Investigation of Protection Strategies: Problem Complexity and Specific Aspects for WDM Networks

Jan Späth, Heiko Weißschuh*

Institute of Communication Networks and Computer Engineering, University of Stuttgart
IND, Pfaffenwaldring 47, D-70569 Stuttgart, Germany
Tel: +49 711 6857990, Fax: +49 711 6857983, E-Mail: spaeth@ind.uni-stuttgart.de

** The author is now with Colt Telecom, Frankfurt (Heiko.Weissschuh@colt.de)*

Abstract. This paper investigates protection strategies for WDM networks. We classify related work according to the level of abstraction. Several link and path protection schemes are described and qualitatively compared. Finally, the high problem complexity due to the large number of influencing parameters is shown and selected effects are shown using quantitative case studies.

1 Introduction

WDM (wavelength division multiplexing) technology is widely used to cope with rapidly increasing bandwidth demands. While at the moment point-to-point systems are already installed, “real” optical networks including optical routing and switching are approaching. Ring networks are promising for a first step towards optical networks due to reduced realisation complexity.

However, with the ever increasing bit rates handled by single network elements, also the impact of failures is increasing. Therefore, *protection* and *restoration* schemes become more and more important [8]. Both use spare capacities in the network to restore interrupted traffic: protection uses pre-calculated and pre-assigned protection resources for fast reaction in case of a failure, whereas restoration tries to make most efficient use of spare capacities available when a failure occurs. Restoration usually works slower than protection, but is in general more efficient and can deal also with “unexpected” failures. Thus, it is very probable that both schemes will be applied in real networks. Moreover, real networks will carry traffic with different priorities and also different “levels of protection”.

In this paper, we concentrate on protected traffic in WDM networks, i. e. all working paths have to be protected. The efficient design of a protected network was shown in literature to be a very complex problem with many parameters and degrees of freedom. The goal of this paper is first a short classification of already presented work according to the level of abstraction applied. Section 3 gives an overview of several different protection schemes and a qualitative evaluation for various criteria. Finally, we elaborate on the problem complexity by describing the large number of influencing parameters and their complex relationship and present a quantitative evaluation of some strategies. Throughout the paper, we use the expression “*channel*” to describe a wavelength channel on a single link, “*path*” to describe an end-to-end concatenation of wavelength channels (which may include wavelength conversion in some cases), and “*route*” to describe the way of either a channel or a path.

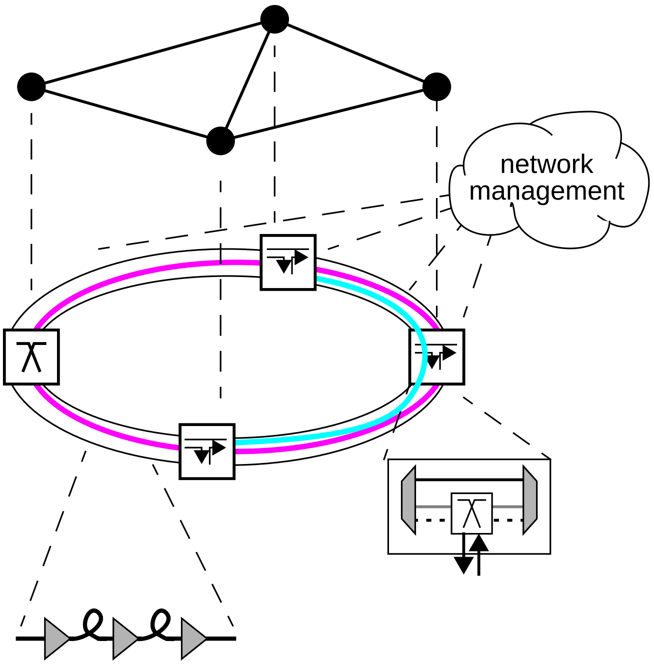
2 Classification of Related Work

In literature, many work on design and evaluation of protected networks is reported. However, due to the complexity of the problem many articles focus on specific aspects only and therefore comparisons between the reported results sometimes are difficult to make. In this section we try to classify some of the recent achievements by first introducing a classification scheme according to the “level of abstraction” and then giving a short survey of some recent reports.

