Resilient Optical Network Design:

Advances in Fault-Tolerant Methodologies

Yousef S. Kavian
Shahid Chamran University of Ahvaz, Iran

Mark Stephen Leeson
University of Warwick, UK

Information Science
REFERENCE

Managing Director:	Lindsay Johnston
Senior Editorial Director:	Heather Probst
Book Production Manager:	Sean Woznicki
Development Manager:	Joel Gamon
Development Editor:	Michael Killian
Acquisitions Editor:	Erika Gallagher
Typesetters:	Adrienne Freeland
Print Coordinator:	Jamie Snavely
Cover Design:	Nick Newcomer, Greg Snader

Published in the United States of America by
Information Science Reference (an imprint of IGI Global)
701 E. Chocolate Avenue
Hershey PA 17033
Tel: 717-533-8845
Fax: 717-533-8661
E-mail: cust@igi-global.com
Web site: http://www.igi-global.com

Copyright © 2012 by IGI Global. All rights reserved. No part of this publication may be reproduced, stored or distributed in any form or by any means, electronic or mechanical, including photocopying, without written permission from the publisher. Product or company names used in this set are for identification purposes only. Inclusion of the names of the products or companies does not indicate a claim of ownership by IGI Global of the trademark or registered trademark.

Library of Congress Cataloging-in-Publication Data

Resilient optical network design: advances in fault-tolerant methodologies /
Yousef S. Kavian and Mark Stephen Leeson, editors.
p. cm.
Includes bibliographical references and index.
ISBN 978-1-61350-426-0 (hardcover) -- ISBN 978-1-61350-427-7 (ebook) -- ISBN
978-1-61350-428-4 (print & perpetual access) 1. Optical communications--
Reliability. 2. Fault tolerance (Engineering) I. Kavian, Yousef S., 1978-
II. Leeson, Mark Stephen, 1963-
TK5103.59.R46 2012
621.382'7--dc23

2011038349

British Cataloguing in Publication Data
A Cataloguing in Publication record for this book is available from the British Library.

All work contributed to this book is new, previously-unpublished material. The views expressed in this book are those of the authors, but not necessarily of the publisher.

Chapter 10

New Dimensions for Survivable Service Provisioning in Optical Backbone and Access Networks

Paolo Monti
Royal Institute of Technology, Sweden

Cicek Cavdar
Royal Institute of Technology, Sweden

Jiajia Chen
Royal Institute of Technology, Sweden

Lena Wosinska
Royal Institute of Technology, Sweden

Andrea Fumagalli
The University of Texas at Dallas, USA

ABSTRACT

Originally, networks were engineered to provide only one type of service, i.e. either voice or data, so only one level of resiliency was requested. This trend has changed, and today's approach in service provisioning is quite different. A Service Level Agreement (SLA) stipulated between users and service providers (or network operators) regulates a series of specific requirements, e.g., connection set-up times and connection availability that has to be met in order to avoid monetary fines. In recent years this has caused a paradigm shift on how to provision these services. From a "one-solution-fits-all" scenario, we witness now a more diversified set of approaches where trade-offs among different network parameters (e.g., level of protection vs. cost and/or level of protection vs. blocking probability) play an important role.

This chapter aims at presenting a series of network resilient methods that are specifically tailored for a dynamic provisioning with such differentiated requirements. Both optical backbone and access networks are considered. In the chapter a number of provisioning scenarios - each one focusing on a specific Quality of Service (QoS) parameter - are considered. First the effect of delay tolerance, defined as the amount of time a connection request can wait before being set up, on blocking probability is investigated when Shared Path Protection is required. Then the problem of how to assign "just-enough" resources to meet each connection availability requirement is described, and a possible solution via a Shared Path Protection Scheme with Differentiated Reliability is presented. Finally a possible trade off between deployment cost and level of reliability performance in Passive Optical Networks (PONs) is investigated.

DOI: 10.4018/978-1-61350-426-0.ch010

Copyright © 2012, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

The presented results highlight the importance of carefully considering each connection's QoS parameters while devising a resilient provisioning strategy. By doing so the benefits in terms of cost saving and blocking probability improvement becomes relevant, allowing network operators and service providers to maintain satisfied customers at reasonable capital and operational expenditure levels.

INTRODUCTION

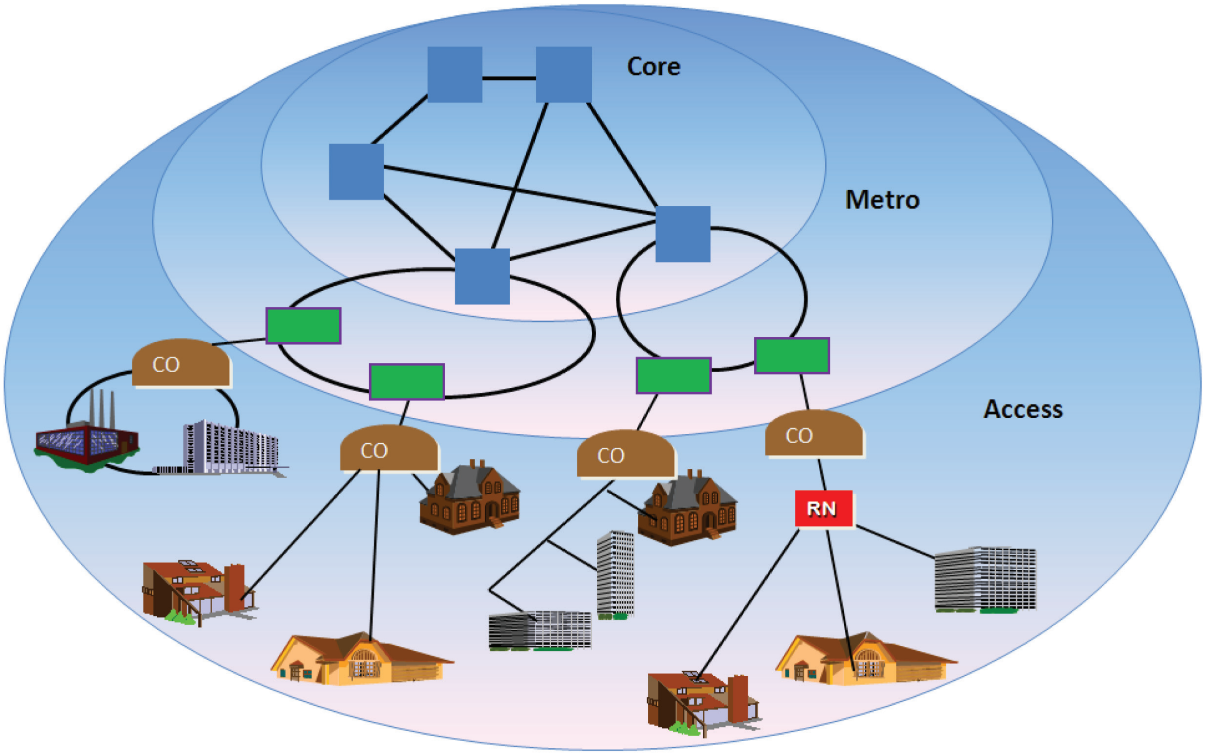
Wavelength Division Multiplexing (WDM) enables optical networks to transport hundreds of wavelength channels through a single optical fiber, with a capacity that currently varies from 10 Gbit/s to 40 Gbit/s for each channel, and that is expected to reach 100 Gbit/s in the near future (Ray, 2010). Moreover, one single fiber cable consists of a large number of optical fibers, and an accidental single cable cut may lead to the interruption of a very large number of optical connections with the likely interruption of an enormous amount of services. For this reason it is extremely important to provide efficient survivability mechanisms in optical networks. With this regard a lot of work can be found in the literature that addresses the resiliency problem in both optical core (Mukherjee, 2006) and access networks (Chen, Mas Machuca, Wosinska & Jaeger, 2010; Yeh & Chi, 2007; Chan, Chan, Chen & Tong, 2003).

The term *core* refers to the backbone infrastructure of a network that usually interconnects large metropolitan areas, and may span across nations and/or continents (Figure 1). Usually interconnected in a mesh pattern the backbone nodes aggregate and transmit traffic from and to the peripheral areas of the network (i.e., the metro/access segment). The term *access* refers to the so called *last mile* or segment of a network where central offices (COs) and remote nodes (RNs) provide connectivity, using tree topologies, between the end users and the rest of the network infrastructure. Depending on the reach of the access segment core and access may or may not be interconnected via a metro infrastructure. With short reach access solutions (i.e., the CO is placed a few tens of kilometers from the end users) the traffic from the end users is aggregate at the metro level before being sent to the core. With long reach access solutions (i.e., the CO is more than one hundred kilometers from the end user) the traffic goes directly from the access into the core segment.

Most of the attention was earlier devoted to reliability methods that were able to provide resiliency to all optical channels, or *lightpaths*, indistinctly. This was motivated essentially by the fact that in the absence of survivability mechanisms the first priority was to develop solutions that provide uninterrupted services in the case of network link or node failures. Another reason for this flat architecture was the nature of the services carried over the lightpaths. Historically, networks were engineered to provide only one type of service, i.e. either voice or data, so only one level of resiliency was needed.

This trend has changed now and today's approach in providing network connections is quite different. Network operators and service providers integrate an increasing number of services with different resilience requirements in the same network. These services are different in nature, e.g., real time versus background data transfer, as well as in their scope, e.g., critical financial transactions versus recreational activities (Cholda, Mykkeltveit, Helvik, Wittner & Jajszczyk, 2007). Examples of this differentiated scenario are optical networks with dynamic connection provisioning where specifics services, e.g., Video-on-Demand (VoD) requests to corporation and backup virtual private networks (VPNs), may require bandwidth capacity during specific time intervals with flexible or strict connection set-up times and differentiated reliability requirements. Another example is bandwidth on demand (BoD) services

Figure 1. Telecom network hierarchy example: core, metro and access segment



with differentiated reliability requirements that enables the customer to order and receive the desired connectivity within hours or minutes of the request. Such services are already provisioned by a large US carrier in the form of Real-Time BoD and Scheduled BoD (Liu & Chen, 2007). Along the same concept, another large US carrier's On-time Provisioning service guideline specifies a deadline for each service order and gives the customer the right to withdraw the request if the carrier cannot set-up the required service within the specified amount of time (ATT, 2009). Table 1 presents a few examples of mapping of specific services with their respective requirements. These requirements are often specified as part of the Service Level Agreement (SLA) between the client and the operator and it is clear that given such a plethora of requirements a "one-solution-fits-all" approach for network resilience is not efficient.

This strong focus on strict end-to-end requirements for the provisioned services has also triggered a growing interest on how and up to which level resiliency is provided in optical access networks. It is known that fiber access networks without any protection are characterized by poor reliability (Tran, Chae & Tucker, 2005; Wosinska & Chen, 2008). Therefore, some type of protection should be provided to satisfy the resiliency requirements of the network services. Obviously, adding redundant components and systems will improve network reliability. However, in the access the network costs are shared by a limited number of users. Therefore, both system deployment cost and network management cost should be minimized.

