Availability Analysis of GMPLS Connections based on Physical Network Topology

Juan Segovia, Eusebi Calle, Pere Vila

Abstract—**This paper presents a study of connection availability in GMPLS over Optical Transport Networks (OTN) taking into account different network topologies. Two basic path protection schemes are considered and compared with the no protection case. The selected topologies are heterogeneous in geographic coverage, network diameter, link lengths, and average node degree. Connection availability is also computed considering the reliability data of physical components and a well-known network availability model. Results show several correspondences between suitable path protection algorithms and several network topology characteristics.**

Index Terms—**Availability, Optical Transport Networks, GMPLS, Network Protection.**

I. INTRODUCTION

THE core networks of telecommunications operators must be capable of transporting large volumes of traffic in aggregated form while fulfilling stringent requirements of quality of service and reliability. Thanks to advances in key technologies such as Wavelength Division Multiplexing (WDM), current optical networks can carry data at hundreds of gigabits per second over a single fiber optic cable. The increase in traffic volume, however, puts even more pressure on the ability of networks to withstand adverse conditions caused by events such as component failure, natural disasters, and fiber cuts. In an Optical Transport Network (OTN) a failure can disrupt service for thousands of users and severely affect operators' revenue, even if the resultant interruption lasts for just a few seconds. In this context, the quality of a service can be characterized and assessed in terms of its reliability and availability.

Generalized Multi-Protocol Label Switching (GMPLS) has emerged as one of the most suitable technologies to manage and operate OTNs. In this context, several techniques have been proposed and deployed for dealing with network failures in order to restore the service as soon as possible. They differ in scope, approach to resource allocation and provisioning, routing strategy and goal, recovery model, etc. [1]. This rich

set of recovery options gave birth to several resilience-oriented routing schemes and QoS architectures such as [2]-[5]. However, network protection techniques improve availability at the cost of increasing resource usage due to the underlying redundancy applied.

Two basic protection schemes are Dedicated Path Protection (DPP), and Shared Path Protection (SPP). DPP offers high level of availability and fast recovery times but requires more than 100% extra network capacity [6]. On the other hand, SPP is able to share resources allocated for recovery purposes and thus reduce the capacity requirements, although the offered availability can be lower. Both DPP and SPP are important protection schemes; the former is currently widely deployed, and the latter appeals for its resource efficiency.

Availability can be measured network wide, by which ISPs and operators can assess the reliability of the network as a whole. However, the unit of service in a transport network is a connection, i.e. the virtual communication channel created between two designated nodes. A connection is unavailable as soon as one of its components becomes unavailable. Therefore, performance parameters defined in Service Level Agreements between operator and customer usually refer to that unit of service. The relevance of connection availability is reflected in the growing number of papers on the topic. Their focus, however, is either on optimal design for availability, or efficient connection provisioning, where the demand is fixed and known beforehand.

The goal of this paper is to study the effects that topology properties of a given network have on connection availability when different path protection schemes are applied. Given that availability is defined as the probability that a system (e.g. a connection) is found in the operating state sometime in the future, it is clear that the components forming a connection should be analyzed. Furthermore, the combination of topology, protection scheme, and routing strategies can generate different connection availability patterns. Therefore, the challenge is to identify such patterns associated to topology properties (e.g., node degree, link length, and network diameter) that can be used for assessing and comparing network performance from the point of view of connection availability.

The rest of this paper is organized as follows. Section 2 presents the concepts on connection availability and protection schemes applied. Section 3 presents the network availability model employed, the main characteristics of the
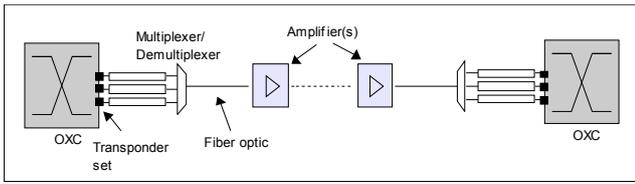
Fig. 1: A link in the network availability model

selected topologies, and the simulation setup. Section 4 discusses the results. Finally, section 5 concludes the paper.