2.1 Levels of Abstraction

Fig. 1 shows an example of defining different levels of abstraction for a classification of protection schemes. The abbreviations shown in the figure are used in the following section to classify articles.

On the highest level graph theoretical aspects are considered (as for example finding disjoint shortest paths or testing a network on k-connectivity). On the WDM network level we can distinguish two sub-levels: one dealing with routing of wavelength channels and dimensioning network resources, the other with additional consideration of switching functionality in network nodes. The element level looks at realising network resources (mainly nodes) in more detail by considering network elements from a functional point of view. The lowest level of abstraction considers physical effects. Finally, also network operation and management aspects are important when comparing protection schemes. Such a classification could be extended in several ways. For example, a more detailed level structure is possible, or multiple network layers could be considered in addition to the WDM layer.



graph level (**G**)
- path search
- disjoint paths
- topological aspects

management aspects (**M**):
- operation
- signalling

WDM network level (**N**)
- routing of wavelength channels and dimensioning (**N1**)
- switching functionality (**N2**)

element level (**E**)
- node realisation aspects
- components

physical level (**P**)
- transmission aspects
- signal degradation

Figure 1: Levels of abstraction for considering protection schemes

2.2 A Short Survey of Related Work

In table 1 on page 3 we give a short overview of some recent articles covering protection schemes for optical networks. Many more references can be found in the mentioned contributions and for example in [10] and [11]. Moreover, many (indeed most) of the listed articles cannot be assigned to one group exclusively because they cover different aspects. But usually, one or two aspects are treated dominantly in which case they were used for a classification. In addition to the groups listed in Fig. 1 there are also “overview articles” which will be marked with ’O’ in table 1.

3 Qualitative Comparison of Protection Schemes

This section classifies and evaluates qualitatively several protection schemes. We consider how the protection paths are routed, i. e. compared with Fig. 1 we concentrate on the WDM network level. In literature, other criteria are used as well, e. g. whether 1+1, 1:1, m:n, ... is applied. These criteria could be additionally applied to enhance our scheme. In section 3.2 we consider additional parameters for a comparison, e. g. on what granularity the schemes work or whether sharing is possible.

3.1 Classification and Description of Protection Schemes

We distinguish two basic groups for classification, namely *link* and *path protection* mechanisms (Fig. 2). The most simple link protection scheme (L0) duplicates all link equipment, i. e. spare capacities are installed parallel to the working capacities. This corresponds to a simple “network doubling” and is not considered any more in the following. Similar to this is scheme L1, which installs dedicated protection capacities equal to full link working capacities for all links on physi-

Table 1: Selected references related to protection schemes for WDM networks

article	group	central contribution
[1]	N1, G	Design algorithm to route “clear channels” in such a way that the virtual topology remains protected in case of a physical failure
[2]	G, E	APS link protection in arbitrary networks by applying full network coverage with uni-directional protection rings
[3]	N2, E	Efficient APS method and required node architecture and functionality for WDM rings with limited wavelength conversion
[4]	O	Evaluation of ring networks, especially Coloured Section Ring and Optical Multiplex Section Shared Protected Ring, focus on cost aspects; results from EURESCOM P615
[5]	O, N	Description, classification and qualitative comparison of several survivability methods
[6]	G, E	Protection overlay using 3-node subnetworks as building blocks to realise APS
[7]	N1, N2	Overlay rings in meshed networks for link protection on fibre basis
[9]	G, N1	Assignment of rings to cover each traffic demand on a single ring; scheme can be enhanced for protection paths