The objective of this chapter is to present a series of network resilience methods that are specifically tailored to offering a dynamic provisioning scenario with such differentiated

Table 1. Service differentiation for sample services

Services	Availability	Holding Time	Set-up time
Sensitive Services (Telemedicine, Financial Trans.)	.99999	Known	Medium
Grid computing	.999	Known	High
Video on demand (VoD), IPTV	.999	Known	Low
Voice Trunks	.9999	Not known	Low
Backup Storage	.99	Flexible	Medium

requirements. In particular the focus will be on three specific parameters: connection establishment time, connection availability and deployment costs of protection resources. The contribution is threefold spanning across both the optical core and access network. In the first part, this chapter presents a protection provisioning algorithm for core networks able to take advantage of the temporal dimension requirements that a specific service has. In particular, the strategy presented makes use of a connection request's holding time and delay tolerance. In the second part, the chapter still focuses on core networks and will investigate a protection strategy that assigns spare resources to connections based on their specific survivability level requirements. More specifically the presented protection algorithm explores the tradeoff between the service availability level and how efficiently network resources are used, measured in terms of connection blocking probability. Finally, the chapter addresses the problem of resiliency in optical access networks with particular focus on deployment cost. A series of protection schemes are presented and compared in terms of level of protection provided versus cost per user.

The chapter is organized as follows. First some background information about survivability techniques and connection availability computation is provided. Then each contribution is presented in separate subchapters. Finally some concluding remarks are provided.

BACKGROUND

This section provides an introduction on how to categorize today's survivability techniques in networking, followed by a brief tutorial on the computation of the value of the connection availability. These notions will be helpful to understand a few important concepts that will be used later in the chapter.

Unused capacity, available in the optical links, can be assigned for protection purposes, making the network survivable, i.e., *resilient*. There are two ways of protecting traffic: *path protection* and *link (or segment) protection*. In path protection schemes the traffic disrupted by a fault is rerouted along a different path between the source and destination nodes. Therefore, each node pair requires an additional link or node disjoint path depending on the type of failure the connection needs to be protected from. In link protection schemes the traffic is rerouted around the failed link only.

Network survivability schemes can be classified in two groups, i.e., *protection* and *restoration* (Mukherjee, 2006). Protection refers to pre-provisioned backup resources allocated for failure recovery. Protection schemes are typically fast and they can offer recovery time below 50 ms. They can offer various protection levels ranging from 1+1 and 1:1 (i.e., *dedicated* protection), to M:N (i.e., *shared* protection). In 1+1 protection, the traffic is transmitted simultaneously on two distinct paths from the source to the destination.

The destination node selects from which path it receives the incoming traffic. In case of a fiber or node failure, the destination node has to switch over to the other path to avoid interruption in data reception. In 1:1 protection, there are also two separate paths between the end nodes. In this case, the transmission takes place only on one path, the working path. In case of a fiber cut, both nodes have to switch to the other path, the protection path. With the M:N protection N working paths share M protection paths. Only single fiber or node failures can be protected while, in the event of multiple failures, survivability is not guaranteed. Protection techniques, however, can be quite expensive due to the need for extra network equipment. Restoration on the other hand refers to the rerouting of traffic around the point of failure if there are resources available. The alternative route is discovered or reserved on the fly. For this reason restoration usually takes longer time than protection. If sufficient network resources are not available upon failure, restoration is not possible.

A parameter often used to define and differentiate the level of protection is the connection asymptotic *availability*, which is referred to as the probability that a connection is up at an arbitrary point in time. The computation of this parameter is not always simple, i.e., as the complexity of a network increases analytical availability calculation becomes more and more time consuming. It is often very hard or even impossible to include all parameters from a real network in the analytical availability calculation. There are two methods that can be used to compute availability: Markovian models and Monte Carlo simulations. They are briefly described next.

The basic assumption for Markovian models is the exponential distribution of time between failures and reparation time. This approximation reflects the real behavior of electronic and photonic component failures during their operational time. The availability for a structure is derived using state transition diagram devised for a certain network. A working state of a component is changed to a non-working state by the occurrence of a failure and the opposite transition occurs as a consequence of a repair action. The state of a connection in the network is evaluated from the component states according to logical expressions that describe the relationship between component events (failure/repair) and the state of a connection (working or non-working state). Basic parameters for each Markov availability model are the component failure rate and the reparation rate.

Monte Carlo simulation can be used to generate the times to failure (*TTF*) and the time to repair (*TTR*) of components in the network. Each *TTF* and *TTR* is derived from a random number generator with a defined probability density function (PDF) that is component related. Statistical data related to the occurrence of a specific component failure is collected during the component lifetest or by measuring *TTF*s for already deployed systems. By monitoring real optical links one can distinguish between failures of cables and failures of optical/electronic devices. By monitoring the maintenance data from the field, the PDF for *TTR* can be estimated. The mean time to failure and the mean time to repair can then be calculated as the mean value of the corresponding PDFs. Each component changes randomly from a working to a non working state. The impact of each component state change is analyzed and a decision is then made whether the connection state is affected by the component state change or not. The connection mean uptime T_{up} and mean downtime T_{down} are then cumulatively calculated. When the simulation is completed the asymptotic connection availability A is computed as:

$$A = \frac{T_{up}}{T_{up} + T_{down}}. \tag{1}$$

The availability calculation based on Monte Carlo simulation also introduces a *simulation error* but the number of simulation iterations can bound this error. Unfortunately, desirable accuracy may require long simulation runs. In addition, the time complexity of the simulation is a function of the number of network elements and the level of network redundancy. In a highly redundant network some network events are very rare and require many single or multiple element failures, including dependent failures, to be simulated before being able to measure the desired outcome.

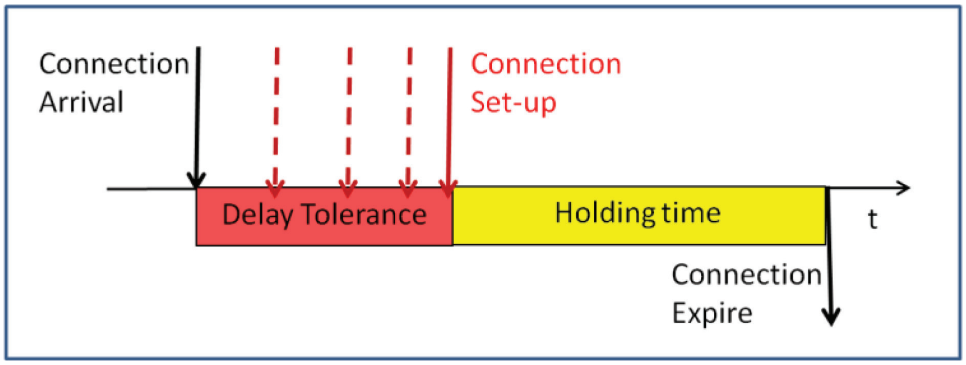
DYNAMIC SCHEDULING OF SURVIVABLE CONNECTIONS IN OPTICAL WDM NETWORKS

User-controlled, large-bandwidth, on-demand services with differentiated timing requirements will play an important role in the future Internet. Connections are set up and released for specific time durations, with sliding or fixed set-up times, for applications such as video-on-demand, IPTV, backup storage, grid computing, and collaborative solutions in finance and R&D. With the development of (*i*) new and agile switching devices, and (*ii*) control and management plane architectures such as Automatically Switched Optical Networks (ASON) and Generalized Multiprotocol Label Switching (GMPLS), optical WDM networks are now able to provide dynamic circuits to meet the high bandwidth requirements of these dynamic services.

To characterize resource requirements for such applications, scheduled traffic models have been proposed by Cavdar *et al.* (2010). In this subchapter, we focus on dynamic scheduling of survivable connections with flexible set-up times. After a customer issues a connection request, the customer waits for a response. The request is accepted or rejected according to the network operator's ability to provide the required level of service quality. If the connection request cannot be satisfied and set up within a certain amount of time, say t_d, the customer withdraws the request. We call t_d the *delay tolerance* of the customer, which describes a customer's patience, i.e., the maximum duration a customer is willing to wait until the connection is set up (Figure 2). Delay tolerance of a connection request can be defined as a service-level specification (SLS) stated in a contract known as the service-level agreement (SLA), which is explained in detail by Clemente *et al.* (2005).

The network performance can be improved by exploiting the various SLA terms in temporal dimension. In particular, this subchapter discusses the use of a connection request's holding time and delay tolerance, where holding time defines the time duration of the service. More specifically, we consider the dynamic scheduling of survivable connections with delay tolerance. We study the performance of a dynamic scheduling approach on shared-path protection (SPP) for

Figure 2. Connection set-up time can slide until the end of the delay tolerance



efficient capacity usage. The performance of different scheduling algorithms is compared and discussed, giving priority to requests according to their (*i*) arrival rates, (*ii*) delay tolerances, or (*iii*) holding times.

There has been a substantial amount of research on survivable connection provisioning in optical networks. In what follows we will categorize the existing work according to traffic models focusing mainly on scheduled traffic models. In general, traffic models can be classified into two groups: *unscheduled* and *scheduled.* In unscheduled models, time-domain specifications, such as holding time of a connection, are ignored. Connections are provisioned at the time they arrive according to the current network state, without considering the connection duration. But scheduled models consider the holding time of connections so that provisioning algorithms can optimize resources in both space and time. Both unscheduled and scheduled traffic models can be either static or dynamic. In a static traffic model, the set of traffic demands (unscheduled or scheduled) is known in advance. In contrast, for a dynamic traffic model, the arrival time and holding time of requests are generated randomly, based on certain distributions.

Set-up and tear-down times for scheduled traffic demands can be fixed, e.g., Li & Wang (2006), or they can be allowed to slide within a larger time window, e.g., Jaekel & Chen (2007), in which case they are called, respectively, fixed scheduled and sliding scheduled traffic demands. In a sliding scheduled traffic model, setup time slides within a time window, where the arrival time, holding time, and maximum end-time of the window are given. Tanwir *et al.* (2008) consider survivable routing and wavelength assignment for a sliding scheduled traffic model and use restoration to provide survivability.

Delay tolerance gives us the time difference between the window size and the holding time and can be used as a measure of flexibility of the time window. As the performance of provisioning algorithms with sliding scheduled demands is dependent on this flexibility, a larger ratio of delay tolerance to holding time can allow more effective temporal sliding and may lead to more efficient resource utilization. Delay tolerance, proposed first by Cavdar, Tornatore & Buzluca (2009) as a connection oriented metric, is defined by each connection request which allows sliding scheduling of the demands.

