İSTANBUL TECHNICAL UNIVERSITY ★ INSTITUTE OF SCIENCE AND TECHNOLOGY

AVAILABILITY-CONSTRAINED ROUTING AND WAVELENGTH ASSIGNMENT AND SURVIVABILITY IN OPTICAL WDM NETWORKS

Ph.D. Thesis by
Burak KANTARCI

Department : **Computer Engineering**

Programme : **Computer Engineering**

MAY 2009

İSTANBUL TECHNICAL UNIVERSITY ★ INSTITUTE OF SCIENCE AND TECHNOLOGY

AVAILABILITY-CONSTRAINED ROUTING AND WAVELENGTH ASSIGNMENT AND SURVIVABILITY IN OPTICAL WDM NETWORKS

Ph.D. Thesis by
Burak KANTARCI
(504042509)

Date of submission :	**26 February 2009**
Date of defence examination:	**07 May 2009**

Supervisors (Chariman) :	**Prof. Dr. Sema OKTUĞ (ITU)** **Prof. Dr. Hussein MOUFTAH (University of Ottawa)**
Members of the Examining Committee :	**Prof. Dr. Emre HARMANCI (ITU)** **Assoc. Prof. Dr. Fatih ALAGÖZ (BU)** **Assoc Prof. Dr. Ezhan KARAŞAN (Bilkent University)** **Assist. Prof. Dr. Ayşegül YAYIMLI (ITU)** **Assist. Prof. Dr. Feza BUZLUCA (ITU)**

MAY 2009

İSTANBUL TEKNİK ÜNİVERSİTESİ ★ FEN BİLİMLERİ ENSTİTÜSÜ

OPTİK WDM AĞLARINDA KULLANILABİLİRLİK KISITI ALTINDA YOL VE DALGABOYU ATAMA VE SÜRDÜRÜLEBİLİRLİK

DOKTORA TEZİ
Burak KANTARCI
(504042509)

Tezin Enstitüye Verildiği Tarih : 26 Şubat 2009
Tezin Savunulduğu Tarih : 07 Mayıs 2009

Tez Danışmanları : Prof. Dr. Sema OKTUĞ (İTÜ)
Prof. Dr. Hussein MOUFTAH (Ottawa Üniversitesi)
Diğer Jüri Üyeleri : Prof. Dr. Emre HARMANCI (İTÜ)
Doç. Dr. Fatih ALAGÖz (BÜ)
Doç. Dr. Ezhan KARAŞAN (Bilkent Üniversitesi)
Yrd.Doç.Dr. Ayşegül YAYIMLI (İTÜ)
Yrd.Doç.Dr. Feza BUZLUCA (İTÜ)

MAYIS 2009

FOREWORD

First of all I would like to thank to Prof. Sema Oktuğ who has supervised my research by supporting every phase of my academic study, and showed me the pleasant view of the scientific research since 2002. It is a great pleasure and a big chance for me to work with her for such a long time with outstanding outcomes. I appreciate for the effort that she put on this study, her valuable comments and considerations to improve the quality of the work. I wish to go on working together with other projects.

I would like to thank to Prof. Hussein T. Mouftah, who accepted to be the co-supervisor of this thesis study, and accepted me to his research laboratory at University of Ottawa. I appreciate for his motivating support, time, and effort on this thesis. He always provided valuable comments and outstanding directions for the efficiency and the quality of the work. I am honored to be one of his students.

The research period at University of Ottawa, was financially supported by Scientific and Technological Research Council of Turkey (TUBITAK) under scholarship number 2214 between September 2007 and September 2008. Thanks for funding the research go to TUBITAK.

I would like to thank to the progress committee members Dr. Ayşegül Yayımlı and Dr.Fatih Alagöz for their valuable feedbacks and comments in the periodical meetings.

In July 2004, I met a very special person who has shared many cheerful times with me. As time went by, we have also noticed our ability to communicate even without speaking. We lived in different continents for two years. Finally, we found ourselves standing by each other where I thought that I am the happiest one in the world. Hence, I would like to thank to my dear future wife Melike Erol-Kantarcı for constructing the most colorful and valuable part of my life. I should also thank to her for putting her tireless effort on proofreading of this thesis book and managing all the details on my defence day. We know that these words are just the beginning of a wonderful future which is waiting to be built by us.

I would like to thank to my dear friend and colleague Dr. Mazen G. Khair. During my stay in Canada, I never thought of being alone and a foreigner by his kind friendship and help. I enjoyed a lot while working, producing, collaborating, sharing many good times, and traveling around the world together.

I also thank to all my colleagues in Networks Research Laboratory and Department of Computer Engineering at Istanbul Technical University for their corporation.

Technical discussions during research in the lab, meetings, and seminars at UOttawa also provided new directions for me so I would like to thank to all my colleagues and friends who are worked under supervision of Prof. Mouftah when I was there.

During the research period at UOttawa, Berk Canberk dealt with most of the bureaucratic issues related to me in Turkey, and had hard times because of me. Therefore Berk deserves many thanks for his great favor. I would also like to thank to Tolga Ovatman for providing me distant technical support many times. On-line technical discussions with Cicek Cavdar between UOttawa and UCDavis also helped me to improve my considerations on the work. I also thank to my officemate Çağatay Talay who has witnessed my stressed times due to the research since my M.Sc thesis.

I would like to thank to Prof. Emre Harmancı for his tireless effort to get into the deep details of this study which also enabled me to verify the integrity of this thesis.

Last period of this work has been the busiest time of all I spent in the department. Therefore, many special thanks go to my dear colleagues Melike Erol, Kenan Kule, and Yusuf Yaslan who did not hesitate providing me any kind of help, support, tolerance, and solidarity during the last semester of this work.

Onur Tuncaboylu, who has been a brother to me since the age of ten deserves very special thanks for his companionship, support, and self-sacrificing help. We have a lot in common related to our lives. I wish to celebrate every happy event related to us together also in the future in the name of our entrenched companionship.

Last but hugely special thanks are for my mother, Mine Kantarcı, my father, Ergünsel Kantarcı and my dear sister, Burcu Kantarcı who have continuously supported, encouraged and stood by me in every single step of my life. I feel happy and also lucky for having them.