cally disjoint, i. e. independent routes. Scheme L2 covers all network links with rings (Fig. 3). A ring protects all links along its route which requires a ring capacity equal to the highest link capacity occurring around the ring. L3 enhances this scheme by allowing to split the traffic of a link onto multiple rings covering this link. In the example of Fig. 3, the traffic of link 2–5 could be protected in part by ring 1 and 2, respectively. This is especially advantageous for very heavily loaded links in a network with unsymmetrical loads. Scheme L4 uses more sharing of protection capacities by making multiple use of the spare ring capacities. In Fig. 3 for example, the spare capacity along link 2–5 would be shared between rings 1 and 2. This allows a more efficient use of spare capacities. But in case of a failure some kind of signalling is required to assign the spare capacities to the affected ring. However, in case of bi-directional traffic, this can be done by simply detecting the signals in the nodes at both ends of a shared link.

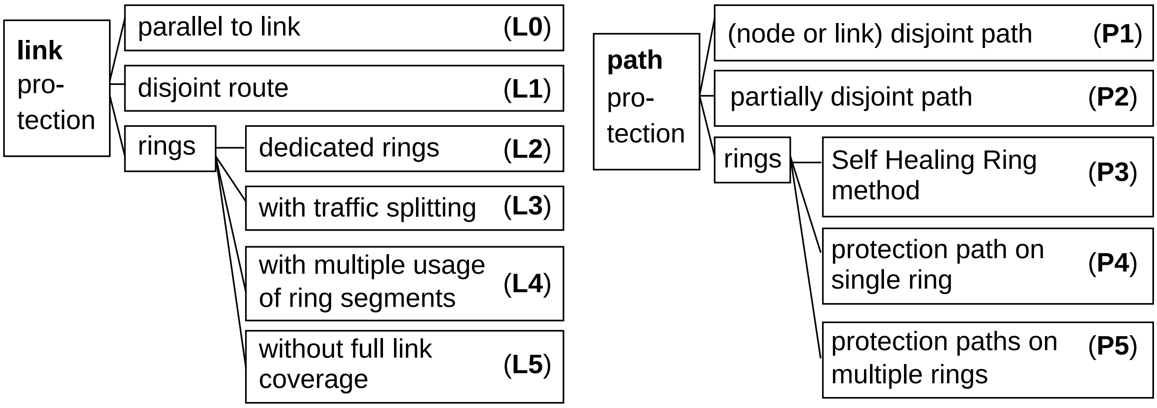


Figure 2: A possible classification of protection mechanisms

The last link protection scheme considered here (L5) does not require a complete coverage of all links in the network: a link may also “cross” a ring, i. e. only the terminating points of a link are located on a ring. Fig. 4 gives an example where link 2–5 is protected by ring 1. This scheme allows rather efficient use of spare capacities (dependent on network topology and traffic pattern) and protection switching is still very simple. Only the terminating nodes of an affected link have to react in case of a failure. All other nodes along a ring remain in their default configuration which simply forwards the protection channels or fibres. Similar schemes were investigated also in [7].

The second group consists of path protection mechanisms which protect a complete end-to-end path. The most simple cases are using completely link or node disjoint paths (P1). Scheme P2 uses partially disjoint paths: for each possible link (or node) failure along a path, a protection path is

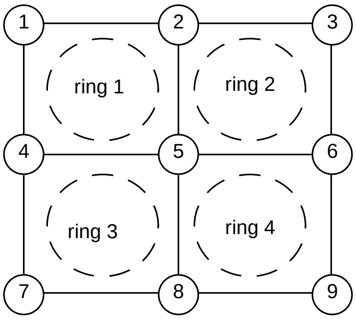


Figure 3: Example for network coverage with rings (L2, L3, L4)

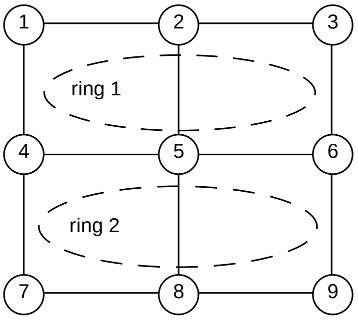


Figure 4: Link protection with rings without full coverage (L5)

assigned which avoids the failed segments but may re-use other parts of the original path. Fig. 5 gives an example for the path 1–4–7–8–9 and two possible link failures. This scheme is only useful if spare capacities are shared among multiple working paths. This allows a very efficient use of spare capacities but requires on the other hand high signalling efforts.