Significant work has been done for dynamic unscheduled traffic with shared-path protection (SPP), e.g., by Ou, *et al.* (2004) and SPP with differentiated reliability, e.g., Fumagalli, Tacca, Unghvary & Farago (2002). Moreover, with fixed set-up times, Tornatore *et al.* (2005) considers the a-priori knowledge of holding time for SPP and Cavdar *et al.* (2007) study holding time aware availability-guaranteed connection provisioning with SPP under dynamic traffic demands. SPP is also studied for static scheduled demand models with fixed window by Li & Wang (2006) and sliding window by Jaekel & Chen (2007). Dynamic provisioning of SPP has been studied with sliding scheduled connection requests by Cavdar, Tornatore & Buzluca (2009) with availability guarantee and by Cavdar *et al.* (2010) with the comparison of different scheduling policies. In this subchapter we will explain the problem of dynamic scheduling of shared-path protected connections with delay tolerance (SDT) and discuss the performance of different dynamic scheduling policies on SPP.

Shared Path Protection with Delay Tolerance (SDT)

This section first provides a formal definition of the shared path protection problem with delay tolerance (SDT), then three different algorithmic solutions are presented as a solution of the problem.

Problem Statement

Given: a) Physical topology of a network represented by a graph G with a set of links and nodes; W specifies the number of wavelengths on each link; b) a connection request R={s, d, t_a, t_h, t_d, n}, between source-destination pair (s,d) with arrival time (t_a), holding time (t_h), delay tolerance (t_d), and counter for retrials (n) to count each attempt to set up the connection request; c) a threshold (T) to restrict the number of retrials.

Output: A shared-path-protected connection comprehensive of a working path (l_w), a backup path (l_b), and setup time (t_s).

Objective: Minimize backup resource consumption and overall network blocking probability.

In SDT, if the network cannot provide a path pair for a specific request, the request is either delayed by sliding the set-up time for the delay tolerance duration, or it is rejected when the delay tolerance expires.

Backup Routing

Our reference algorithm finds primary and shared backup paths using a version of CAFES, which was proposed by Ou, *et al.* (2004). CAFES is a two-step, edge-disjoint path-pair algorithm. In the first step, a minimal cost working path (l_w) is computed, and then the link costs are updated to find a link-disjoint backup path (l_b) with minimal costs.

To keep track of backup resource utilization, we associate a conflict set v_e with a link *e*. To identify the sharing potential between backup paths, $v_e^{e'}$ denotes the number of backup wavelengths reserved on link e to protect primary paths passing through link *e*'. B(e) = number of wavelengths in the backup pool where shared wavelengths are reserved on link *e*, N(e) = number of connections which share wavelengths in the backup pool on link *e*, f(e) = number of free wavelengths on link e, and d(e) = distance of link e. In this study it is assumed that d(e)=1.

To calculate minimal-cost routes for backup paths, the link-cost calculation method proposed by Ou, *et al.* (2004) has been used for shared-path protection (SPP). As a primary objective, SPP encourages shareability, and minimizes hop distance. Therefore, cost C(e) for a candidate backup link e is calculated as follows:

$$C(e) = \begin{cases} \infty, \; \textit{if} \;\; e \in p \; \textit{or} \; \textit{if} \; f(e) = 0 \; \textit{and} \; \exists e' \in p, v_e^{e'} = B(e); & (2) \\ \varepsilon \times d(e), \; \textit{if} \; \exists e' \in p, v_e^{e'} < B(e); & (3) \\ d(e), \; \textit{otherwise}, \; \textit{if} \; f(e) > 0. & (4) \end{cases}$$

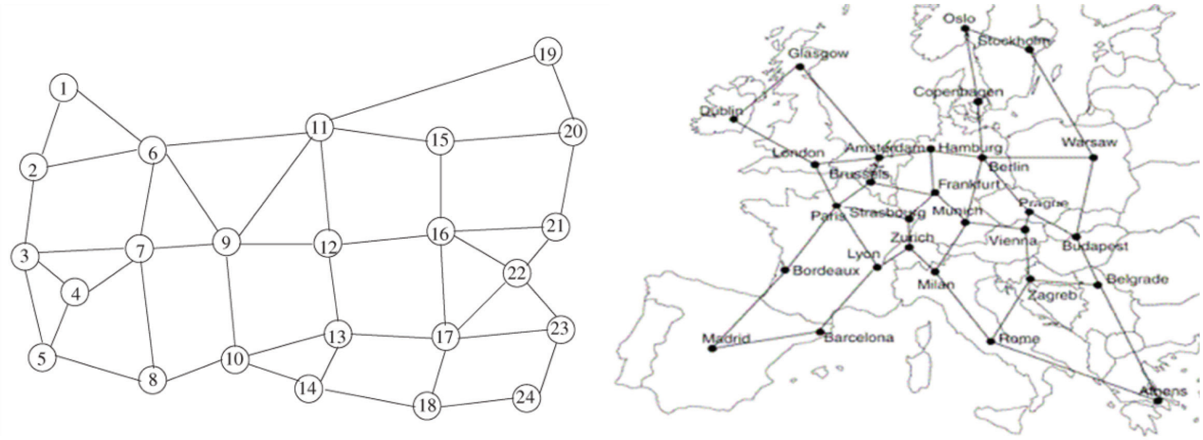
Case (2) (infinite cost) corresponds to insufficient resources on a link to set up the backup path. Case (3) (negligible cost) corresponds to the case of a shareable backup pool where there is no need to allocate extra spare capacity for the incoming connection. Case (4) (full cost) gives the cost of the link where a new wavelength needs to be added in the backup pool.

Different SDT Algorithms

To solve the SDT problem, we introduce three different algorithms, which give priority based on arrival rate, delay tolerance, or holding time of a connection request. Here, the requests that normally would be blocked by a conventional SPP approach are rescheduled by putting the request back into the queue for another set up attempt. For the details, the interested reader is referred to Cavdar, *et al.* (2010).

A request is rescheduled only if an existing connection in the network departs within the current request's delay tolerance (t_d). The connection request is then rescheduled immediately after the departure, and t_d is updated. The resources released with the departure of a connection request change the network state and provide an opportunity to find available resources. A rescheduling algorithm is then needed to assign priorities when more than one connection request are to be delayed after a departure. Three different scheduling strategies are considered:

Figure 3. Network topologies used during the performance evaluation phase



(a) USNET topology

(b) EON topology

- **Algorithm SDT_ar:** the main strategy in SDT_ar is prioritizing connections according to their arrival time, which is the traditional first-come-first-served (FCFS) queuing policy.
- **Algorithm SDT_dt:** gives priority to the impatient connection requests with smaller t_d in the queue.
- **Algorithm SDT_ht:** gives priority to requests with smaller holding time in the queue.

Illustrative Numerical Examples

For performance evaluation of three scheduling policies, a dynamic network environment is simulated. Connection arrivals follow a Poisson process with exponentially distributed holding time and delay tolerance, with each connection requiring one wavelength unit of bandwidth. Average delay tolerance (D) is normalized to the holding time, while the average holding time (H) has average equal to one. Therefore, offered network traffic load in Erlangs equals the arrival rate. In this study, we used 2 different network topologies: USNET with 24 nodes representing a backbone topology in US (Figure 3(a)); and EON with 28 nodes, representing a pan-European backbone network (Figure 3(b)). In both cases, each link has 16 bidirectional wavelength channels. In each experiment, 100000 unicast connection requests, symmetric and uniformly distributed among all node pairs, are considered. Each plotted value has a 95% confidence level, with confidence interval not larger than 0.05 of the plotted value except in case of very small value of blocking probability (BP).

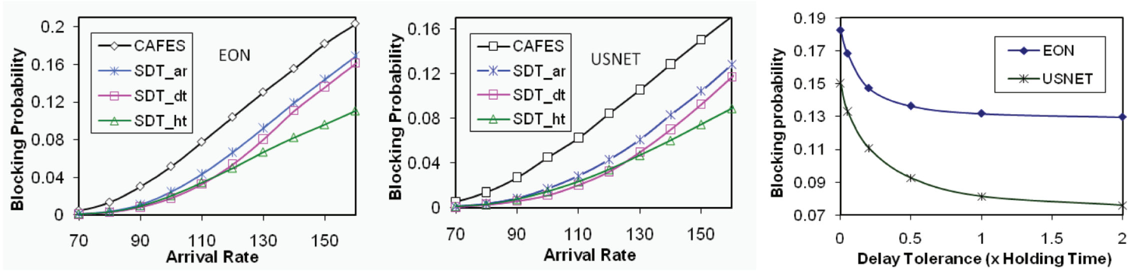
Figures 4(a) and 4(b) compare, in terms of BP versus arrival rate, the three different scheduling algorithms with CAFES, applied to USNET and to EON network topologies for D = 0.5. In order to have a fair comparison with CAFES, all three scheduling algorithms are based on the same routing strategy used in CAFES: two-step primary-backup routing without wavelength continuity constraint. Significant savings in BP are achieved at all load levels by applying SDT_ar, SDT_dt and SDT_ht in both topologies. The savings are larger for lower load values (e.g., 50% at arrival rate of 150 compared to 70% at 100 connections per time unit in USNET for SDT_ht). An asymptotic decrease of the gain is reached when the network load increases over a specific value in SDT_ar and SDT_dt, since connections wait in the queue for a restricted amount of time, delay tolerance. Nevertheless, although requests wait to be provisioned only for a limited time, SDT_ht achieves the best performance for high loads, because it gives priority to connections that remain in the system for shorter durations. Note that SDT_dt is superior to SDT_ar and SDT_ht for lower loads where BP is less than 8%. At low loads, it is better to give priority to impatient connections over requests with smaller holding times versus the priority that needs to be given at higher loads. For the more detailed results the reader is referred to the paper by Cavdar, *et al.* (2010) where it is also shown that there is no significant change in resource overbuild (which measures the usage of backup resources over primary resources) by applying SDT, except a slight decrease which occurs due to the increase in provisioning success rate. As a result, all three SDT algorithms bring significant gain in BP, without sacrificing resources for spare capacity usage.

Another important aspect is the duration of the delay tolerance (in our examples so far, D is normalized to the holding time of the connection). Longer delay tolerance allows more opportunities for re-scheduling and re-routing, especially if the holding times of connections are small and traffic dynamicity, i.e., number of arrivals and departures in a unit of time, is high. Figure 4 (c) shows the reduction of BP vs. D for the two topologies. In USNET, even for D=0.2·H, SDT achieves a 50% saving in BP. Even for a delay tolerance value of 0.05, the algorithm SDT_dt achieves around 7% savings in BP for both topologies at an arrival rate of 150.

DYNAMIC PROVISIONING OF OPTICAL CIRCUITS WITH DIFFERENTIATED SURVIVABILITY REQUIREMENTS

WDM networks can be made survivable by means of path protection schemes implemented at the WDM layer (Mukherjee, 2006). A path protection scheme requires allocation of spare (or standby) resources that can be used in the event of a fault. For a lightpath, a path protection scheme consists of assigning a working and a protection path between the source and the destination. The working path carries the offered traffic during normal network operation. When the working

Figure 4. BP comparison of different scheduling schemes as a function of the load: EON network (a) and USNET (b). Effect of delay tolerance on the BP for both network topologies (c)



(a) Topology EON (b) Topology USNET (c) EON and USNET path is disrupted by a fault, the affected traffic is rerouted over the protection resources.