May 2009

Burak Kantarcı
Computer Engineer, M.Sc

TABLE OF CONTENTS

Page

ABBREVATIONS

WDM	:	Wavelength Division Multiplexing
OXC	:	Optical Cross-Connect
DPP	:	Dedicated Path Protection
SBPP	:	Shared Backup Path Protection
SLA	:	Service Level Agreement
MRP	:	Most Reliable Path
MTTF	:	Mean Time To Fail
MTTR	:	Mean Time To Repair
FIT	:	Failure in 10^9 hours
CAFES	:	Compute-A-Feasible-Solution
GSS	:	Global Shareability Surveillance
LSS	:	Link-by-link Shareability Surveillance
ILP	:	Integer Linear Programming
G-DAP	:	Global Availability-Aware Differentiated Provisioning
LBL-DAP	:	Link-By-Link Availability-Aware Differentiated Provisioning
GSP	:	Generalized Segment Protection
AC-GSP	:	Availability-Constrained Generalized Segment Protection
SDAC-GSP	:	Shareability-Driven Availability-Constrained GSP

LIST OF TABLES

LIST OF FIGURES

LIST OF SYMBOLES

$\mathbf{A}$	:	Availability of a connection
A_{wc}	:	Availability of the working path of $connectionc$
A_{pc}	:	Availability of the protection path of $connectionc$
$\mathbf{U}$	:	Unavailability of a connection
δ_c	:	Surviving probability of connection c in case of multi-failure
Λ	:	Set of wavelengths on a specific link
ε	:	A negligible value very close to zero multiplied by the cost of a shareable link
$C_b(e)$	:	Cost of $link\ e$ when searching for a backup path
RD	:	Resource gain
RG_k	:	Resource gain for $class-k$
$S_e^{(k)}$	:	Average sharing degree for $class-k$ on $link\ e$
S_{avg}^k	:	Feasible sharing degree for $class-k$
ρ_e	:	number of connections utilizing $link\ e$ as a backup link
L_b	:	The set of backup links
C	:	The set of active connections
C_k	:	The set of active connections of $class-k$
$\lambda_s(e)$	:	Number of spare wavelengths on $link\ e$
$\lambda_f(e)$	:	Number of unutilized wavelengths on $link\ e$
S_c	:	Backup resource sharing group of $connection\ c$.

AVAILABILITY-CONSTRAINED ROUTING AND WAVELENGTH ASSIGNMENT AND SURVIVABILITY IN OPTICAL WDM NETWORKS

SUMMARY

Due to the tremendous development in the Internet applications, user demands which point to high bit rate downlink and uplink capacity with reliable, secure and robust connection requests have been increasing continuously. At this point, optical networks have appeared as the best solution for the Internet backbone due to the huge capacity of the fiber. A single fiber is able to multiplex the transmission capacity of a number of wavelength channels so that each separate connection can transmit its data stream at the speed of light and at a specific frequency without interfering the other channels. Thus, a single fiber can offer terrabits of bandwidth by multiplexing those wavelength channels each offering a transmission capacity of some tens gigabits per second. This multiplexing scheme is called Wavelength Division Multiplexing (WDM).

Besides the advantage of the huge capacity offered by the fiber, a serious problem due to this huge capacity co-exists with the advantages. In case of a failure of any optical component, such as a fiber or an optical node, all the connections passing through those components are prone to lose huge amount of data. Moreover, based on the repair time of the component, due to the long service outage time, the data lost may increase dramatically. Therefore, survivability schemes are proposed to set up the connections with pre-determined reliability requirements. Basically a survivability scheme reserves spare resources for a connection to be used in case of a failure along the connection's primary path. The spare resources can correspond to a whole path, spare links, sub-paths or ring-mesh protection structures. The spare resources can either be dedicated to a single connection or shared by a group of connections.

The probability of a connection to be in operational state at an arbitrary time is called the availability of the connection. Setting up a connection with a survivability scheme does not guarantee that the corresponding connection has 100% availability. Long switching time durations to the protection resources, multi-failures corresponding to the primary and backup resources or multi-failures corresponding to the sharing group of connections may cause a connection to be unavailable. Therefore, setting up a connection which consists of routing and wavelength assignment (RWA) has to consider these constraints to guarantee high availability for the provisioned connection.

This thesis study deals with availability constrained routing and wavelength assignment and survivability in optical networks. A detailed literature survey is provided for the related work in availability constrained connection provisioning. The main contribution of the thesis study to the literature has three main parts: 1) Availability-aware connection provisioning for network planning, 2)Availability-aware routing and wavelength assignment for differentiated availability services, 3)Availability analysis and connection provisioning in shared segment protection. Generally, the common target of all of the three points is to deal with the tradeoff between backup resource consumption and connection availability.

The first part deals with shared backup path protection (SBPP) to offer high availability for the connections under static and dynamic traffic demands by considering the resource consumption. A provisioning scheme, *dynamic sharing*, is derived from a conventional scheme that attempts to decide a feasible sharing degree for the wavelength channels, and assigns the costs of the arcs in the topology graph by using this estimated feasible sharing degree. The performance of this scheme is compared to a previously proposed scheme under SBPP and to a dedicated path protection (DPP) method. DPP is used as a reference for the connection availability and wavelength utilization. It is shown that the proposed scheme offers better availability to the connections in a static demand matrix and keeps the wavelength utilization significantly lower than DPP.

The *dynamic sharing* scheme is then adapted to work under dynamic traffic environment, and called *Global Shareability Surveillance (GSS)*. Obviously, determination of the sharing degree for the wavelength channels is a heuristic. Relying on the tradeoff between availability and the resource consumption, an integer linear programming (ILP) model is built to determine the feasible sharing degrees per-link basis, and called *Link-By-Link Shareability Surveillance (LSS)*. The determined global and link-by-link sharing degrees are used to assign appropriate link costs for RWA. The proposed schemes are compared to a conventional connection provisioning scheme. It is shown that GSS and LSS introduce better availability to the connections while keeping the resource overbuild in a feasible range. Moreover, LSS seems to outperform GSS and the conventional reliable connection provisioning scheme.

The second part of the thesis study deals with connection provisioning with differentiated availability requirements under dual failure consideration and resource limited environment. GSS and LSS are modified to work under differentiated availability requirements and dual failure consideration, and evolve to *Global Differentiated Availability-Aware Connection Provisioning (G-DAP)* and *Link-By-Link Differentiated Availability-Aware Connection Provisioning (LBL-DAP)*. Here, the estimated global and link by link feasible sharing degrees for the RWA link cost assignment are considered per-availability-class-basis. Obviously, G-DAP runs a heuristic periodically to obtain a global feasible sharing degree for a specific availability class while LBL-DAP constructs an ILP model periodically to obtain feasible sharing degrees on each link for each availability class. The proposed schemes are compared to a conventional reliable connection provisioning scheme, and it is shown that the proposed schemes introduce high acceptance rate to the connections while providing availability satisfaction. Besides this does not increase the resource overbuild.

In the last part, other than SBPP, the thesis study focuses on a different survivability scheme which is overlapping shared segment protection. Since there is no specific availability analysis for shared segment protection, an availability calculation method is introduced. The proposed method treats a segment protected connection as a serial system of protection domains. Each protection domain consists of the corresponding primary link and the segments that can provide spare capacity for it. Besides this, availability constraints due to sharing are also considered in the proposed availability analysis model. The proposed method is verified by simulation under different failure rate values and different loads.

The last part of the contribution in the thesis study proposes two availability aware connection provisioning schemes that are built on top of a conventional segment selection scheme, *Generalized Segment Protection (GSP)*. The first proposed scheme can be considered as the availability-aware version of GSP. Therefore it is named as *Availability Constrained Generalized Segment Protection (AC-GSP)*. The second scheme considers the tradeoff between connection availability and resource overbuild. It attempts to arrange the link costs by using this tradeoff function and its output of feasible sharing degree for each availability class. Therefore it is named as *Shareability Driven Availability Constrained Generalized Segment Protection (SDAC-GSP)*. SDAC-GSP also forces the connections to be protected by more number of segments by assigning the link costs for this aim under consideration of the feasible sharing degrees. The two proposed schemes are proposed under different environments and with respect to different performance parameters. The applicability of each of them is justified in terms of environmental constraints and certain parameters.