The following path protection schemes are all based on protection rings. P3 corresponds to a concept similar to the well-known SDH Self-Healing-Ring concept where working and protection paths are routed along two “halves” of a ring. With P4 we propose a scheme where working paths can be routed arbitrarily in a meshed network, but protection paths are routed along a single ring. The ring assignment has to be done in such a way that protection and working path are disjoint. For this scheme all node pairs terminating a working path have to be covered by one single ring. Fig. 6 shows one solution for a full network coverage and a protection assignment for path 1–2–5–6–9.

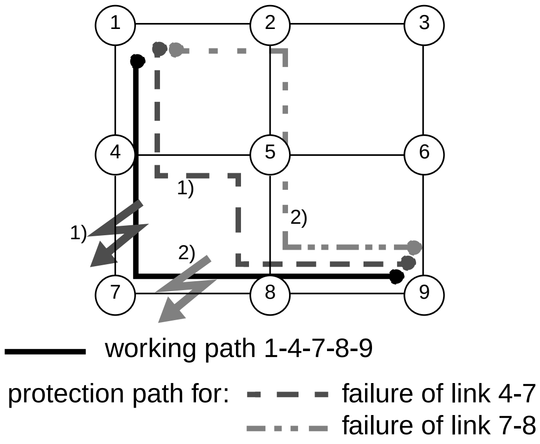


Figure 5: Path protection with partially disjoint protection paths (P2)

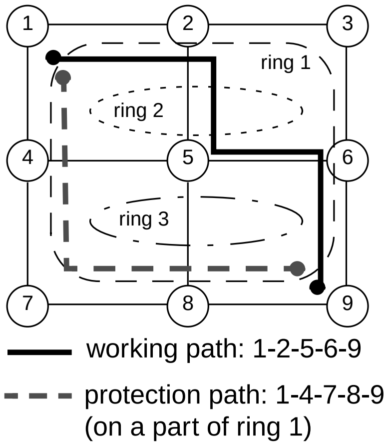


Figure 6: Path protection along a single ring (P4)

This scheme can be further enhanced by allowing a coverage of a working path by multiple rings, i. e. the complete end-to-end path is protected by several rings each protecting only a segment of the path (P5). Instead using a single ring, in Fig. 6 the working path could also be protected by rings 2 and 3, while ring 1 is no longer needed: the first part (1–2–5) is protected by ring 2, the second part (5–6–9) is protected by ring 3. This increases flexibility and efficiency of the scheme. However, it leads to higher complexity because signalling between nodes terminating a segment is required. If link 2–5 fails in our example, nodes 1 and 5 have to know to which ring segment the traffic has to be switched. This type of signalling is simpler and faster than the end-to-end signalling required for P2 but it requires more functionality in the “ring interconnection” nodes (node 5 in our example) which usually will have to work on a wavelength channel basis.

3.2 Qualitative Comparison of Selected Schemes

The following table compares the schemes described above qualitatively. “+” (“++”) denotes (very) advantageous properties of the scheme for the considered parameter, “0” means an average behaviour, whereas “-” (“--”) depicts (strong) drawbacks. However, it has to be considered that an exact evaluation of a scheme for a specific case study depends on many parameters. Some of these relationships are presented in more detail in section 4.