Even though the aim of a protection scheme is straightforward, the amount of spare capacity a lightpath should be allocated to guarantee the required level of resiliency is a question without a univocal answer. For example, should a lightpath always be protected against any single fault regardless of the reliability requirement for the specific service, or it can tolerate some downtime if possible? Conventional protection schemes are not able to answer this type of questions because they are meant to guarantee either a full protection in the presence of a network fault or no protection at all. These approaches are very simple and have proven to be a valid solution in many network scenarios. However, their simplicity comes with a cost in terms inefficiency in using the network resources. For example, with the Dedicated Path Protection (DPP) scheme (Mukherjee, 2006) the resources reserved for the protection are dedicated to a specific connection. In order to have a better resource efficiency multiple working paths may be allowed to share resources reserved for protection, i.e., the Shared Path Protection (SPP) scheme (Mukherjee, 2006). Nonetheless, both DPP and SSP lack the ability to adapt to the different protection requirements, and may not be adequate in those scenarios where over-reservation of redundant network resources is not acceptable.

This problem can be addressed by applying a concept called Differentiated Reliability (DiR). The DiR approach leverages on the intuition that different connections may require different protection levels, e.g., backup storage may sustain some brief interruptions while, for example, bank transactions cannot tolerate any disruption at all. The validity of such intuition is supported by the strong role concepts such as Quality of Service (QoS) and Differentiated Services have in today's communication networks. According to the DiR paradigm, each arriving connection request comes with a specific reliability requirement that must be met by the protection scheme and accordingly is assigned a certain protection level. This assumption makes it possible to reserve the minimum amount of network resources that are necessary to meet the level of protection required by a connection. In fact, the DiR approach focuses only on the protection level offered to each individual connection. There are several ways to express the level of protection. One option is to have the service protection level defined in terms of conditional failure probability, referred to as the probability that, once established, the connection survives a single fault in the network. Another option is to define an asymptotic connection availability, as specified for example by the Service Level Agreement (SLA).

The DiR concept was first introduced in the work by Fumagalli & Tacca (2006) where it was applied to provide different degrees of protection level in networks with a ring topology. The same concept was then extended to be used in more general mesh topologies under single (Fumagalli, *et al.*, 2002) and dual (Tacca, Fumagalli & Unghvary, 2003) link failure scenario. In all these studies the DiR approach was able to yield a significant reduction of the total number of network resources that are needed to accommodate a given set of lightpaths, i.e., a static provisioning scenario. In this subchapter the DiR problem is studied while considering a WDM network with dynamic traffic provisioning. The contribution is twofold. The first part of this subchapter focuses on describing how the SPP scheme can be combined with the DiR concept in a dynamic provisioning environment (resulting in the so called SPP-DiR scheme) when each connection protection level is described in terms of maximum conditional failure probability, assuming a single link failure scenario. The second part of the subchapter illustrates how to apply the SPP-DiR concept to account also for the impact of node failure on the connection survivability. In this part of the study, the level of protection of each lightpath is specified in terms of asymptotic connection availability. The failure scenario considered is also more general where multiple link/node failures are assumed.

The SPP-DiR Problem with Dynamic Provisioning

This section presents the SPP-DiR problem applied in dynamic provisioning scenario under the assumption of a single link failure. Consider a WDM network with an arbitrary mesh topology, where wavelength conversion is not available. It is assumed that only link failures are possible, and the probability that two or more links are down at the same time is considered to be negligible (Mukherjee, 2006). The WDM mesh network is modeled as a graph *G(N,L)*, where *N* represents the set of network nodes and *L* the set of network links. Each link (m,n)$\in$*L* is characterized by the value of its conditional failure probability, P_f(m,n). Based on the single failure assumption, the *conditional link failure probability* is the probability that a link is failed, given that a single link failure has occurred in the network. By assuming a single link failure scenario, the link failure probability is given by the product between the conditional link failure probability and the probability of having a single failure. For example, assuming a uniform distribution of faults among all the links, the *conditional link failure probability* can be expressed as:

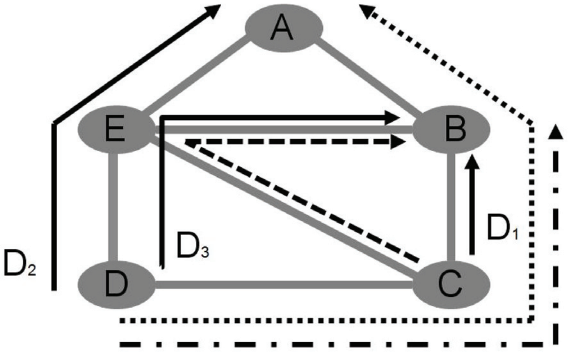
$$P_f(m,n) = \frac{1}{|L|}\ \forall(m,n) \in L. \tag{5}$$

In such a scenario, it is assumed that each arriving connection request is characterized by a *Maximum Conditional Failure Probability (MCFP)* value. MCFP represents the maximum acceptable probability that, given the occurrence of a network link failure, the service data flow will be permanently disrupted.

With this rationale in mind, it is possible to select a set of links of the working path for which an arriving connection request *d* will not need to resort to the protection path. This set must be selected to satisfy the required protection level, formally expressed by the connection's MCFP. Notice that with SPP-DiR two (or more) connections whose working paths have a common link may also share a link and a wavelength for their respective protection paths. This option is available when at least one of the two connections can afford to be permanently disrupted upon the failure of the link that is shared by the working paths. By the same reasoning, it is also possible to have a working path completely unprotected if the working path failure probability still satisfies the reliability requirement indicated by the connection's MCFP. These last options are not supported by the conventional SPP scheme where 100% protection against any single failure is offered, i.e., SPP supports MCFP = 0 only. The following example illustrates how the SPP-DiR scheme works in a dynamic provisioning scenario.

Assuming a uniform link failure distribution, the link conditional failure probability for the network in Figure 5 is P_f(m,n)=1/7, $\forall$(m,n)$\in$*L*. Three connection requests are shown. d_1 arrives first and requires MCFP_{d1} = 0. The chosen working path is *C-B*. The protection path is *C-E-B*. d_2 arrives next and requires MCFP_{d2} = 0. The chosen working path is *D-E-A*. The protection path is therefore *D-C-B-A*. Finally, d_3 arrives and requires MCFP_{d3} =1/7. According to its reliability requirement of d_3 can sustain the failure of one link along its path. Taking advantage of this possibility, the working path is routed along *D-E-B*. The protection path for d_3 is *D-C-B* and is used only in the case of a failure on link (*E,B)*, leaving link (*D,E)* unprotected, i.e., should link (*D,E)* fail d_2 will revert to its protection path since it cannot sustain any link failure. As shown in the example, protection resources along link (*C,B)* can be shared between connections d_2 and d_3 even though their working paths are not route

Figure 5. SPP-DiR problem, an example



disjoint. Notice that by requiring a higher protection level, i.e., $MCFP_{d3} < 1/7$, connection d_3 is then blocked due to the lack of available wavelengths in the network. Although manually constructed, this example serves the purpose of showing that the SPP-DiR scheme has the potential to yield better resource utilization when compared to the conventional SPP scheme, while still guaranteeing each connection request sufficient resources to satisfy its protection requirement.

SPP-DiR Problem Definition and Solution

Let $H_{w,d}$ be the set of wavelength links used by the working lightpath to accommodate connection request d and $H_{p,d}$ be the set of wavelength links used by the protection lightpath assigned to connection request d. To guarantee the availability of a protection lightpath when the working lightpath is affected by a failure, working and protection lightpaths must be route-disjoint:

$$H_{w,d} \cap H_{p,d} = \varnothing, \tag{6}$$

Let U_d be the set of unprotected links along the working lightpath of d, the conditional failure probability of d can be calculated as:

$$P_{f,d} = \sum_{(i,j)\in U_d} P_f(i,j) \le MCFP_d, \tag{7}$$

where $P_f(i,j)$ is the conditional link failure probability. Let $H_{s,d} \subseteq H_{p,d}$ be the set of links, used by the protection lightpath of d, that share resources with other protection lightpaths already routed in the network. Based on the routing for both working and protection lightpaths, a cost function measuring the goodness of the choice for the routing is defined as:

$$C_d = \left|H_{w,d}\right| + \left|H_{p,d}\right| + \left|H_{s,d}\right| + (MCFP_d - P_{f,d}). \tag{8}$$

The cost function measures the amount of resources provisioned to a connection. In addition it measures the excess of reliability ($MCFP_d$-$P_{f,d}$) that d receives. Solving the SPP-DiR problem means to provision each connection request with enough resources to satisfy equation (7), while minimizing the cost function defined in equation (8), which in turn has an impact on the overall blocking probability.

In order to solve the SPP-DIR problem presented above a two-step algorithm is used. The approach works as follows. In the first step, called SPP-DiR-FF, the algorithm aims at solving the Routing and Wavelength Assignment (RWA) problem for each connection request d while guaranteeing that the MCFP requirement is met by the protection scheme. The protection strategy is based on a modified version of the conventional Shared Path Protection (SPP) scheme where the DiR concept is applied with a larger granularity, i.e., connections can be fully protected or fully unprotected only. In the second step, called SPP-Dir-SA, the algorithm aims at reducing the reliability degree of the connection requests provisioned in the first step, with the intent of reducing the output of the cost function defined in equation (8). This is accomplished by selecting a subset of links along the working lightpath for which protection is not required. These links are chosen using a meta-heuristic algorithm based on Simulated Annealing (SA). For more information about the presented two-step strategy the interested reader is referred to Monti, Tacca & Fumagalli (2004).