In summary, in this thesis, new approaches for availability planning of optical networks, differentiated availability aware routing and wavelength assignment under SBPP are proposed. Besides this, a less popular but more robust survivability scheme with availability constraint is also considered with availability-aware connection provisioning and its applicability. It is expected that the introduced methods are considerable for the service providers for their long term decisions.

SÜRDÜRÜLEBİLİR OPTİK WDM AĞLARINDA KULLANILABİLİRLİK KISITI ALTINDA YOL VE DALGA BOYU ATAMA VE SÜRDÜRÜLEBİLİRLİK

ÖZET

İnternet uygulamalarındaki hızlı ilerleme, kullanıcıların yüksek bit hızında veri alışverişinde bulunan, güvenilir, güvenli ve dayanıklı bağlantı isteklerindeki artışı da beraberinde getirdi. Bu şartlar altında, optik fiberin yüksek kapasitesinden ötürü, optik ağlar internet omurgası için en uygun çözüm olarak görünmüştür. Bir optik hat üzerindeki fiber, her biri farklı frekansta çalışarak birbiriyle girişimde bulunmayan ve ışık hızında veri iletimi sağlayan çok sayıdaki dalgaboyu kanalını üzerinde çoğullayabilmektedir. *Dalgaboyu Bölmeli Çoğullama (Wavelength Divison Multiplexing (WDM))* olarak adlandırılan bu yaklaşım kullanılarak, her biri saniyede on gigabitler (Gbps) düzeyinde iletim kapasitesi sağlayan çok sayıda dalgaboyu kanalı bir fiber üzerinde çoğullanarak saniyede terrabitler (Tbps) düzeyinde kapasite sağlanmaktadır.

Optik fiberin iletim kapasitesinden kaynaklanan avantajların yanı sıra, aynı özelliğinden kaynaklanan problemler de bulunmaktadır. Fiber veya optik düğümlerdeki kısa süreli bir arıza bile, sözkonusu optik elemanları kullanan tüm bağlantıların çok yüksek miktarda veri kaybında yol açabilir. Üstelik optik elemanlarda oluşan arızanın giderilme süresinin uzunluğuna bağlı olarak, kaybedilen veri miktarı da çarpıcı miktarda artabilir. Bu nedenle, bağlantı isteklerini önceden belirlenmiş güvenilirlik gereksinimlerini karşılayacak şekilde kurmak amacına yönelik sürdürülebilirlik mekanizmaları önerilmiştir. Temel olarak, sürdürülebilirlik yöntemleri, kurulan bir bağlantının kullandığı asal ışık yolu (*primary lightpath*) üzerindeki bir veya birden fazla hatta oluşabilecek hata durumunda, bağlantının kesintisiz devam etmesini sağlamak amacıyla yedek kaynak ayırırlar. Yedek kaynaklar kimi zaman kaynaktan varışa bütün bir yola karşılık düşerken kimi zaman bir hatta, birkaç optik hattın oluşturduğu parçalı bir yola veya halka-örgü yapılara karşılık düşebilir. Ayrılan yedek kaynaklar, tümüyle bir bağlantıya yedek kaynak olarak atanmış olabileceği gibi, bir grup bağlantı tarafından yedek kaynak olarak da paylaşılabilirler.

Bir bağlantının rastgele bir anda çalışır durumda olması, bağlantının kullanılabilirlik özelliği olarak tanımlanmaktadır. Bir bağlantının herhangi bir sürdürülebilirlik yöntemi ile birlikte kurulmuş olması 100% kullanılabilirlik özelliği olduğu anlamına gelmez. Asal ışık yolundan yedek kaynaklara anahtarlanma süresinin uzunluğu, asal ve yedek kaynaklar üzerinde çoklu hata durumlarından veya yedek kaynakları paylaşan bağlantılardan kaynaklanan çoklu hata durumlarından kaynaklanan nedenlerden ötürü bağlantının kullanılamaz olması durumu her zaman sözkonusudur. Bu nedenle, yol ve dalgaboyu atamadan oluşan bağlantı kurma aşaması, kurulan bağlantıya yüksek düzeyde kullanılabilirlik sağlayabilmek amacıyla bu kısıtları göz önünde bulundurmak durumundadır.

Bu tez çalışması optik ağlarda kullanılabilirlik kısıtı altında yol ve dalgaboyu atama ve sürdürülebilirlik konularını ele almaktadır. Kullanılabilirlik kısıtlı bağlantı kurma yöntemleri üzerine ayrıntılı bir literatür taraması kitabın ilk bölümlerinde verilmektedir. Bu çalışmanın literatüre ana katkısı temel olarak 3 bölümden oluşmaktadır: 1) Optik ağ planlamaya yönelik kullanılabilirlik kısıtlı bağlantı kurma, 2) Farklı servis sınıfları için kullanılabilirlik kısıtlı yol ve dalga boyu atama 3)Paylaşımlı segman koruma için kullanılabilirlik analizi ve kullanılabilirlik kısıtlı bağlantı kurma. Genel olarak her üç bölümün de üzerine eğildiği temel sorun kullanılabilirlik ve kaynak tüketimi arasındaki çelişkidir.

İlk bölüm paylaşılan ışık yolu korumasını (*Shared Backup Path Protection, SBPP*) sürdürülebilirlik yöntemi olarak kullanmakta ve kaynak tüketimini göz önünde bulundurarak, sabit bir trafik matrisinde belirtilen bağlantı isteklerine koşullar elverdiğince yüksek kullanılabilirlik sağlamayı amaçlamaktadır. Daha önceden önerilmiş ve bilinen bir yöntemden türetilerek *dinamik paylaşım* (*dynamic sharing*) olarak adlandırılan bu yöntem, dalgaboyu kanallarının olası paylaşılabilirlik derecesini dinamik olarak kestirmeye çalışmakta ve elde ettiği olasıl paylaşılabilirlik değerini de topolojide iki düğüm arasındaki her bir bağın maliyetini atamakta kullanmaktadır. Önerilen bu yöntemin, önceden önerilen yöntemle ve atanmış yol koruması (*dedicated path protection-DPP*) ile başarım karşılaştırması yapılmıştır. DPP'nin kullanım nedeni, bağlantı kullanılabilirliği ve dalgaboyu tüketimi için bir referans noktası oluşturmasından kaynaklanmaktadır. Önerilen yöntemin, bilinen yönteme kıyasla bağlantı başına kullanılabilirlik değerini arttırdığı ve dalgaboyu tüketiminin de DPP'den büyük oranda düşük tuttuğu görülmüştür.