Table 2: A qualitative comparison of protection schemes

	L1	**L2**	**L3**	**L4**	**L5**	**P1**	**P2**	**P3**	**P4**	**P5**
efficiency	– –	–	0	0/+	+	–	++	–	+(+)	++
signalling requirem.	++	++	++	–	++	++	–	++	++	–
restoration speed	++	++	++	0	++	+	– –	+	+	0
flexibility	++	++	++	0	0	–	0/+	– (–)	– (–)	–
granularity	w/f	w/f	w/f	w/f	w/f	w	w	w	w	w
length increase	0/+	0/+	0/+	0/+	0/–	+(+)	++	0/–	0/–	0
sharing	poss.	poss.	poss.	yes	yes	poss.	yes	no	yes	yes

The first line evaluates how efficient spare capacity is used by a scheme. With *flexibility* we mean the suitability of a protection scheme to cover reconfigurations of working paths due to traffic changes which do not need additional capacity. Here, schemes which impose strict requirements on the protection design (e. g. path routes along rings) are in general less flexible than link protection schemes which are more or less independent of the working path assignment. Moreover, all link protection schemes can work on a wavelength basis (*w*) or on a fibre basis (*f*; corresponds to the Optical Multiplex Section level OMS) whereas path protection schemes usually are used only on a wavelength basis (although for special cases also a protection on fibre basis is possible). *Length increase* of protection routes compared to working routes may be critical, thus schemes with small length increases are advantageous. Additionally, for some schemes sharing is possible (*poss.*) although in the table above for these schemes (L1, L2, L3, P1) a dedicated protection is considered. For many other schemes some kind of sharing is implicitly used (*yes*).

The table above is not exhaustive. For example also the failure scenarios covered by a protection scheme could be considered (i. e. whether only link or also node failures are protected, or whether only single or multiple failures are protected).

4 Results

This section first describes a variety of parameters influencing the protection design. The large number of parameters leads to a high problem complexity. Therefore, in many studies reported in literature several parameters are neglected or arbitrarily fixed. Although this may be inevitable to get the problem tractable, it has to be kept in mind that a generalisation of results may be critical. In sections 4.2 to 4.4 selected results are shown which are representative examples out of many studies performed.

4.1 Overview of Influencing Parameters

Fig. 7 shows various parameters with a strong influence on the design of a protected network (i. e. basically on performance and cost of a planning solution). Apart from “obvious” parameters as protection strategy, topology, or technology, also other parameters have to be considered. For example, traffic characteristics have a large impact: results depend not only on absolute traffic volumes, but also on geographical distribution. Moreover, the solution approach is important. There are differences between the basic methods (e. g. linear or non-linear optimization, iterative or integrated dimensioning, ...) but also more “subtle implementation details” such as ring design (see next section) or path search orders may have a big influence.

4.2 Influence of Topology and Ring Assignment

It is well-known that the network topology has a strong influence on the performance of protection schemes – some schemes achieve good results for densely meshed networks, others for scarcely meshed ones. Thus, we used a network generator which allows automatic creation of many network examples. In Fig. 8 we show the ratio between number of protection channels (i. e. channels counted