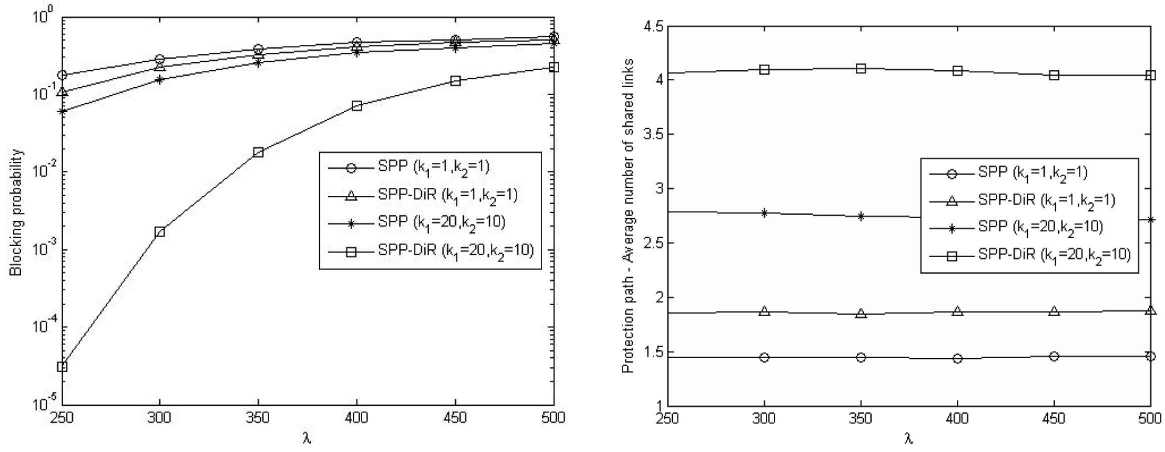
SPP-DiR Performance Study

This section presents a collection of results obtained while solving the SPP-DiR dynamic provisioning problem presented in the previous section. Since the number of candidate paths between a source and a destination grows exponentially with the network size, to reduce the search complexity the candidate paths for each connection request are generated using the disjoint path-pair matrix (DPM) approach (Monti, Tacca & Fumagalli, 2004). DPM uses the first k_1 shortest paths as candidates for the working path. For each working path candidate, the first k_2 shortest paths found when the links in the primary path are removed are used as candidates for backup paths. The European optical network (Batchelor *et al.*, 2000) with 19 nodes and 39 bidirectional links is used as reference. It is assumed to have one fiber for each direction of propagation, with 32 wavelengths per fiber. The conditional link failure probability is obtained assuming a uniform distribution of failures over all links i.e., $P_f(i,j) = 1/39\ \forall(i,j)\in L$. The connection requests arrive according to a Poisson process with arrival rate λ. Source and destination nodes of each connection are randomly chosen using a uniform distribution over all possible node pairs. Unless otherwise specified, each connection request is assigned a reliability degree requirement of MCFP = 0.03, i.e., in the network topology under consideration each connection may be able to have up to one working link that is unprotected. Once established, a connection remains in the system for a time that is exponentially distributed with parameter $1/\mu = 1$, i.e., the value of the arrival rate is equal to the value of the network load. The results shown in Figures 6 and 7 provide a performance comparison between the SPP-DiR and the conventional SPP schemes. As already mentioned, the SPP scheme can offer only 100% protection against any single failure.

Figure 6 (a) shows the value of the blocking probability as a function of the arrival rate λ. The plot shows that with a mild reduction of the offered reliability degree, i.e., MCFP = 0.03, the SPP-DiR scheme is able to decrease the blocking probability when compared to the SPP scheme. The reduction is more significant in the presence of multiple candidate paths, i.e., k_1=20, k_2=10, since the algorithm is able to find path options that better match the reliability requirement of each service. Figure 6 (b) plots the value of the average number of shared protection links versus λ. Results obtained for both the SPP-DiR and SPP schemes are shown. In the case under study, it is found that by closely matching the service's reliability requirement, the SPP-DiR scheme improves the number of shared protection links by 49% when compared to SPP.

Figure 7 (a) shows the normalized average excess of reliability as a function of the arrival rate. The excess of reliability of a connection, defined in equation (8) is averaged over all the provisioned connection requests, and normalized to MCFP=0.03. The excess of reliability obtained is always below 20%, a considerable reduction when considering that the SPP scheme has a value for the excess of reliability always equal to 100%. Figure 7 (b) shows the value of the blocking probability versus MCFP. The plots indicate the existing trade-off between the reliability degree that is guaranteed and the blocking probability. The values shown at MCFP = 0 represent the blocking probability of the SPP scheme. These results confirm that by attempting to closely match the connection's reliability requirement, the SPP-DiR scheme is successful in reducing the average

Figure 6. Performance evaluation: blocking probability (a) and average number of shared links (b) as a function of the arrival rate



(a)

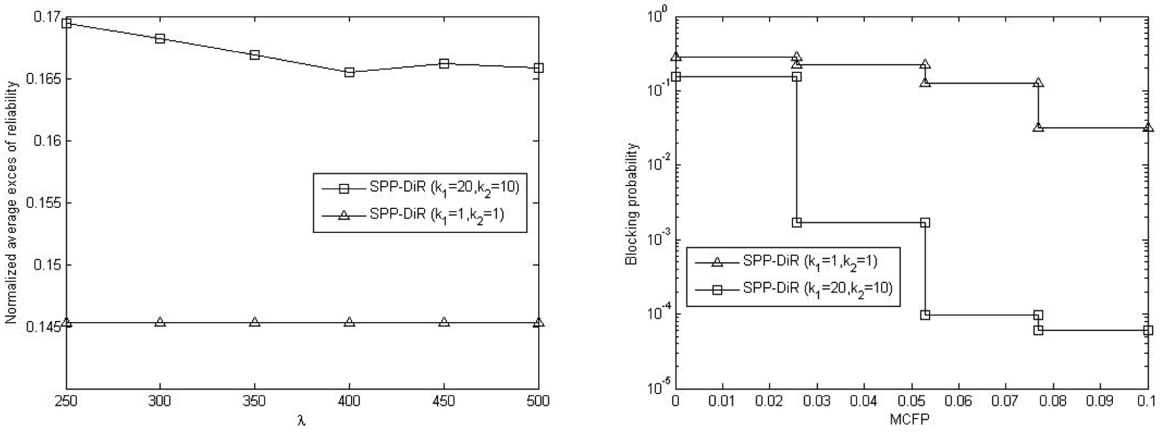
(b)

amount of network resources that must be reserved to establish a newly arrived connection. In turn, this fact may significantly reduce the value of the blocking probability.

Impact of Optical Node Failures on Network Reliability Performance

This section extends the previously presented study where only link failures were considered. Network survivability scenario with only link

Figure 7. Performance evaluation: excess of reliability as a function of the arrival rate (a) and blocking probability as a function of the maximum conditional failure probability (b)



(a)

(b)

failure assumption is in line with what can be found in the literature where most of the contributions, e.g. (Ramamurthy, *et al.*, 2003; Doucette, Coloqueur & Grover, 2003; Ou, *et al.*, 2004; Schupke, Gruber & Autenrieth, 2002), consider only fiber link failures while the probability of optical node failures is assumed to be negligible. This approach can be valid in a number of cases, but probably not in all the possible scenarios. Therefore, a comprehensive analysis should also take into account the reliability performance of the optical nodes in the network.

In the study presented in this section we consider an optical circuit switched network (also referred to as wavelength routed network) where a circuit corresponds to a wavelength channel (*lightpath*) and optical cross-connects (OXCs) are the switching nodes. This study analyses the impact of an optical node failure on the end-to-end lightpath provisioning in survivable WDM networks by combining both the node level and the network wide reliability calculations in a single reliability provisioning framework. The node level reliability calculations based on the models in Wosinska (1993) are embedded in a network level protection scheme, i.e., the SPP-DiR approach, making it possible to study the effect of node reliability performance on end-to-end service provisioning.

Node Reliability

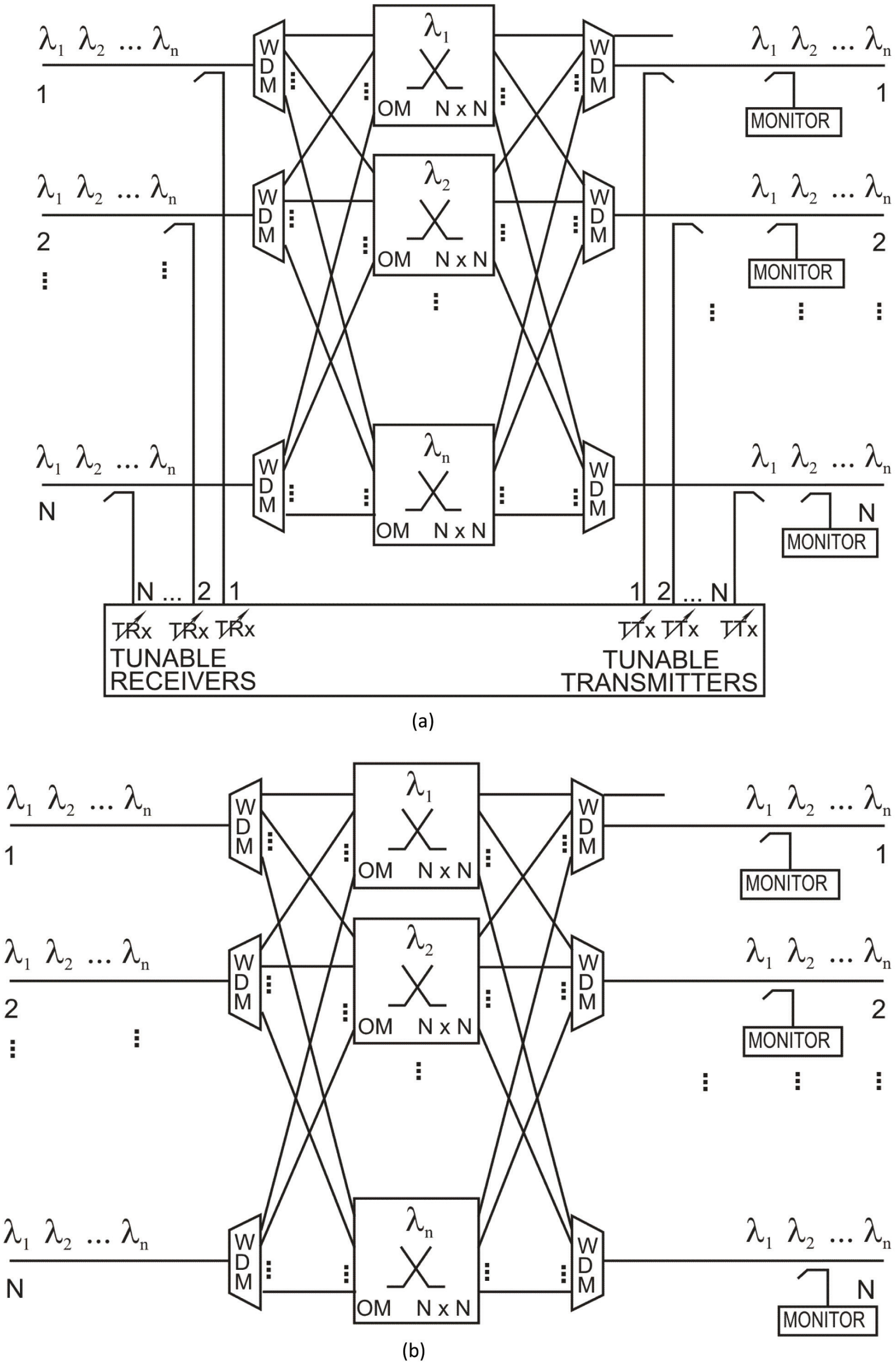
To calculate the availability of the optical nodes in the network we adopt the models presented in Wosinska (1993) where the number of wavelengths on each fiber is equal to 4, 32 and 64. The optical MEMS technology has been selected for this study due to the relatively low energy consumption, high reliability performance and low cost compared to an OXC based on tunable wavelength converters (TWC) and a passive wavelength selective device, i.e. arrayed waveguide grating (AWG). Moreover, we consider two OXC architectures, namely with and without inherent protection (Figure 8).