Dinamik paylaşım yöntemi, dinamik trafik ortamına uyarlanmış ve *Global Paylaşılabilirlik Gözetimi* (*Global Shareability Surveillance (GSS)*) olarak adlandırılmıştır. Dalgaboyu kanalları üzerindeki olası paylaşılabilirlik değerlerinin kestirimi sezgisel bir yönteme dayanmaktadır. Kullanılabilirlik ve kaynak tüketimi arasındaki çelişkiden yola çıkarak bir optimizasyon modeli (*integer linear programming (ILP) model*) kurulmuş ve ILP modelinin çözümü ile her bir optik hat için ayrı bir paylaşılabilirlik değeri kestirilmeye çalışılmıştır. Bu gelişmiş yöntem, *Optik Hat Bazında Paylaşılabilirlik Gözetimi* (*Link-By-Link Shareability Surveillance, LSS*) olarak adlandırılmıştır. Elde edilen paylaşılabilirlik değerleri, yol ve dalgaboyu atama sırasında uygun maliyet atanması için kullanılmaktadır. GSS ve LSS yöntemlerinin başarımları, geleneksel bir güvenilir bağlantı kurma yöntemi ile karşılaştırılmıştır. GSS ve LSS'nin bağlantı istekelerine daha yüksek kullanılabilirlik sağladığı ve yedek kaynak tüketim oranını da kabul edilebilir bir aralıkta tuttuğu gözlenmiştir. Ayrıca kendi aralarındaki başarımları göz önünde bulundurulduğunda LSS yönteminin GSS ve geleneksel güvenilir bağlantı kurma yönteminin çok üzerinde bir başarım ile kullanılabilirlik sağladığı görülmüştür.

Çalışmanın literatüre katkısının ikinci kısmı, çoklu (çift) hata olasılığı bulunan ve kaynak kısıtlı ortamda, farklılaşmış servis sınıfları için kullanılabilirlik kısıtlı yol ve dalgaboyu atama problemini ele almaktadır. GSS ve LSS çift hata olasılığı, kaynak kısıtı ve farklı kullanılabilirlik sınıflarının bulunduğu ortamda çalışacak değişikliklerle yenilenerek sırasıyla *Global Farklılaşmış Kullanılabilirlik-Kısıtlı Bağlantı Kurma* (*Global Differentiated Availability-Aware Connection Provisioning, G-DAP*) ve *Optik Hatlar Bazında ve Farklılaşmış Kullanılabilirlik-Kısıtlı Bağlantı Kurma* (*Link-By-Link Differentiated Availability-Aware Connection Provisioning,*

LBL-DAP) adlarını almışlardır. Burada, dalgaboyu kanallarının, global veya optik hat bazında kestirimi yapılan paylaşılabilirlik değerleri her bir kullanılabilirlik sınıfı için ayrı ayrı hesaplanmaktadır. G-DAP, her bir kullanılabilirlik sınıfı için periyodik olarak çalıştırdığı bir kestirim fonksiyonu aracılığıyla kanal paylaşılabilirlik değerini kestirmektedir. LBL-DAP ise, aynı amaca yönelik kurduğu bir ILP modelini periyodik olarak çalıştırmakta ve her bir kullanılabilirlik sınıfına yönelik dalgaboyu paylaşılabilirlik değerini her bir optik hat için ayrı ayrı hesaplamaktadır. Önerilen yöntemler geleneksel bir güvenilir bağlantı kurma yöntemiyle karşılaştırılmış ve önerilen yöntemlerin yüksek bağlantı kullanılabilirliği, yüksek bağlantı kabul oranı sağladıkları, bunun karşılığında da yedek kaynak tüketim oranında da bir artışa neden olmadıkları gösterilmiştir.

Çalışma son kısmında, farklı bir sürdürülebilirlik mekanizmasının, örtüşen paylaşımlı segman korumanın üzerine eğilmektedir. Paylaşımlı segman koruma için bilinen belirli bir kullanılabilirlik analizi yöntemi bulunmamasından ötürü, öncelikle paylaşımlı segman koruma için bir kullanılabilirlik hesaplama yöntemi önerilmiştir. Önerilen hesaplama yöntemi, segman korumalı bir bağlantıyı seri bağlı koruma alanları olarak değerlendirmektedir. Her bir koruma alanı, bağlantının asal ışık yolundaki bir optik hat, ve bir hata durumunda o optik hat üzerinden akan trafiğin kotarılabileceği koruma segmanından oluşmaktadır. Bunun dışında, önerilen kullanılabilirlik hesaplama yönteminde, yedek dalgaboyu kanallarının paylaşımından kaynaklanan kullanılabilirlik kısıtı da göz önünde bulundurulmaktadır. Önerilen yöntem, simulasyonlar aracılığıyla farklı hata oranları ve yükler altında test edilerek doğrulanmıştır.

Son olarak, genelleştirilmiş segman koruması (*Generalized Segment Protection, GSP*) olarak bilinen geleneksel bir segman seçme algoritmasının üzerine kurulan iki farklı, kullanılabilirlik kısıtlı bağlantı kurma tekniği, paylaşımlı segman koruma için önerilmiştir. Birinci teknik, GSP'nin kullanılabilirlik kısıtını göz önünde bulunduran versiyonu olarak düşünülebilir. Bu nedenle *Kullanılabilirlik Kısıtlı Genelleştirilmiş Segman Koruma* (*Availability-Constrained Generalized Segment Protection, AC-GSP*) adı verilmiştir. İkinci teknik ise, kullanılabilirlik ve yedek kaynak tüketim oranı arasındaki çelişkiyi göz önünde bulundurmaktadır. Bu çelişkiden yararlanarak, segman oluşturmaya aday optik hatlar üzerindeki kanallar için olası paylaşılabilirlik dereceleri kestirmeye çalışarak, elde ettiği değerleri yol seçimindeki maliyet atamasında kullanmaktadır. Sözkonusu ikinci yöntem, *Paylaşılabilirliğe Yönelik Kullanılabilirlik Kısıtlı Genellleştirilmiş Segman Koruma* (*Shareability Driven Generalized Segment Protection, SDAC-GSP*) olarak adlandırılmıştır. SDAC-GSP aynı zamanda, bağlantı isteklerini, paylaşılabilirlik değerlerini de göz önünde bulundurarak, daha fazla segmanla korunacak şekilde yol seçimi yapmaya zorlamaktadır. Önerilen iki yöntem farklı başarım parametreleri ile farklı ortamlarda denenmiş ve karşılaştırılmıştır. Yöntemlerin uygulanabilirliği, çalıştıkları ortama ve başarım parametrelerine bağlı olarak belirlenmiş ve doğrulanmıştır.

Özetle, bu tez çalışması, paylaşımlı yol koruması altında optik ağların kullanılabilirlik planlaması ve farklı servis sınıflarının kullanılabilirlik kısıtlı bağlantı kurma gibi temel sorunlarına yeni yaklaşımlar tanıtmaktadır. Buna ek olarak, optik ağlarda kullanılabilirlik kısıtı altındaki çalışmalarda değinilmemiş olan paylaşımlı segman koruması da sözkonusu kısıt ile birlikte bağlantı kurma problemi ile ele alınmış ve uygulanabirliği tartışılmıştır. Çalışmanın bütününde, servis sağlayıcılar ve ağ

operatörlerinin uzun vadeli kararlarını alırken yararlanabilecekleri bilgilerin içerildiği umulmaktadır.

1. INTRODUCTION

As a result of the increase in the bandwidth demand of the next generation Internet applications, optical networks appeared as the best solution in order to offer bandwidth values in Tb/s by partitioning this bandwidth into a number of gigabits per second wavelength channels [1].