II. CONNECTION AVAILABILITY AND PROTECTION SCHEMES

A. Availability Evaluation

In terms of reliability, a connection can be seen as a composite system whose components are network elements such as fiber optic cables, amplifiers, and switches. The availability of such a system can be computed statistically based on reliability data, i.e. the failure frequency and failure repair rate of its components, measured over long periods of time. Two such reliability measures are the Mean Time to Repair (MTTR), and the Mean Time Between Failures (MTBF). The MTTR is the average time spent performing corrective actions; during that time the affected equipment is non-operative or "down". The average time between two consecutive failure events is measured by the MTBF; it includes the time spent in the operative or "up" state, as well as the subsequent "down" state. A component's availability can then be defined as the proportion of the duration of its "up" state in the total time [7]:

$$A = (MTBF - MTTR) / MTBF \qquad (1)$$

Computing the availability of a connection means obtaining the availability of one or more paths. A path is a sequence of interconnected nodes forming a series system. Assuming statistically independent component availability, path availability is the product of the availability of each node and link from an origin to a destination, as shown in (2). Therefore, a path is available only if all the components along its route are available.

$$A_{path} = A_{N_1} \cdot A_{L_1} \cdot A_{N_2} \cdot A_{L_2} \cdot \ldots \cdot A_{N_k} \cdot A_{L_k} \cdot A_{N_{k+1}} \qquad (2)$$

A_{N_i} and A_{L_i} denote the availability of the nodes and links forming a given path of k hops. Every A_{L_i} can be computed by assimilating it to a series system based on the components of that link (i.e. spans of fiber optic cables and amplifiers). Although a node has many subsystems, it has much higher reliability than other network components. Hence, A_{N_i} can be obtained by the application of (1), as if a node were a simple component.

B. Connection Availability and Basic Protection Schemes

There are many protection schemes proposed in the literature; they differ in their provisioning method, their number of working paths per backup paths, their recovery scopes and so on. This paper studies two basic GMPLS protection schemes, namely a) Dedicated Path Protection (DPP), and b) Shared Path Protection (SPP) [8]. The availability of unprotected connections is also presented for comparison purposes. Due to the peculiarities of protection schemes, connection availability is computed differently for every case studied, as explained in the following paragraphs.

When no protection is applied, connection availability is equal to path availability. It is assumed in this paper that connections, protected or otherwise, are bi-directional and symmetric, i.e., capacity is allocated so that traffic can flow in both directions simultaneously following exactly the same route. If a failure arises in components serving one direction, the whole connection is considered unavailable. To take this situation into account, a connection's availability is obtained by squaring its path availability:

$$A = A_{path}^2 \qquad (3)$$

In the case of DPP, a connection is treated as a parallel system from the reliability point of view. One dedicated backup path protects exactly one working path. Traffic is duplicated at the ingress node so that both paths carry the same data towards the destination node, where the best one is chosen for use. Working and protection paths are set up so that no node or link is shared between them. Hence, a connection is available if at least one of paths is operative, as expressed in (4). A_w and A_b represent working and backup path respectively, computed as per (3).

$$A = A_w + (1 - A_w)A_b \qquad (4)$$

When connections are protected with SPP, working and protection paths are also selected node disjoint. However, traffic flows exclusively through the working path, unless a failure is detected, at which point it is changed over to the protection path. Furthermore, under the assumption that there can only be one outstanding failure at any given time, several working paths can be sharing a single protection path, leading to the usual 1:N notation (i.e., 1 protection path for N working paths). It is also possible to assign more than one protection path for a number of working paths (M:N shared protection), but that case is not considered in this paper.

In principle, availability under DPP and SPP are computed in the same way, that is, by applying (4). However, because of the sharing nature of the latter, if two or more simultaneous or near simultaneous failures affect unrelated (disjoint) working paths, there is no guarantee that all of them will be recovered because they might be sharing backup resources. A successful corrective action could leave other(s) failing connection(s) without the needed backup resources because the capacity for protection was already used up by the first failing working path. A penalty for this potential access conflict should then be considered when using SPP, lowering the initial

Property	DFN-GWIN	GER-MANY50	COST-266	KL-A	JANOS-US-CA	NSF-NET-A
a) Number of nodes	17	50	37	15	39	14
b) Number of links	47	88	57	28	61	21
c) Avg. node degree	8.5	3.52	3.08	3.73	3.13	3.00
d) Net. diameter [1]	2 698	13 950	11 4052	5 2814	11 5035	6 4558
e) Avg. min. distance [1]	1.15 343	4.05 383	3.74 1479	2.13 1257	4.21 2198	2.14 2155
f). Min. link length[2]	80	27	147	147	134	383
g). Max. link length[2]	603	254	1585	1064	1205	2748
h) Avg. link length (km) and std. deviation	317 123	102 45	440 247	634 256	525 269	1083 558