Table 2 shows the unavailability values for OXCs in Figure 8 with different number of wavelengths per fiber, which are later used in the network level protection scheme. Asymptotic unavailability (U) is a reliability performance measure denoting the probability that a component or system is down at an arbitrary instance of time. Calculations are based on the component availability values published in Wosinska, Thylen & Holmstrom (2001). Devices used at nodes for link termination, i.e., splitters, transmitters, receivers, couplers, and multiplexers, are treated as components connected to links in series configuration. That is, when determining the availability measure of links the failure rate of these optical components is also considered in addition to the failure rate of fiber links. Table 2 displays also the asymptotic unavailability of link terminations at nodes, derived using the same technique as in the case of the node level availability results. The difference of the unavailability figures of link terminations at nodes between protected and unprotected node architectures comes from the optical power splitter used at the input fibers in the protected architecture.

Network Level Reliability

We assume a dynamic network scenario where incoming connection (lightpath) requests arrive with specified reliability requirements. The network topology, the link capacities and the switching equipment deployed at nodes are given as input parameters. Incoming connection requests arrive with specified availability requirements and a centralized decision mechanism, similar to the one described in the first part of the subchapter, is utilized for lightpath setup. Lightpaths are provisioned only when there are enough free resources in the network to meet their reliability requirements. In order to obtain efficient resource utilization in the network the shared path protection scheme (SPP) is combined with differentiated reliability (DiR). This combination is referred to

Figure 8. Considered OXC architectures: with protection (a), and without protection (b)



(a)

(b)

as SPP-DiR (Monti, Tacca & Fumagalli, 2004). The results of SPP-DiR are compared with the ones obtained with dedicated path protection scheme (DPP). In order to provide suboptimal solutions in polynomial time, a heuristic technique is utilized, which makes use of a time-efficient

Table 2. Node and link termination reliability performance

Number of wavelengths per fiber	Node unavailability (10^{-6})		Unavailability of link terminations (10^{-6})	
	OXC without protection	OXC with protection	OXC without protection	OXC with protection
4	24.0	0.00036	0.6	0.9
32	192.0	0.018	2.4	2.7
64	384.0	0.072	4.8	5.1

method to estimate the end-to-end connection availability in the presence of multiple link and node failures. Using the heuristic presented, the influence of the node equipment on the overall network performance is assessed.

Results presented in Pandi, *et al.* (2006) confirm the intuition that the significance of node failures is relatively high in networks with short fiber links since the asymptotic unavailability of nodes may be comparable or higher than the unavailability of the fiber links. Thus, the higher the node unavailability the higher the impact on the connection availability in networks with longer fiber links. This is reflected in Figure 9 where U_{min} denotes the minimum connection unavailability that can be guaranteed in the network of different size and based on nodes with and without inherent protection, which corresponds to higher and lower value of node availability, respectively.

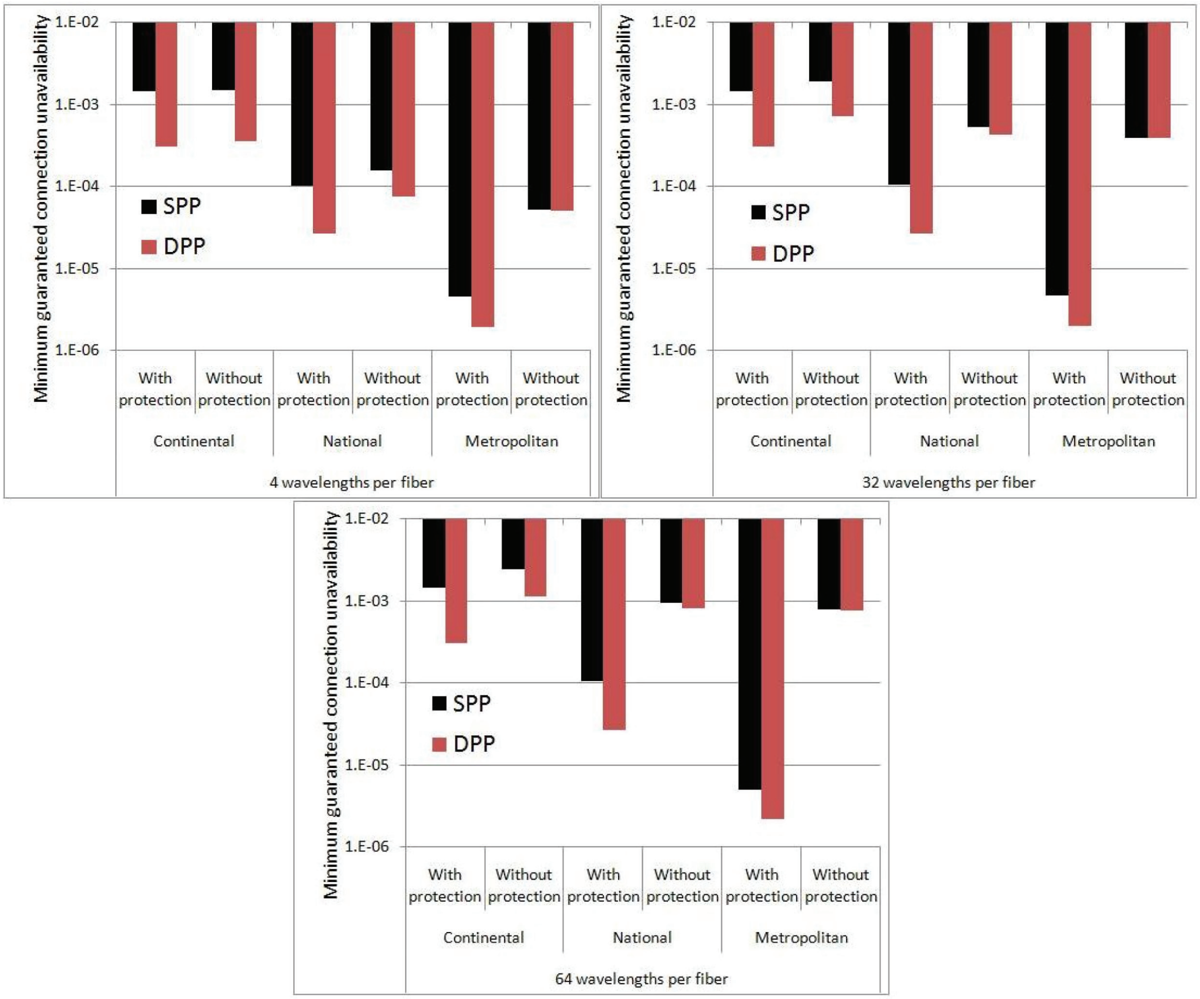
SURVIVABLE FIBER ACCESS NETWORK

Due to the increased dependency on electronic services all over society and due to the growing importance of reliable service delivery, an efficient fault management strategy has to be considered in both the access and the core segment of an optical network to ensure an uninterrupted end-to-end service provisioning. However, in contrast to the core segment, access networks are very cost sensitive due to low sharing factor of the network infrastructure.

Among several existing fiber access network architectures, passive optical networks (PONs) are considered as an important candidate to offer high capacity at relatively low cost. Three types of PON solutions, each one utilizing different resource sharing technologies can be identified: time-division multiplexing (TDM) PON, wavelength-division multiplexing (WDM) PON and hybrid WDM/TDM PON. The evolution of PON is progressing towards not only higher bandwidth but also towards a larger coverage of the access areas and an increased number of users. This is driven by the fact that extending the PON reach from a few kilometers to hundred kilometers enables the replacement of multiple central offices (COs) with a single one, with significant saving in capital and operational expenditure. On the other hand, it has already been shown that an unprotected PON with a reach up to twenty kilometers is characterized by a very poor reliability performance (Wosinska, Chen & Larsen, 2009; Chen, *et al.*, 2010). Such poor performance will be even worse in the case of long-reach (i.e. up to 100 km expected in the future) PONs. Therefore, providing protection in future PON installations becomes essential for a reliable service delivery.

On the other hand, the deployment of fiber access networks require a considerable investment from operators, while, as mentioned before, in this network segment cost is a very important factor. Therefore, operators may choose to provide at first mostly unprotected services. Up to now, only business users are including in their Service Level Agreement (SLA) some penalties

Figure 9. Minimum connection unavailability as function of the network size and as a function of different switch architectures



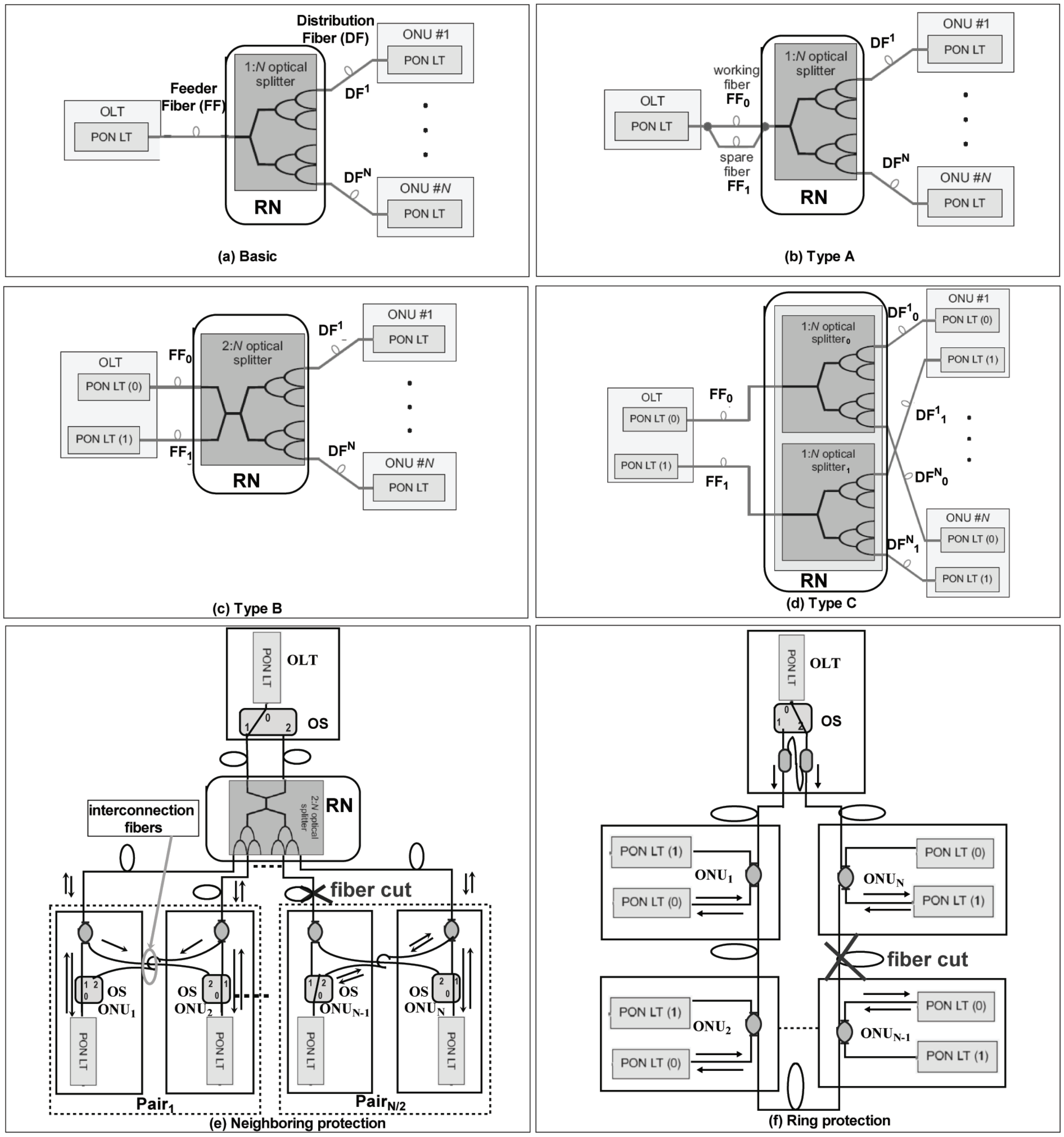
to be paid for those service interruptions that exceed an agreed time threshold. However, new services (e.g. telehealth) may in the future extend this requirement to the private users. In such a case, operators will be facing the need to upgrade their access networks with protection resources to improve reliability performance in order to avoid penalties for service interruptions.