The deployment of optical networking can be either circuit switched (Wavelength Division Multiplexing, WDM) [2] or optical packet/burst switched (OBS/OPS) [3, 4]. Obviously, packet/burst switched architectures provide more efficient utilization of the fiber capacity, and they are the strongest candidates for future optical networking technology. However, currently, due to the lack of optical logic and constraints due to optical buffering, WDM seems the main concern for today's Internet backbone. Therefore, in this work, we focus on WDM as the optical networking technology.

The main components of a WDM network are the optical nodes consisting of optical cross-connects (OXC) and the transceivers. This node architecture routes the data transmission of the connections over several wavelength channels without interfering each other. Once the connection is provisioned, the data stream is converted to the optical format, and sent from source to the destination in the optical domain with neither any processing nor any optical-electronic-optical (o-e-o) conversion. The connection can either use the same wavelength or different wavelengths along the lightpath based on the deployment of wavelength converters at the intermediate nodes. Similar to the previous work in this topic, this thesis study deals with the nodes with wavelength conversion capability. Thus, a connection can switch between the wavelengths along the lightpath.

In WDM, each wavelength channel in a fiber is used as a virtual circuit, namely a $lightpath$, for an accepted connection request. Thus, each connection can transmit data at the speed of light. The capacity of fiber is partitioned into wavelength channels that provide the connections to use tens of gigabits per second. However, in case of a service interrupt on any component along the *lightpath*, the amount of data loss is also huge since the offered bandwidth is as huge as the fiber capacity [5]. Therefore, in case of a failure of a physical component along the lightpath, the delivery of the data to destination without error, preemption and loss introduces the problem of survivability and reliability in optical networks. Based on this fact, optical WDM networks should be designed based on a pre-determined survivability and reliability criteria for protection due to physical component failure. The survivability policy can be either protection or restoration. Protection reserves backup resources in advance at the time of connection provisioning while restoration finds an available lightpath on which the connection is to be switched when a failure occurs. Most of the survivability work relies on the protection schemes because of guaranteed recovery. Therefore, in this work we use the term "survivability policy" to represent "protection strategy".

Basically, survivability schemes can be implemented based on link protection, path protection [6] path-segment protection [7], or p-cycles [8]. These schemes can be implemented based on dedicated backup or shared backup concepts. Both the dedicated and shared protection schemes have advantages and disadvantages. The former one consumes more network resources while the latter one leads to less availability as it requires less redundancy. This phenomenon shows the trade-off between resource redundancy and restoration capability. Path-segment protection combines the advantages of the path protection and segment protection schemes [9]. On the other hand, p-cycle protection provides a mesh-like redundancy and ring-like restoration speed [10]. However, p-cycles lead to a high computational overhead during the cycle selection process.

Although an efficient survivability scheme is employed, in case of multiple errors and / or long switching durations to the backup path / segment / link, availability constraint on some links, channels, nodes and/or other physical components occurs. This phenomenon introduces the availability constraint as an input parameter for survivable protection/restoration and routing-and-wavelength assignment schemes in optical WDM network design [11]. Therefore, the availability of a connection is a function of the precise details of the failures (repair times, locations, etc.), the amount of backup resources, and the backup resource allocation scheme (shared

/ dedicated) [1]. Generally, availability (A) of a network resource (switch, fiber, wavelength channel, amplifier, multiplexer, demultiplexer, etc.) is computed as given in Eq.1.1, where MTTF is the mean time to fail, and MTTR is the mean time to repair. MTTR is usually fixed. The availability values of the components are obtained by the statistical data collected from the industry related to MTTF and MTTR parameters. MTTF is represented in terms of FIT (number of failures in 10^9 hours) while MTTR is represented in terms of hours. Besides these, since users require significantly high availability of resources, in most cases the unavailability (U) is also a major concern, and it is the complement of availability parameter as shown in Eq.1.2

$$A = \frac{MTTF}{MTTF+MTTR} \tag{1.1}$$

$$U = 1 - A = 1 - \frac{MTTF}{MTTF+MTTR} = \frac{MTTR}{MTTF+MTTR} \tag{1.2}$$

As it is seen from the equations above, availability stands for the probability of a system to be operational at an arbitrary time [12]. Therefore, a connection between a source-destination ($s-d$) pair is said to be available if it is in the *on* state at a random time.

Availability requirements of a connection are usually specified in the Service Level Agreement (SLA) which is signed between the user and the service provider. In case of a violation of the SLA, the service provider faces a certain penalty. Therefore, availability-constrained network design and connection provisioning is one of the key concerns for the network operator [13]. Some hardware solutions exist in the standards, such as the tandem connection monitoring module of the ITU-T G.709 standard. Thus, when a signal degradation is monitored by the module, the link is shut down before the failure occurs on the corresponding link so network availability and optical link availability is increased and the users are protected from the failure [14, 15]. However, rather than link-by-link hardware solutions, protocol based solutions are still emergent to guarantee the SLA requirements of the connections.

In the literature, majority of the routing and wavelength assignment (RWA) and survivability schemes do not consider the availability issue as a constraint. There are some availability analysis for the dedicated path protection (DPP), shared backup path protection (SBPP) [16], and p-cycles [17]. However, availability has started to be considered as a major concern in routing and wavelength assignment recently [18–22].

Most of the availability aware design schemes are centralized, however, there are also some works that consider distributed provisioning [23, 24]. Majority of the availability design works assume a working and backup path pair for the availability guaranteed provisioning of the connection, however it is rarely considered for a connection to be protected by multiple backup paths [25] or provisioned over multipaths [26] considering the availability constraints. In addition to all, although most of the availability-aware schemes deal with SBPP and DPP, there are also availability-aware design connection provisioning works with p-cycles [27], WDM rings [28, 29], and demand-wise shared protection which is a compromise of DPP and SBPP [30]. There are also some studies that deal with the economical solutions to offer certain level of availability for the connections [31].

In this thesis study, we come up with centralized survivable and reliable design schemes for optical WDM networks where the RWA for the connection provisioning is constrained to connection availability. We consider the trade-off between resource consumption and connection availability. Thus, the higher consumption, the better availability. However, in resource-scarce environment connections can be blocked either due to resource limitation or due to availability dissatisfaction. Therefore backup resource consumption is also considered by the proposed schemes. We work on shared protection schemes, namely SBPP and overlapping shared segment protection.

We start with connection provisioning in non-differentiated environment where connections are attempted to be provisioned by targeting the maximum availability per connection under consideration of the resource consumption. We propose an availability constrained connection provisioning scheme that is designed for and evaluated under static traffic demand and shared backup protection. The proposed scheme takes a two-step conventional connection provisioning scheme as a base. It is widely known that there is a tradeoff between efficient usage of resources and connection availability [32]. By using the tradeoff between availability and resource consumption, it tries to find the appropriate number of connections that can share a backup channel, namely the sharing degree. Obviously, sharing degree is one of the major factors that affect connection availability; the more shareability the less availability. We show that the proposed design scheme introduces enhanced unavailability to the connections, and it still consumes significantly less resources compared to a provisioning scheme with dedicated path protection [11]. In SBPP part of the work we use two topologies, namely 14-node NSFNET and 28-node European Optical Network(EON) topologies to evaluate also the topology dependence of the proposed schemes.

