Networks Algorithms for Diverse Routing", pp. 22-29, pp. 86-92, Kluwer Academic Publishers, 1999.

[3] G..Dahl, M.Stoer, "A cutting plane algorithm for multicommodity survivable network design problems", INFORMS Journal on Computing, vol. 10, no. 1, pp. 1-11, 1998.

[4] A. Groebbens et al, "Use of Backup trees to Improve Resource Efficiency of MPlambdaS Protection Mechanisms", DRCN 2001, pp.152-159.

[5] C.G. Gruber, A.M.C.A. Koster, S. Orlowski, R. Wessäly, A. Zymolka, "A computational study for Demand-wise Shared Protection", DRCN 2005, pp. 421-425.

[6] R. Hülsermann et al, "A Set of Typical Transport Network Scenarios for Network Modelling", 5th ITG-Workshop on Photonic Networks 2004, pp. 129-136.

[7] M. Jäger, R. Hülsermann, "Service Availability of Shared Path Protection in Optical Mesh Networks", ECOC 2004.

[8] A.M.C.A. Koster, A. Zymolka, M. Jäger, R. Hülsermann, "Demand-wise Shared Protection for meshed optical networks", Journal of Network and Systems Management,vol. 13, no. 1, pp. 35-55, 2005.

[9] C. Mauz, "Allocation of Spare Capacity for Shared Protection of Optical Paths in Transport Networks", DRCN 2001, pp.22-27.

[10] OPNET, "WDM Guru", http://www.opnet.com

[11] S. Verbrugge, D. Colle. P. Demester, R. Hülsermann, M. Jäger, "General Availability Model for Multilayer Transport Networks", DRCN 2005, pp. 85-92.

[12] R. Wessäly, S. Orlowski, A. Zymolka, A.M.C.A. Koster, C.G. Gruber, "Demand-wise Shared Protection revisited: A new model for survivable network design", INOC 2005, pp. 100-105.

[13] A. Zymolka, A.M.C.A. Koster, R. Wessäly, "Transparent optical network design with sparse wavelength conversion", ONDM 2003, pp. 61-80.