This subchapter focuses on survivable PON architectures aiming at comparing the cost and reliability performance of some representative approaches. First, different PON protection schemes are reviewed, including both solutions proposed in the standards and in the literature. Then the cost and reliability performance are evaluated for all the presented reliable PON architectures.

Protection Schemes in PON

Tree is the most commonly used topology in fiber access networks. Among the various options, trees with a single splitting point (Figure 10 (a)) are the most commonly used configuration in PONs. In such configuration one single fiber, called feeder fiber (FF), connects an optical line terminal (OLT) at the CO to a remote node (RN), which is an intermediate node where the optical signal is split to reach each and every optical network unit (ONU) deployed in the PON. An ONU represents a termination point at the user side, and each ONU is connected to the RN through a separate fiber, called distribution fiber (DF). The drawback in having a tree structure is that it requires additional fiber deployment to provide protection paths between the OLT and the ONUs to be used in case of a fiber cut.

Figure 10. TDM PON architectures: (a) basic, (b) Type A, (c) Type B, (d) Type C, (e) neighboring protection (Chen, Chen & He, 2006), and (f) ring protection (Yeh & Chi, 2007)



(a) Basic

(b) Type A

(c) Type B

(d) Type C

(e) Neighboring protection

(f) Ring protection

In order to provide a more reliable service delivery over the PON infrastructure several protection architectures have been proposed. In the late 90s, some standard protection architectures were defined by ITU-T (ITU-T, 1997). The ITU-T standard proposes a simple and straightforward concept, i.e., provision of duplicated components for the parts that need to be protected. Figures 10 (b), (c) and (d) show three standard protection architectures defined by ITU-T. They are based on the duplication of network resources and are referred to as type A, B, and C. In Type A (Figure 10 (b)) only the FF is duplicated. Type B protection (Figure 10 (c)) duplicates the shared part of the PON (i.e., both FF and the line terminals at the OLT). Type C protection (Figure 10 (d)) represents 1+1 dedicated path protection with full duplication of the PON resources. In addition to the protection schemes just explained, ITU-T also defined a scheme referred to as Type D protection where the FF and the DFs can be duplicated independently. This additional protection scheme enables network operators to offer different reliability levels to different users. Type D protection provides end users with either full or partial protection referred to as Type D1 or D2 respectively.

Type C and Type D1 protection schemes are able to offer a relatively high reliability performance but they require duplication of all network resources to realize their protection function. This may result in deployment costs that are too high. Therefore, a lot of research work has been done to develop cost-efficient and reliable access network architectures. The work presented in Chan, *et al.* (2003), Chen, Chen & He (2006), Chen & Wosinska (2007), and Chen, Wosinska & He (2008), proposed neighboring protection (NP) schemes where two adjacent ONUs protect each other using interconnection fibers (see Figure 10 (e)). In this way, the cost invested in burying redundant disjoint DFs to each ONU can be saved and, consequently, the deployment cost can be significantly reduced. Figure 10 (e) shows a neighboring protection architecture for TDM PON proposed in Chen, Chen & He (2006) where two geographically disjoint fibers provide dedicated protection against a FF cut between OLT and RN, and adjacent ONUs are paired to realize dedicated protection for DFs. Figure 10 (e) provides also an example on what would happen with the presented protection scheme should a fiber failure occur between ONU$_{N-1}$ and the RN, where N denotes the total number of ONUs. ONU$_{N-1}$ detects the loss-of-light and a control signal is generated to trigger the optical switch (OS) from port 1 (the normal state) to port 2 (the protection state). The corresponding interconnection fiber, which connects port 2 of the OS in ONUN-1, works for both the upstream and downstream traffic flows associated with ONU$_{N-1}$. This NP scheme can also be used with WDM PON (Chan, *et al.*, 2003) and with hybrid WDM/TDM PON (Chen & Wosinska, 2007; Chen, Wosinska & He, 2008).

On the other hand, ring topologies are able to offer resiliency with a minimum number of links. Therefore a protection scheme based on rings can also offer a cost-effective solution for PON by reducing the fiber deployment cost. A ring protection for TDM PON proposed in Yeh & Chi (2007) is shown in Figure 10 (f). During normal operation, the downstream signal from the OLT is transmitted counterclockwise to the line terminal LT(0) at each ONU, while the upstream signal from line terminals LT(0) at each ONU is transmitted clockwise. Figure 10 (f) provides an example on what would happen when a fiber cut occurs between ONU$_{N-1}$ and ONU$_N$, where N denotes the total number of ONUs in the TDM PON. In the presence of a fiber cut, the ONUs where LT (0) loses its connection to the OLT will start using LT (1) to reconnect the OLT. In the meantime, the OLT will also switch the direction of its optical switch to the port number 2. In this way, the downstream signal will be separated to pass counterclockwise and clockwise simultaneously. For the upstream signal, LT (0) at each ONU not affected by the fiber cut maintains its clockwise transmission while LT (1) at the ONUs in protection mode sends the signal counterclockwise.

Reliability Performance

This section studies the availability of a connection between the OLT and each ONU using the method presented in Wosinska, Chen & Larsen (2009). The analysis is done for the resilient PON architectures presented in the previous section where different values of the total length of the FF plus the DF (referred to as *reach*) are assumed. Two values of the reach are considered, namely 20 km and 100 km. The other input data (e.g., failure rate, mean time to repair) used for the presented availability calculations is obtained from Chen, *et al.* (2010). The results for connection unavailability and their relative deployment cost per user are shown in Table 3. The cost is computed as a function of the equipment cost value, the cost for the fiber infrastructure and installation cost (Chen, *et al.*, 2010) and it normalized to the cost of the non protected (i.e., Basic) TDM PON case.

In future, it is expected that network operators will need to offer 5 nines connection availability (i.e. connection availability greater than 99.999%), which corresponds to a connection downtime of less than 6 minutes per year. From Table 3, it can be seen that basic TDM PON without any protections shows reliability performance lower than 99.999% for both 20 km and 100 km reach. Therefore, it is necessary to provide protection in PONs in order to improve their reliability performance. On the other hand, Type C and D1 schemes with neighboring protection and ring protection can offer very high connection availability (higher than 99.999%) for both 20 km and 100 km reach. However, the comparison of deployment cost per user shows that neighboring and ring protection schemes are much more cost-efficient than Type C and D1. In addition, it can be seen that ring protection has the lowest deployment cost per user while maintaining an acceptable reliability performance. On the other hand, ring protection has a problem with the power budget. When the optical signal passes through several ONUs, it becomes degraded and attenuated. It restricts the total number of ONUs that can be connected to the ring. Therefore, compared with cost efficient NP scheme, ring protection cannot be applied to PONs deployed in dense populated areas. Furthermore, it can be observed that the

Table 3. Reliability performance results

Network Architectures		Unavailability		Relative deployment cost per user (%)	
		Reach=20km	Reach=100km	Reach=20km	Reach=100km
Basic	TDM PON	2.76E-04	1.37E-03	100%	100%
Standard protection (TDM) (ITU-T, 1997)	Type A	7.20E-05	7.36E-05	101%	106%
	Type B	7.03E-05	7.19E-05	103%	108%
	Type C	7.64E-08	1.88E-06	200%	200%
	Type D1	4.72E-08	1.70E-06	200%	200%
	Type D2	6.92E-05	7.08E-05	104%	111%
Neighboring protection (NP)	TDM	5.22E-06	6.86E-06	121%	127%
	WDM	7.50E-06	9.14E-06	126%	132%
	Hybrid I	6.42E-06	8.06E-06	121%	123%
	Hybrid II	4.80E-06	6.44E-06	121%	123%
Ring protection	TDM	2.41E-06	4.305E-06	65%	87%

reliability performance for a PON with NP scheme does not suffer as much from reach extension, while connection unavailability for basic PON, Type C and D1 increases significantly (5 to 25 times more).

CONCLUSION

This chapter presented a series of resiliency strategies that can be used in network scenarios where operators and service providers have to accommodate services with different resilience requirements. The common denominator of these strategies is their ability to leverage the different requirement levels imposed by each service to make a more efficient use of the network resources and to reduce the network deployment costs.

The first part of the chapter demonstrated a new dimension for the shared-path protection (SPP) scheme called Shared Path Protection with Delay Tolerance (SDT). Exploiting the flexibility provided by this QoS specification, SDT is able to significantly decrease blocking probability without sacrificing spare capacity utilization. The focus of the presented study was on different scheduling strategies for SPP that can be used in a dynamic provisioning scenario. It was shown that significant reduction of blocking probability is achievable in typical backbone network topologies independently of the load condition. Delaying connection requests even for a short duration brings approximately 50% reduction of blocking probability.

In the second part of the chapter an on-line Shared Path Protection scheme with differentiated Reliability (SPP-DiR) was described. SPP-DiR dynamically reserves network resources to set up incoming connection requests, with the objective of guarantee the required availability with the minimum possible redundancy. Two cases were analyzed. In the first case only single link failures were considered. In the second case the impact of nodes faults was also taken into account in a scenario where multiple simultaneous network failures are possible. It was shown that when compared to the conventional SPP scheme, the presented SPP-DiR algorithm reduces the overall blocking probability by making use of the spare protection wavelengths, while guaranteeing the required availability of each connection. The presented results also confirm that the widely used assumption of negligible node failures may not be acceptable in networks with relatively large number of nodes and short fiber links where the asymptotic unavailability of nodes may be comparable or higher than the unavailability of the fiber links.

In the last part, the chapter provided an overview of recent advances in protection schemes for different types of PONs along with an assessment of some representative approaches in terms of reliability and deployment cost.