[1] In hops and km
[2] In km

availability computed by (4). Equation (5) is used in this paper for approximating this penalty A_p, as suggested in [9].

$$A_p = (1 - A_w)A_b(1 - A_w^{n-1})\left[1 - \frac{1}{2 + (n-2)(1 - A_w)}\right] \quad (5)$$

In Equation (5) n is the size of the backup path sharing group. If b is the backup path selected for a new connection, and b_i is every link in path b, then n is the maximum of the number of working paths that have b_i as part of their own backup path. The final connection availability is then $A_{spp} = A - A_p$.

III. NETWORK AVAILABILITY MODEL AND SIMULATION SETUP

A. Network Availability Model

In the network availability model considered in this paper, every link consists of the following components [7]:
a) A pair of Optical cross connects (OXC)
b) Two sets of transponders, one at each end of a link
c) A pair of multiplexer/demultiplexer
d) Fiber optic cable, whose length depends on the distance between the two nodes it connects
e) Zero or more optical amplifiers, depending on the length of the fiber optic cable. It is assumed that they are deployed every 100 km.

Figure 1 shows how these components are arranged to form a link at the optical level. Although not considered in this paper, components of other higher-level layers could also be added. A node is assumed to consist of only an OXC, while links are viewed as a generalized data pipe capable of transporting all the offered traffic without regard to the actual number of optical channels that might be needed. Thus, a link needs only one pair of transponders, a single fiber optic cable, and one set of amplifiers. The MTBF and the MTTR of

network components presented in [7] are used in the application of (1) to obtain the availability of single components. That collection of reliability numbers include a variety of equipment types for OTNs, without being tied to vendor-specific products.

B. Topologies studied

Six topologies were selected for this study (see Table I):
1. DFN-GWIN: Germany's National Research and Education Network.
2. GERMANY50: a reference network originating from the European project NOBEL.
3. COST266: a reference network defined in the context of the European project Cost266. It interconnects 37 cities across Europe. Details can be found in [10].
4. JANOS-US-CA: a reference network that interconnects cities in the USA and Canada. It has both short and very long links.
5. KL-A: a variation of the KL topology. Nodes of the original topology were mapped to European cities of the COST266 topology.
6. NSFNET-A: an adaptation of NSFNET, a topology of 14 nodes and 21 links.

The first four are from SNDlib (Survivable Network Design Library), a repository of topologies, models and solutions for the design of survivable fixed telecommunication networks [11]. KL-A and NSFNET-A are two are adaptations developed for this study of two well-known topologies. These six topologies were selected in order to obtain heterogeneity in average node degree, number of nodes and links, network diameter, geographical coverage, and diversity in link lengths. The following observations can be made about the properties of these networks:
a) GERMANY50 is the smallest network in terms of geographic coverage; its links are short and their lengths do not differ much. It also has the smallest average minimum distance between node pairs (1.15 hops; 343 km).
b) The node degree varies in general between 3.00 and 3.73. DFN-GWIN, however, has a node degree of 8.5.
c) If the number of hops along the shortest paths (in km) is used to measure the network diameter, there are two groups of topologies: those with 6 or less (DFN-GWIN, KL-A, and NSFNET-A), and those with 11 or more (GERMANY50, COST266, JANOS-US-CA). However, if the diameter is measured only in kilometers, the topologies are quite dissimilar.
d) The link length distributions are such that links in NSFNET-A are generally long (85% is at least 500 km). They are also long in JANOS-US-CA (about 50%) and KL-A (about 70%). COST266 has much shorter links (around 70% with less than 500 km).

C. Simulation Setup

Connection availability was evaluated with an event-based simulator. The events considered were the arrival of