We adapt the proposed scheme that is for static traffic matrices to provide maximum availability for the dynamically arriving and releasing connections and resource-plentiful networks. The adapted scheme is called *Global Shareability Surveillance (GSS)*, and attempts to find a feasible global sharing degree for the backup channels on the links. As time passes, the protocol increments or decrements the feasible sharing degree on the links based on the feedback information on the connection availability and backup resource consumption information collected from the network. We then construct an ILP based model, *Link-by-Link Shareability Surveillance (LSS)*, to predict a separate feasible sharing degree for each link's channels in the network. This scheme periodically takes a snapshot of the network, and builds an ILP model. The output of the ILP model is a set of the feasible sharing degrees on the links. In the proposed techniques estimated shareability values are used to define link costs for backup path search. We evaluate GSS and LSS in terms of resource overbuild and average unavailability per connection and show that the proposed schemes lead to enhanced unavailability per connection while keeping the resource overbuild in a feasible range.

The second part of the work related to SBPP considers connections arriving with differentiated availability requirements. Here, the network is also assumed to be resource-scarce. Therefore, connection blocking probability arises as another issue other than connection availability and resource overbuild. We propose two connection provisioning schemes that are derived from GSS and LSS to work under differentiated availability, and are called *Global Differentiated Availability-Aware Connection Provisioning (G-DAP)* and *Link-By-Link Differentiated Availability-Aware Connection Provisioning (LBL-DAP)*. G-DAP attempts to determine a feasible global sharing degree for each availability class by running a heuristic function. LBL-DAP constructs and runs an ILP model to determine a separate feasible sharing degree for each availability class on each link. We show that the proposed schemes lead to low blocking probability, low resource overbuild, and high availability per connection. We also support the performance evaluation of the schemes by various statistical data.

Segment protection can be either overlapping or non-overlapping way [9, 33]. Non-overlapping segment protection leads to sub-path protection where the availability analysis is not hard but can be done by partitioning the availability analysis of SBPP. To the best of our knowledge, availability-constrained overlapping segment protection is not considered in the literature. Here, we also propose an availability analysis method for this protection policy. We validate our proposed method by simulation. Based on our proposed analysis model, we present two availability aware connection provisioning schemes, namely *Availability Constrained Generalized Segment Protection (AC-GSP)*, and *Share ability Driven Availability Constrained Generalized Segment Protection (SDAC-GSP)* that are availability-aware adaptation of a conventional segment selection algorithm, namely the *Generalized Segment Protection (GSP)* [34]. We evaluate and analyze the performance of our proposed schemes under resource-plentiful and resource-scarce environments. The reference topology used for performance evaluation of availability-constrained segment protection is the USNET topology which has more number of nodes and heterogeneous connectivity.

The rest of the thesis chapters are organized as follows:

• Chapter 2 starts with a summary of the survivability schemes in optical networks, defines the availability concept, and the existing availability analysis methods for different protection schemes. This chapter also summarizes existing availability-aware connection provisioning approaches.

• Chapter 3 includes the non-differentiated availability-aware optical network design issues under resource-plentiful environment with SBPP. It contains two subsections for the design under static and dynamic traffic, respectively. The performance evaluation and simulation details are also given at the end of the chapter.

• Chapter 4 presents the proposed differentiated availability-aware connection provisioning schemes for optical WDM networks under resource-scarce environment with SBPP. Performance analysis, comparison and the simulation details are also included at the end of the chapter.

- Chapter 5 proposes an availability analysis scheme for overlapping shared segment protection. This chapter includes the validation of the proposed analysis. Following the validation, based on the analysis we propose two availability-constrained connection provisioning schemes for overlapping shared segment protection. We analyze and compare the performance of the proposed schemes under resource-plentiful and resource-scarce environments. We support the performance comparison by presenting statistical data for the schemes under each condition.

- Chapter 6 concludes the thesis by discussing the outcomes and the possible future directions for the work.

2. SURVIVABLE OPTICAL NETWORKS AND AVAILABILITY

2.1 Survivability

Due to the huge capacity of the fiber, in case of a component failure, the data loss can be as huge as the capacity of the fiber. A component can be an OXC, a wavelength channel, an amplifier, a transceiver, or the fiber itself. Therefore, optical network connections have to be provisioned with a pre-determined survivable design. Survivable connection provisioning is achieved by protection and restoration mechanisms [35]. The most basic protection strategy is the deployment of the self-healing rings for the ring topologies [36]. In Figure 2.1 working of a self-healing ring is illustrated. The figure on the left show the normal working condition. The traffic from *node A* to *node D* flows through *node B* and *node C*. As seen in the figure on the right, once the link between B and C fails, the traffic is re-routed and switched on the protection path, i.e it is sent through *node E*. The connection can switch from the working path to the protection path in approximately 50-60 ms. Although this switching time is significantly fast, the overhead of this protection strategy occurs in resource consumption where 100% redundancy exists. Here, note that the terms primary path and working path are used interchangeably so as the terms backup path and protection path.

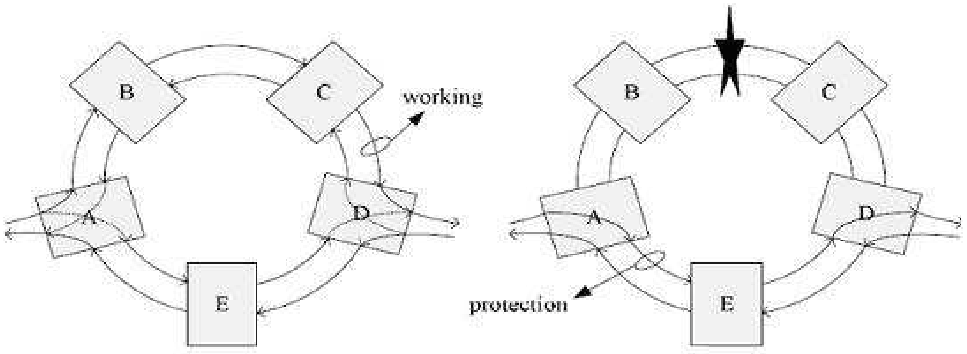


Figure 2.1: A sample of self-healing protection before and after the failure

Obviously, self-healing rings are not the appropriate protection strategy for the mesh topologies. To avoid resource consumption, span or path oriented protection-based strategies are used [37]. These protection techniques can be implemented either as dedicated protection or shared protection [6]. Restorability and redundancy are the main design objectives in survivable optical networks.

$$Restorability = \frac{Restored\_capacity}{Failed\_capacity} \qquad \textbf{(2.1)}$$

$$Redundancy = \frac{Number\_of\_spare\_capacity}{Number\_of\_protected\_capacity} \qquad \textbf{(2.2)}$$

As seen in the equations, there exists a tradeoff between restorability and redundancy. Thus, the more redundant resources are deployed, the more restorable connections are provisioned.

2.1.1 Span-oriented protection

The aim of the span oriented protection is the recovery of the traffic on a single span if a failure occurs on the corresponding location. Once a component fails on the span, the traffic is rerouted on the backup span which surrounds the failed span [6]. The protection can be implemented either in dedicated or shared way. In Figure 2.2.a, dedicated link protection scenario is illustrated. In case of a failure on the links 1-2 or 5-6, the traffic flowing from *node* 1 to *node* 2 has to be routed through the nodes 1-5-2 over the wavelength λ_2. Similarly, the traffic between 5-6 has to be routed through the path 5-2-6 over the wavelength channel λ_1. As it is seen, the backup paths for the spans 1-2 and 5-6 intersect on the link 2-5. Therefore the traffic flows should be carried on different wavelength channels in case of failure.