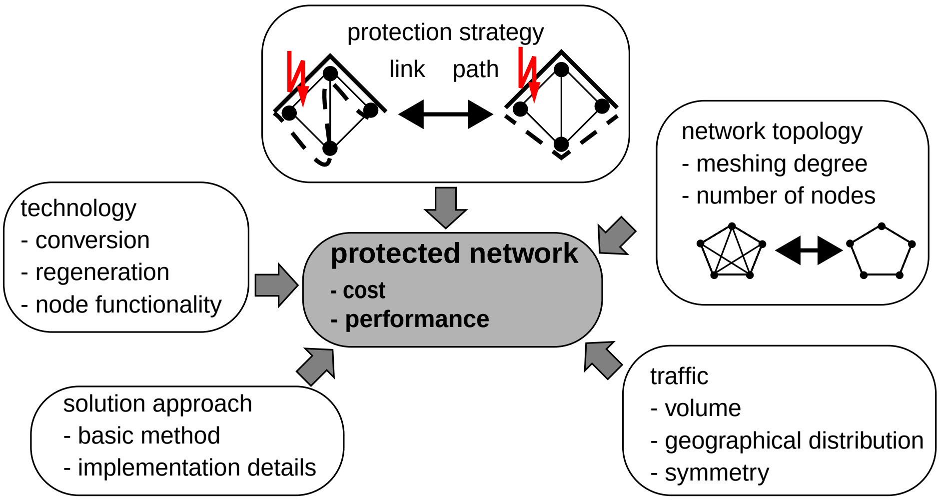


Figure 7: Parameters with strong influence on protection design

link-by-link) and total number of channels (i. e. working and protection channels) for two variants of link protection scheme L5 which differ only in the ring design algorithm. The result is shown for a network with 10 nodes and a varying number of bi-directional links (45 links corresponds to a full mesh). All links carry the same traffic load.

Fig. 8a) shows that with the link protection strategy using long rings the network can be dimensioned more efficiently with an increasing number of available links. The reasons are that i) more links can be protected by one ring, and ii) there are more chances to avoid unnecessary duplicate covers for certain links. However, Fig. 8b) reveals that this behaviour depends on the size of rings used to protect the network. For short rings, the efficiency – which is for a low number of links comparable or even slightly better than with long rings – is nearly independent of network topology.

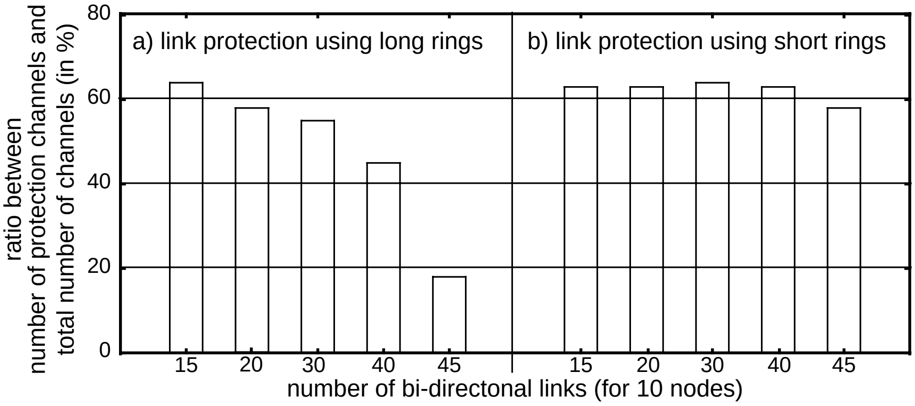


Figure 8: Variation of protection channel requirements for different topologies and ring assignment strategies

4.3 *Influence of Traffic Pattern on Link Protection Schemes*

The following figure presents the influence of the geographical traffic distribution in a network for the same total amount of working channels. The required number of protection channels is shown for different link protection schemes for a network with 10 nodes and 30 bi-directional links. In Fig. 9a) all links are equally loaded. It can be seen that the protection schemes based on rings are significantly better than the simple scheme based on dedicated disjoint routes. Moreover, large rings are better than short rings, but the differences between various schemes using large rings are rather small.

Fig. 9b) compares the same strategies for very unsymmetrical loads on the links. Now, differences between ring based schemes and L1 are reduced because the achievable efficiency for ring based schemes decreases. This is due to the fact that the ring capacity must correspond to the largest link