TABLE II
UNPROTECTED CONNECTIONS

Aspect	DFN-GWIN	GER-MANY50	COST266	KL-A	JANOS-US-CA	NSFNET-A
a) Average Connection Availability	0.996097	0.996797	0.987971	0.988759	0.987545	0.983112
b) Availability Standard Deviation (±hours/year)	0.002236 (±10 h)	0.002669 (±12 h)	0.008814 (±39 h)	0.007177 (±31 h)	0.011242 (±49 h)	0.011861 (±52 h)
c) Down-time for given Average Conn. Availability (hours per year)	34	28	105	98	109	148
d) Worst Availability	0.979198	0.978522	0.929671	0.940580	0.924385	0.913965
e) Down-time for Worst Availability (hours per year)	182	188	616	521	662	754
f) Average hop count	1.76	3.93	4.17	2.57	3.62	2.44

connection requests and their corresponding release, arrivals following a Poisson process, with exponentially distributed connection holding times. The results reported correspond to an average of ten runs, and every run processed 80,000 connections, where de demanded capacity was chosen randomly following a uniform distribution. Link capacity was assumed to be uniform in the network; its value was chosen so that connection blocking would be around 30%, and network utilization around 70% in every case. Using distance in km as the sole metric, routing was carried out along the shortest path. Node-disjoint working and protection paths were chosen for DPP and SPP. Dijkstra's algorithm was used to find the shortest paths, and a two-step approach was applied to select protection paths. To evaluate the behaviour of connections, the following figures of merit were used:

a) *Average Availability*: The average connection availability of all accepted requests.

b) *Worst Availability*: The lowest connection availability obtained for the given topology and protection scheme.

c) *Average Hop Count of Paths*: The average length of the working and protection paths assigned to accepted connections.

d) *Restoration Overbuild*: Measures how much extra capacity is committed to protection, compared to the capacity required by working paths alone. It is an average taken over all accepted connections. When DPP is applied, this extra capacity is simply the product of number of hops by demand. However, under SPP it is more complex. Equation (6) was used in this paper for this purpose, as suggested in [12].

$$ Cp_i^{spp} = \sum_{m=1}^{k} \left(CT_m (d / \sum_{j=1}^{p} C_{m,j}) \right) \qquad (6) $$

where k is the number of links in a given protection path of connection i, p is the number of backup paths that exist when the new connection is being set up, CT_m is the maximum demand of all backup paths that pass through link m, d is the demand of the arriving connection i, and $C_{m,j}$ is the capacity required by the other connections that are sharing link m.

IV. SIMULATION RESULTS AND DISCUSSION

A. Availability of Unprotected Connections

As can be seen in Table II, the Average Availability of unprotected connections is lower than two nines in four cases out of six. These values represent an average down time of 30 hours per year in the best cases (DFN-GWIN and GERMANY50), and up to six days in the worst case (148 hours/year, NSFNET-A). The individual availabilities are quite disperse with respect to their average, see row b). The lowest connection availability is given by Worst Availability in row d). Compared to the Average Availability, the down times corresponding to these worst values are from five to six times higher.

NSFNET-A offers the worst average connection availability. In terms of unreliability, fiber links are dominant because of the frequency of cable cuts and the long repairing time, compared to other components. It was observed during the simulations that about 97% of the unavailability of an unprotected connection can be attributed to the unavailability of the fiber optic cable, while the contribution of optical amplifiers was minimal. This is similar to what was reported in the sensitivity analysis performed by [13], which highlights the importance of MTTR and link failure rates in path protection. NSFNET-A's poor performance is expected due to the fact that it has much longer links than the other topologies.

Figure 2 shows how the mean down time of connections in GERMANY50 and COST266 increases when the link lengths are multiplied by a given factor. It can be seen that the average down time increases linearly when connections are unprotected, with different slopes for different topologies. When protection is applied, however, the degradation rate is lower.

B. Availability with DPP

Compared to the unprotected case, DPP produces substantially improved Average Availability (see Table III). Up to 50 times better values are obtained with the four geographically larger topologies. Nevertheless, the performance of these topologies in terms of average connection availability is far from 5 minutes per year of down-time, a usual requirement of highly-available services.

With respect to Worst Availability, it has consistently one "nine" less than the average availability, giving down times per year of around 20 hours/year in half of the topologies. This is more than 200 times worse than the goal of 5 minutes per year.

It can be seen in Table III that the lower the average minimum distance in hops, the lower the total hop count of connection paths. However, no discernible relationship exists between total hop count and connection availability, at least not without also considering link lengths. For example, NSFNET -A has the second lowest total hop count, but the worst availability by a large margin.

Protection paths in the studied topologies tend to be between 50% and 70% longer than their corresponding working paths when measured in hop counts. The average Restoration Overbuild is 2.7. A higher node degree helps in finding shorter paths in general, and in particular can decrease Restoration Overbuild because it makes it easier to find disjoint backup paths. For example, disregarding distances in kilometers, KL-A and NSFNET-A have similar properties, except that KL-A's node degree is 25% higher. This can explain why KL-A's backup paths are 60% longer on average than their working paths, while those of NSFNET-A are 90% longer.