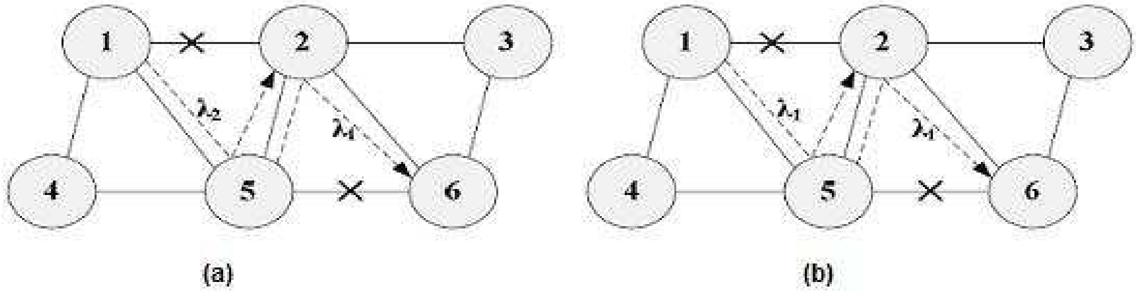


Figure 2.2: Span Protection a. Dedicated b.Shared

Figure 2.2.b illustrates the same protection strategy by means of shared protection where the traffic flows can share their backup resources. The spans 1-2 and 5-6 are protected by the same backup route. However, on the shared link in their backup paths, they share the dedicated wavelength, λ_1. Thus, in case of a failure on either of the links, the shared resource is activated by the connection that has the failed span on its working path. However, if both of the spans fail, only one of the connections is able to activate and use the protection path for the failed span while the other connection is unavailable. Therefore for the sake of decreasing the resource consumption, this mechanism can restore at most one of the failures while the dedicated scheme survives in case of dual-failure (and multi-failure).

2.1.2 Path protection

Path protection is an enhanced version of link protection. Similar to link protection, path protection may be dedicated or shared as link protection is implemented. In path protection, the primary path is protected by a backup path which is link-and-wavelength-disjoint to itself. In Figure 2.3, a dedicated path protection scenario is shown. In the figure, two connections are illustrated. $Conection-1$ is set between $node$ 1 and $node$ 3 while $Connection-2$ is set between $node$ 4 and $node$ 6. Figure 2.3.a, shows a dedicated path protection scenario for these connections. $Connection-1$ is routed along the path 4-5-6 over the wavelength λ_1. $Connection-2$ is routed through the path 1-2-3 over the wavelength λ_1. Backup paths of the connections are routed along the lightpaths (4-1-2-6, λ_2), and (1-5-2-6-3, λ_1) respectively. Here the notation ($i-j-k$, λ_w) represents the lightpath passing through the nodes i, j, k and uses the wavelength λ_w on the links.

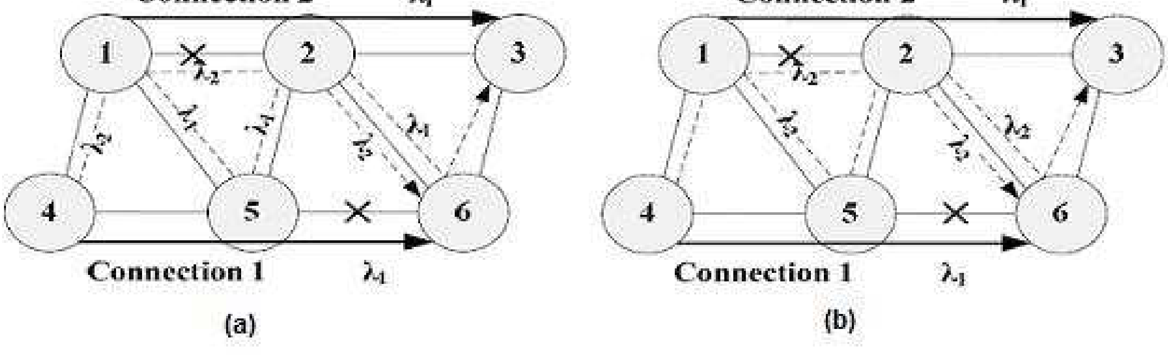


Figure 2.3: Path Protection a. Dedicated b.Shared

Figure 2.3.b illustrates shared backup path protection scenario for the same connections in Figure 2.3.a. Thus, the primary and backup routes for $Connection-1$ and $Connection-2$ are the same as they are in DPP. Wavelength utilization for the primary paths of the connections is also the same as it is in DPP. However, the backup paths are routed over the same wavelength, namely λ_2 for both of the connections. The backup paths of the connections intersect on the link 2-6. However, the backup paths are allowed to share the wavelength λ_2 for restoration. In case of a failure on the path passing through the links 4-5-6, $Connection-1$ switches to its backup path and utilizes the backup wavelengths on each link, and vice versa. If there is a concurrent failure on the primary paths of the connections, at most one of them can utilize the backup wavelength on the shared link. Thus, the other one will be unavailable.

Here, the term shared risk link group (SRLG) occurs. The connections that are affected by the failure of each other's primary resources are supposed to be in the same SRLG. In a network that is designed with a survivability constraint, the connections that are in the same SRLG, affect the availability parameter of each other. It is worth noting to mention that Figures 2.1, 2.2, and 2.3 are adapted from [38].

2.1.3 Segment protection

A hybrid of path protection and span protection is called path-segment protection or segment protection [39]. The primary path of the connection is partitioned into fixed or variable length path-segments. Each segment is protected by a protection segment. The primary segment and its protection segment form a protection domain. The consecutive protection domains may be either overlapping or non-overlapping.

If there exists two disjoint paths between a source and a destination, then a non-overlapping segmented protection solution is guaranteed for any selected primary path. However, for any primary path, disjoint end-to-end protection paths are not guaranteed. Therefore, segment protection is resource efficient like span protection and timely as path protection. Thus, path-segment protection introduces the advantages of low blocking probability, QoS guarantee, and improved resource utilization [40].

Figure 2.4 shows a sample of overlapping segment protection. The primary path is partitioned into adjacent segments, and each segment is covered in a protection domain [41] that overlaps with its adjacent protection domains. In case of a failure

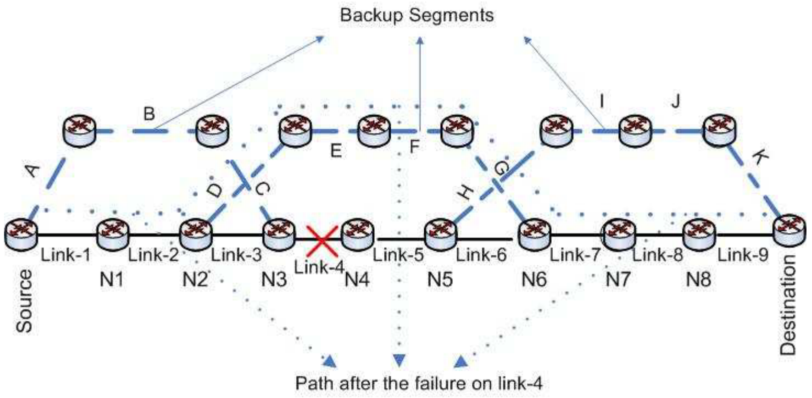


Figure 2.4: Overlapping Segment Protection

in any primary segment, the traffic flowing over that segment is dilated within the corresponding protection domain. Thus, this scheme can handle multi-failure along the primary lightpath, and even multi-failure on the backup links set. Figure 2.4 also illustrates a simple failure scenario. There are three protection domains in the figure. The start and the end node pairs of the protection domains are as follows: ($Source$, $N3$), ($N2$, $N6$), and ($N5$, $Destination$). Once $link-4$ which is in the second protection domain fails, the traffic from the $Source$ node to the $Destination$ node is routed through the protection segment of the protection domain between $N2$ and $N6$. The traffic is routed through the primary path beyond $N6$.