FUTURE TRENDS

This section briefly explores how the protection concepts presented in this chapter can be extended to account for other critical aspects of optical networks.

One interesting issue that can be investigated is the possibility of exploiting sub wavelength granularities. All the results presented in this chapter for the backbone segment assume that each lightpath uses the bandwidth of a full wavelength. It would be interesting to explore how the proposed mechanisms (i.e., both SPP-SDT and SPP-DiR) perform when they have to protect sub wavelength channels. Another interesting aspect to consider is how the presence of optical physical impairments will influence the differentiated QoS protection mechanisms presented in the chapter. Degradation of optical signal due to the physical layer phenomena limits the maximum span of a lightpath and influence the choices made during the routing phase. Their effect, in terms of reduced lightpath reach, is expected to be even more critical in the provisioning phase of protection lightpaths that are, on average, longer then their respective primary lightpaths.

In one of the sections this chapter highlighted a trade-off between the deployment cost (CAPEX) and the level of reliability performance in fiber access networks. Since economical aspects are most critical in the access part of the networks, the future trend will migrate towards minimizing the operational expenditures (OPEX) during the access network operation time in order to minimize the total cost of ownership (TCO) for the operator. In this respect, the work presented in this chapter can be extended to include consideration of failure related OPEX, such as service interruption penalty and reparation cost.

REFERENCES

ATT. (2009). *AT&T high speed internet business edition service level agreements*. Retrieved May 2009, from http://www.att.com/gen/general?pid=6622

Batchelor, P., Daino, B., Heinzmann, P., Hjelme, D. R., Inkret, R., & Jäger, H. A. (2000). Study on the implementation of optical transparent transport networks in the European environment-Results of the research project COST 239. *Photonic Network Communications*, *2*(1), 15–32. doi:10.1023/A:1010050906938

Cavdar, C., Song, L., Tornatore, M., & Mukherjee, B. (2007). *Holding-time-aware and availability-guaranteed connection provisioning in optical WDM mesh networks. High-Capacity Optical Networks and Enabling Technologies (HONET), Dubai*. UAE.

Cavdar, C., Tornatore, M., & Buzluca, F. (2009). *Availability-guaranteed connection provisioning with delay tolerance in optical WDM mesh networks*. Optical Fiber Communication Conference and Exposition, San Diego, CA, USA.

Cavdar, C., Tornatore, M., Buzluca, F., & Mukherjee, B. (2010). Shared-path protection with delay tolerance (SDT) in optical WDM mesh networks. *IEEE/OSA. Journal of Lightwave Technology*, *28*(14), 2068–2076. doi:10.1109/JLT.2010.2051414

Chan, T., Chan, C., Chen, L., & Tong, F. (2003). A Self-protected architecture for wavelength division multiplexed passive optical networks. *IEEE Photonics Technology Letters*, *15*(11), 1660–1662. doi:10.1109/LPT.2003.818657

Chen, J., Chen, B., & He, S. (2006). Self-protection scheme against failures of distributed fiber links in an ethernet passive optical network. *OSA Journal of Optical Networks*, *5*(9), 662–666. doi:10.1364/JON.5.000662

Chen, J., Mas Machuca, C., Wosinska, L., & Jaeger, M. (2010). Cost vs. reliability performance study of fiber access network architectures. *IEEE Communications Magazine*, *48*(2), 56–65. doi:10.1109/MCOM.2010.5402664

Chen, J., & Wosinska, L. (2007). Analysis of protection schemes in PON compatible with smooth migration from TDM-PON to hybrid WDM/TDM PON. *OSA Journal of Optical Networks*, *6*(5), 514–526. doi:10.1364/JON.6.000514

Chen, J., Wosinska, L., & He, S. (2008). High utilization of wavelengths and simple interconnection between users in a protection scheme for passive optical networks. *IEEE Photonics Technology Letters*, *20*(6), 389–391. doi:10.1109/LPT.2007.915655

Cholda, P., Mykkeltveit, A., Helvik, B. E., Wittner, O., & Jajszczyk, A. (2007). A survey of resilience differentiation frameworks in communication networks. *IEEE Communications Surveys and Tutorials*, *9*(1-4), 32–55. doi:10.1109/COMST.2007.4444749

Clemente, R., Bartoli, M., Bossi, M. C., D'Orazio, G., & Cosmo, G. (2005). *Risk management in availability SLA*. Italy: Design of Reliable Communication Networks, Island of Ischia.

Doucette, J., Coloqueur, M., & Grover, W. D. (2003). On the availability and capacity requirements of shared backup path-protected mesh networks. *SPIE Optical Networking Magazine*, *4*(6), 29–44.

Fumagalli, A., & Tacca, M. (2006). Differentiated reliability (DiR) in wavelength division multiplexing rings. *IEEE/ACM Transactions on Networking*, *14*(1), 159–168. doi:10.1109/TNET.2005.863708

Fumagalli, A., Tacca, M., Unghvary, F., & Farago, A. (2002). *Shared path protection with differentiated reliability.* International Conference on Communications, New York, NY, USA.

ITU-T. (1998). *Recommendation G983.1.*

Jaekel, A., & Chen, Y. (2007). Demand allocation without wavelength conversion under a sliding scheduled traffic model. *International Conference on Broadband Communications, Networks, and Systems (Broadnets)*, Raleigh, NC, USA.

Li, T., & Wang, B. (2006). *Approximating optimal survivable scheduled service provisioning in WDM optical networks with iterative survivable routing*. International Conference on Broadband Communications, Networks, and Systems (Broadnets), San Jose, CA, USA.

Liu, S., & Chen, L. (2007). *Deployment of carrier-grade bandwidth-on-demand services over optical transport networks: A Verizon experience.* Optical Fiber Communication Conference and Exposition, San Diego, CA, USA.

Monti, P., Tacca, M., & Fumagalli, A. (2004). Resource-efficient path-protection schemes and online selection of routes in reliable WDM Networks. *OSA Journal of Optical Networking, special issue on Next-Generation WDM Network Design and Routing, 3*(4), 188-203.

Mukherjee, B. (2006). *Optical WDM networks*. New York, NY: Springer.

Ou, C., Zhang, J., Sahasrabuddhe, L. H., & Mukherjee, B. (2004). New and improved approaches for shared-path protection in WDM mesh networks. *IEEE/OSA*. *Journal of Lightwave Technology*, *22*(5), 1223–1232. doi:10.1109/JLT.2004.825346

Pandi, Z., Tacca, M., Fumagalli, A., & Wosinska, L. (2006). Dynamic provisioning of availability-constrained optical circuits in the presence of optical node failures. *IEEE/OSA*. *Journal of Lightwave Technology*, *24*(9), 3268–3279. doi:10.1109/JLT.2006.879505

Ramamurthy, S., Sahasrabuddhe, L., & Mukherjee, B. (2003). Survivable WDM mesh networks. *IEEE/OSA*. *Journal of Lightwave Technology*, *21*(4), 870–883. doi:10.1109/JLT.2002.806338

Ray, M. (2010). *100G DWDM optical networking transport: The telecom industry prepares*. Retrieved December 2010, from http://searchtelecom.techtarget.com/feature/100G-DWDM-optical-networking-transport-The-telecom-industry-prepares

Schupke, D. A., Gruber, C. G., & Autenrieth, A. (2002). *Optimal configuration of p-cycles in WDM networks*. International Conference on Communications, New York, NY, USA.

Tacca, M., Fumagalli, A., & Unghvary, F. (2003). *Double-fault shared path protection scheme with constrained connection downtime*. Banff, Alberta, Canada: Design of Reliable Communication Networks.

Tanwir, S., Battestilli, L., Perros, H., & Karmous-Edwards, G. (2007). Dynamic scheduling of network resources with advance reservations in optical grids. *International Journal of Network Management*, *18*(2), 79–105. doi:10.1002/nem.680

Tornatore, M., Ou, C. S., Zhang, J., Pattavina, A., & Mukherjee, B. (2005). PHOTO: An efficient shared-path protection strategy based on connection-holding-time awareness. *IEEE/OSA. Journal of Lightwave Technology*, *23*(10), 3138–3146. doi:10.1109/JLT.2005.856174

Tran, A. V., Chae, C., & Tucker, R. S. (2005). Ethernet PON or WDM PON: A comparison of cost and reliability. *TENCON*, IEEE Region 10.

Wosinska, L. (1993). Reliability study of fault-tolerant multiwavelength nonblocking optical cross connect based on InGaAsP/InP laser-amplifier gateswitch arrays. *IEEE Photonics Technology Letters*, *5*(10), 1206–1209. doi:10.1109/68.248429

Wosinska, L., & Chen, J. (2008). Reliability performance analysis vs. deployment cost of fiber access networks. 7th International Conference on Optical Internet, Tokyo, Japan.

Wosinska, L., Chen, J., & Larsen, P. C. (2009). Fiber access networks: Reliability analysis and Swedish broadband market. *IEICE Transactions on Communications*. *E (Norwalk, Conn.)*, *92-B*(10), 3006–3014.

Wosinska, L., Thylen, L., & Holmstrom, R. P. (2001). Large-capacity strictly nonblocking optical cross-connects based on microelectrooptomechanical systems (MEOMS) switch matrices: Reliability performance analysis. *IEEE/OSA. Journal of Lightwave Technology*, *19*(8), 1065–1075. doi:10.1109/50.939785

Yeh, C., & Chi, S. (2007). Self-healing ring-based time-sharing passive optical networks. *IEEE Photonics Technology Letters*, *19*(15), 1139–1141. doi:10.1109/LPT.2007.900155

ADDITIONAL READING

Chen, J., & Wosinska, L. (2010). *Efficient next-generation optical networks - design and analysis of fiber access and core networks*. VDM Verlag, Dr Muller Aktiengesellschaft & Co. KG.

Tacca, M., Fumagalli, A., Paradisi, A., Unghvary, F., Gadhiraju, K., & Lakshmanan, S. (2003). Differentiated reliability in optical networks: theoretical and practical results. *IEEE/OSA. Journal of Lightwave Technology*, *21*(11), 2576–2586. doi:10.1109/JLT.2003.819554

Tacca, M., Monti, P., & Fumagalli, A. (2004). The disjoint path-pair matrix approach for online routing in reliable WDM networks. *International Conference on Communications,* Paris, France, 2004.

Wosinska, L. (1999). *A study of the reliability of optical switching nodes for high capacity telecommunications networks* (TRITA-MVT Report 1999:4). Ph.D. dissertation, Royal Institute of Technology, Stockholm, Sweden, 1999.

KEY TERMS AND DEFINITIONS

Availability: The probability of a network resource to be in an operating state at a random time t in the future.

Delay Tolerance: The maximum time that a customer can wait after issuing the connection request to have the connection set-up.

Holding Time: The time duration between the set-up time and the teardown time of a connection.

Service Level Agreement: A contract signed between bandwidth provider and customer, which defines different level of service specifications to be met during the connection's life-time or set-up.

Set-up Time: The time it takes to establish a connection since the connection request is issued.