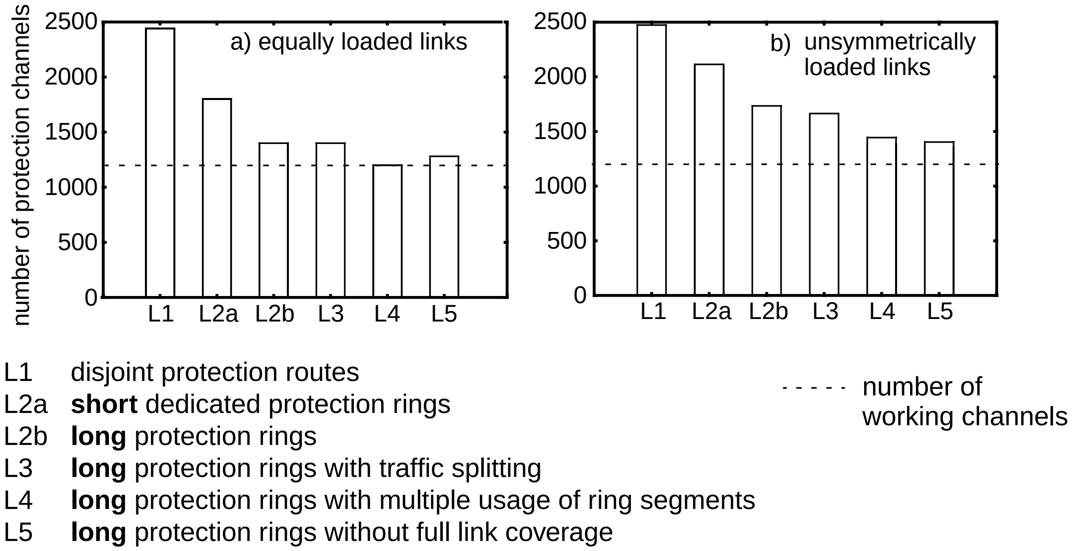


Figure 9: Required protection channels for different link protection schemes

capacity occurring along a ring. But on the other hand ring schemes itself reveal large differences: only schemes L4 and L5 are capable of dealing with this unsymmetrical traffic pattern rather efficiently.

Finally, it has to be mentioned that the results shown describe the mean values of many optimization runs with differing traffic patterns and ring designs. However, for some "extreme" cases the results differed significantly: a scheme with rather low efficiency in the mean nevertheless could achieve the best result for some specific cases.

4.4 Comparison of Link and Path Protection Schemes

A first conclusion from the previous results – which were confirmed for many scenarios – is that the picture is very complicated due to complex relationships between topology and parameters such as ring selection strategies, traffic patterns, or other parameters not shown here as for example conversion capabilities. Nevertheless, we try to make a comparison of different protection strategies in this section keeping in mind that for certain scenarios the outcome may be different.