The effects of topology properties on connection availability in geographically small networks seem to be negligible. This is exemplified by DFN-GWIN and GERMANY50. These topologies are very different with respect
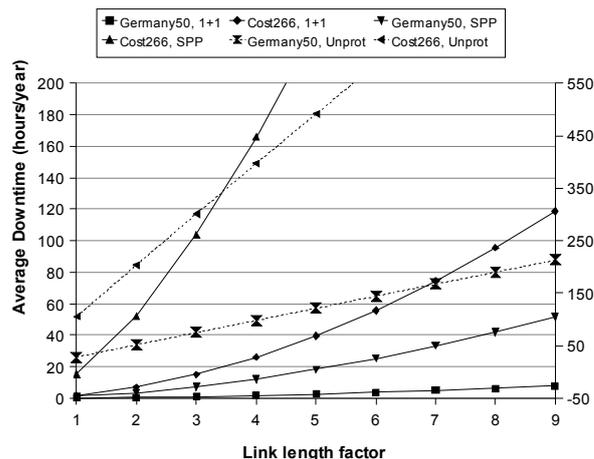
Fig. 2. Average downtime as a function of scaled link length. Dotted lines are plotted against the secondary *y* axis.

to average node degree, network diameter, and average minimum distance. Despite of this, their average connection availabilities under DPP are very close.

C. Availability with SPP

Improvement in Average Availability can also be observed under SPP (see Table IV), but it is both lower and more irregular than in DPP. Sharing affects connection availability both positively and negatively. Positively, as it helps in finding shorter backup paths (with sharing, more usable capacity is available). It affects negatively because the penalty

TABLE III
DEDICATED PATH PROTECTION (DPP)

Aspect	DFN-GWIN	GERMANY50	COST266	KL-A	JANOS-US-CA	NSFNET-A
a) Average Connection Availability	0.999983	0.999985	0.999790	0.999838	0.999723	0.999620
b) Down-time for given Average Conn. Availability (hours per year)	0.15	0.13	1.84	1.42	2.43	3.33
c) Worst Availability	0.999845	0.999738	0.997600	0.998834	0.997539	0.997408
d) Down-time for Worst Availability (hours per year)	1.36	2.3	21.02	10.21	21.56	22.71
e) Restoration overbuild	2.45	2.78	2.70	2.65	2.73	2.96
f) Average hop count for Working paths	1.49	3.26	3.57	2.20	3.15	2.00
g) Average hop count for Backup paths	2.19	5.52	5.93	3.52	5.36	3.79
h) Total hop count (f+g)	3.68	8.78	9.50	5.72	8.51	5.79

TABLE IV
SHARED PATH PROTECTION (SPP)

Aspect	DFN-GWIN	GERMANY50	COST266	KL-A	JANOS-US-CA	NSFNET-A
a) Average Connection Availability	0.999932	0.999884	0.998272	0.999483	0.996525	0.998842
b) Down-time for given Average Conn. Availability (hours per year)	0.60	1.02	15.14	4.53	30.44	10.14
c) Worst Availability	0.998616	0.997458	0.964259	0.987672	0.952472	0.982196
d) Down-time for Worst Availability (hours per year)	12.12	22.27	313.09	107.99	416.35	155.96
e) Restoration overbuild	1.69	1.85	2.02	2.24	2.06	2.30
f) Average hop count for Working paths	1.68	3.82	3.92	2.40	3.29	2.30
g) Average hop count for Backup paths	2.54	6.43	6.92	4.13	7.08	4.13
h) Total hop count (f+g)	4.22	10.25	10.84	6.53	10.37	6.43

for potential sharing access conflict grows with sharing group size. Hence, a trade-off that has to be faced when applying protection with SPP. As the routing algorithm in our simulations does not restrict the sharing group size, the negative effect outweighs the positive one.

As expected, Restoration Overbuild is lower in SPP than in DPP, the average being 2.03 for the six topologies. However, as in our simulations the sharing group size is not limited and the routing strategy is simple, the existence of preferred shared paths (short paths that are frequently selected) can be affecting this value, making it lower that it would be otherwise.