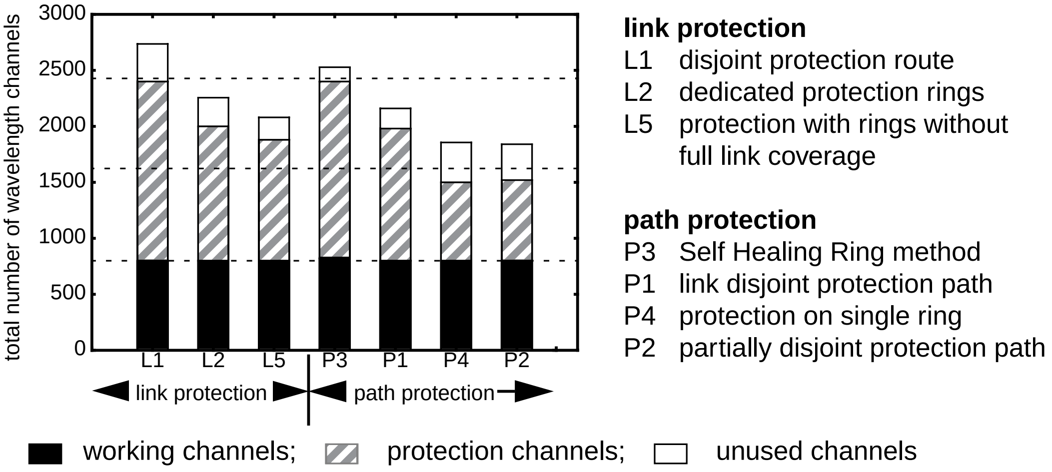


Figure 10: Channel requirements for different protection schemes

Fig. 10 compares channel requirements for different link and path protection schemes for the following parameters: the network consists of 8 nodes and 16 bi-directional links, there is no conversion capability in the network and between all node pairs the same traffic demand has to be fulfilled. The results – which are representative for many other configurations – confirm the basic trade-off between "efficiency" and the parameters discussed in section 3.2. In general, we see that path protection schemes can be more efficient although the total numbers – especially for the unused channels – strongly depend on specific values for the amount of traffic and also on the applied WDM scheme (i. e. number of channels per fibre). Especially the schemes P2 and P4 are very efficient. However, the signalling required for P2 (and therefore the achievable protection time) is rather high so that scheme P4 appears to be a very promising path protection approach.

5 Conclusions

This paper investigated protection mechanisms for WDM networks. A scheme based on abstraction levels to classify the variety of mechanisms was presented and used to classify some of the work reported in recent literature. Furthermore, several link and path protection schemes were described and qualitatively compared by considering in addition to spare capacity requirements other parameters such as signalling requirements or flexibility against changing traffic patterns. Then, we have shown that a large number of parameters such as topology, technology or traffic patterns influence the performance of a network design and that there are complex relations between these parameters. Thus, generalisations from studies where several parameters are fixed (which is necessary in many cases due to the complexity of the problem) are very difficult to make. Moreover, we presented some selected results showing the influence of protection strategy, network meshing degree, geographical traffic distribution, and algorithmic details on the performance of the protected network design. A proposed path protection scheme using ring covers turned out to be very efficient while at the same time signalling complexity is low. Finally, it has to be stated that a selection of a specific protection strategy for a network depends not only on the efficiency of the scheme, but also on many other parameters shown in table 2.

Further work will focus on improvements by using enhanced optimization processes or an integrated design of working and protection capacities. In addition, the consideration of traffic with different protection levels (e.g. fully protected, restorable, or non-protected) in one network will lead to new problems such as the development of a strategy for an efficient sharing of spare capacities.

Acknowledgement

The authors thank Volker Feil for his valuable support to design the planning tool. This work has been supported in part by the German BMBF (Bundesministerium für Bildung, Wissenschaft, Forschung und Technologie) under contract 01 BP 504/2.

References

[1] J. Armitage et al., “Design of a survivable WDM photonic network”, *IEEE Infocom 1997*, pp. 244-252

[2] G. Ellinas, T.E. Stern, “Automatic protection switching for link failures in optical networks with bi-directional links”, *GLOBECOM 96*, paper 4-4

[3] O. Gerstel et al., “Fault tolerant multiwavelength optical rings with limited wavelength conversion”, *IEEE Journal on Sel. Areas in Comm.*, Vol. 16, No. 7, Sept. ’98, pp. 1166-1178

[4] T. Jakab et al., “Cost efficient optical ring architectures - results from EURESCOM P615 Project”, *8th Int. Telecom. Networks Planning Symposium (Networks ‘98)*, pp. 371-376

[5] L. Nederlof et al., “A comparison of survivability methods for the optical layer”, *NOC ‘97, Photonic Networks, Optical Technology and Infrastructure*, pp. 103-110

[6] F. Tillerot et al., “Efficient network upgrade based on a WDM optical layer with automatic protection switching”, *Proceedings of the OFC 1998*, p. 296f

[7] B. Van Caenegem et al., “Implementation approaches for spare capacity in meshed WDM transport networks”, *IEEE/LEOS Symposium BENELUX*, 1997, pp. 97-100

[8] T.-H. Wu, *Fiber Network Service Survivability*, Artech House, 1992

[9] L. Wuttisittikulkij, M.J. O’Mahony, “Design of a WDM network using a multiple ring approach”, *GLOBECOM ’97*, pp. 551-555

[10] IEEE Journal on Selected Areas in Communications, *Special Issue on High-Capacity Optical Transport Networks*, Vol. 16, No. 7, September 1998

[11] *Proceedings of the Optical Fiber Communications Conference (OFC) ’99*