V. CONCLUSION

This paper presented a novel study considering the influence of topology properties on connection availability in the context of Optical Transport Networks. Results show that independently of the application of DPP or SPP, continental-size network topologies have average availability values very different compared to small or medium size networks, where no differences can be observed. On the other hand, results have shown that the dominant component in the network availability model is the fibre optic cable, due the frequency of cable cuts and the relative long duration of repair times. Therefore, connection availability is dependent on the length of links, or in general terms, on the link length distribution of its network topology.

Another interesting result concerns the average minimum distance, evaluated in hops between node pairs. For topologies with a small average minimum distance, a short total hop count can be expected in both DPP and SPP, and consequently a suitable availability value. However, other factors such as link length distribution, and sharing rules, can modify the expected values. It has also been observed in SPP that the sharing group size can change the expected availability values if only topology features are considered. This aspect is to be further studied in our future work. With respect to average node degree, it can be noted that under DPP it improves restoration overbuild because it helps in finding disjoint paths for backup.

REFERENCES

[1] J. L. Marzo, E. Calle, C. Scoglio, T. Anjali, "QoS On-Line Routing and MPLS Multilevel Protection: a Survey," IEEE Comunication Magazine, vol. 41(10), pp. 126-132, October 2003.

[2] A. Urra, E. Calle, J. L. Marzo, "Reliable Services with Fast Protection in IP/MPLS over Optical Networks," Journal of Optical Networking,OPTICAL, SOC AMER, ISSN: 1536-5379 Vol. 5, No. 11. November 2006.

[3] A. Autenrieth, A. Kirstadter, "Engineering end-to-end IP resilience using resilience-differentiated QoS," IEEE Communications Magazine, 2002, Vol. 40. Issue 1, January 2002, pp. 50-57.

[4] J. Tapolcai, P. Cholda, T. Cinkler, K. Wajda, A. Jajszczyk, A. Autenrieth, S. Bodamer, D. Colle, G. Ferraris, H. Lonsethagen, I.-E. Svinnset, D. Verchere, "Quality of Resilience (QoR): NOBEL Approach to the Multi-Service Resilience Characterization", in Proc. Workshop on Guaranteed Optical Service Provisioning (GOSP) co-located with BroadNets 2005, 10/2005, Boston, USA, pp. 405-414.

[5] P. Cholda, A. Jajszczyk, and K. Wajda, "A Unified Framework for the Assessment of Recovery Procedures," Proc. IEEE 2005 Workshop on High Performance Switching and Routing HPSR 2005 (Hong Kong, China), May 12-14, 2005.

[6] M. Jaeger, R. Huelsermann, D.A. Schupke, R. Sedlak, "Evaluation of Novel Resilience Schemes in Dynamic Optical Transport Networks", Asia-Pacific Optical Communication Conference APOC 2003, Shanghai (China), 2003.

[7] S. Verbrugge, D. Colle, P. Demeester, R. Huelsermann, and M. Jaeger, "General availability model for multilayer transport networks," Proceedings 5th IEEE Int. Workshop on Design of Reliable Communication Networks (DRCN), Naples, Italy, 2005

[8] E. Mannie (Ed.), D. Papadimitriou (Ed.), "Recovery (Protection and Restoration) Terminology for Generalized Multi-Protocol Label Switching (GMPLS)". RFC 4427, March 2006.

[9] R. Huelsermann, M. Jaeger, A. Koster, S. Orlowski, R. Wessaely, and A. Zymolka, "Availability and Cost Based Evaluation of Demand-wise Shared Protection," in 7th ITG-Workshop on Photonic Networks, VDE Verlag GmbH, Leipzig, Germany, 161-168, 2006.

[10] S. de Maesschalck et al., "Pan-European Optical Transport Networks: An Availability-based Comparison," Photonic Network Communications, 5(3), 2003.

[11] S. Orlowski, M. Pióro, A. Tomaszewski, and R. Wessäly, "SNDlib 1.0–Survivable Network Design Library," in Proceedings of the 3rd International Network Optimization Conference (INOC 2007), Spa, Belgium, 2007.

[12] Piotr Cholda, "The Reliability Analysis of Recovery Procedures in GMPL-based Optical IP Networks," AGH University of Science and Technology, Kraków, Poland, 2005 (PhD Thesis).

[13] M. Held, L. Wosinska, P. M. Nellen, C. Mauz, "Consideration of connection availability optimization in optical networks," Proceedings of the Fourth International Workshop on Design of Reliable Communication Networks (DRCN), 2003.