In shared implementation of the segment protection, to guarantee 100% survivability, the connections can share the all the backup channels on the protection segments unless those segments protect the common links of the primary paths of the connections. Thus, shared risk group concept works similar to path protection.

2.1.4 Pre-configured Protection Cycles

Pre-configured protection cycles (p-cycles) are proposed to be a compromise between self-healing rings and mesh protection. They offer ring-like fast recovery, and mesh-like capacity efficiency [8,10,38,42]. A simple illustration of p-cycle protection is shown in Figure 2.5. Under the failure-free state, the allocated spare capacity is idle. There are two types of links, namely the on-cycle links and the straddling links. Like a self-healing ring, an on-cycle link on a p-cycle is protected by the remaining part of the cycle in the reverse direction. A straddling link has its end nodes on the cycle although it is not on the cycle. Therefore a straddling link is protected by two protection paths in opposite directions. Several integer linear programming (ILP) solutions [10] and heuristics [43–45] are proposed for determining and/or reconfiguration of p-cycles for single or multiple failure cases.

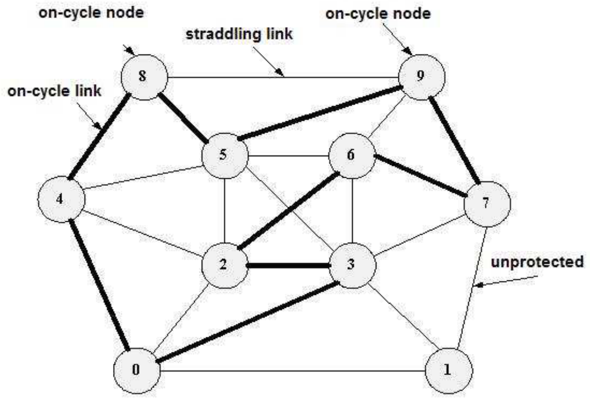


Figure 2.5: A sample p-cycle protection

In the figure above, the sample p-cycle consists of the links between the nodes 0-4-8-5-9-7-6-2-3-0. The spare capacities on the links are used to form the p-cycle which between the nodes 0-3-2-6-7-9-5-8-4-0. 0-3, 3-2, 2-6, 6-7, 7-9, 9-5, 5-8, 8-4, 4-0 are the on-cycle links. The straddling links that are off-cycle and whose end nodes are on the cycle for this p-cycle are 0-2, 2-4, 2-5, 3-5, 3-6, 3-7, 4-5, 5-6, 6-9, and 8-9. Consider the on-cycle link 4-8 fails. The traffic on the failed link is routed on the path 4-0-3-2-6-7-9-5-8. Consider the straddling link 4-5 fails. The traffic on the failed link is routed either through the path 4-8-5 or 4-0-3-2-6-7-9-5.

2.2 Availability

Survivability is a major concern as explained in the previous subsection. However, although the network is designed by using an appropriate survivability scheme, the connection is not guaranteed to be always at the "on" state. Due to dual/multiple failure of some components or long switching durations to the backup resources, availability constraint on the connections occurs. Basically, as a design constraint, availability stands for the probability of a network component, a wavelength channel or a connection path working at a random time t [46]. For a restorable system, the mathematical formulation for the availability (A) is introduced in Equation 1.1 where $MTTF$ stands for the mean-time-to-failure, and $MTTR$ stands for mean-time-to-repair after a component fails. Theoretically, A lies between 0 and 1. However, practically it is expected to be at the level of 0.99. Therefore, in some calculations, the unavailability parameter U (U = 1 - A) is preferred as the design constraint. The closed formulation for unavailability is also given in Equation.1.2. The $MTTF$ and $MTTR$ values are statistical data that are usually collected from the industry.

In network's point of view, the availability of a connection is a function of the failure probabilities of the hardware components along the transmission path [11]. Most of the studies model the failure of a component as a memoryless system with a constant failure rate λ in terms of FIT (1 FIT = probability of one failure in 10^9 hours). Thus, λ stands for $\frac{1}{MTTF}$. Failure rates are usually modeled with respect to Poisson arrival distribution. Thus, for a connection to have one failure in a time duration of t is shown below in Equation 2.3. $MTTR$ can follow exponential, weibull or lognormal distribution [47]. However, it is very common that $MTTR$ is taken as fixed or exponentially distributed. Thus, the probability distribution of the repair model of a system is considered as shown in Equation 2.4.

$$P(Failure,t) = \frac{t}{MTTF} \cdot e^{-(\frac{t}{MTTF})} \tag{2.3}$$

$$P(Repair,t) = \frac{t}{MTTR} \cdot e^{-(\frac{t}{MTTR})} \tag{2.4}$$

In [19, 48], the availability formulae of the parallel and series systems are given. Let the availability of a series system consisting of n elements be represented by A_s, and let the i^{th} component in the system has the availability A_i. A_s can be represented by the closed formula in Equation 2.5. If the system is parallel configured, at least one component has to be available for the system to be available. Therefore, A_s can be calculated as given in Equation 2.6. The product term stands for the unavailability of the system where all the components are unavailable. Taking one's complement of the system leads to the availability of the parallel system.

$$A_s = \prod_i A_i \tag{2.5}$$

In optical networking research, common assumption is that the optical nodes have 100% availability so the major failures are on the optical links. However, there are also some works that deal with availability in presence of node failure [49].

$$A_p = 1 - \prod_i (1 - A_i) \tag{2.6}$$

2.2.1 Availability Analysis in Optical WDM Networks

2.2.1.1 Linear Models

The first studies on availability in optical networks starts with the SONET rings [50, 51]. Later, it is also possible to see some works on availability and multi-services IP networks [52]. Today, majority of the works on availability and optical networks move towards optical WDM networks [6, 11, 16, 53–57], and multi-granular optical networks [18, 58].

In [57], the availability of the optical connections are analyzed subject to the distance between the nodes and the number of hops in the route. The failure rates of the network components are based on realistic measurements of the recent studies. The summary of the failure rates of those components are given in 2.1. The network components considered for the availability analysis are as follows:

The failure rate of a (de)multiplexer (*MUX / DEMUX*) is considered to be proportional to the number of wavelengths per fiber. The failure rate of the optical amplifier (*EDFA*) is considered to be constant.

Two different optical switch architectures are considered, namely Optical Switch 1 and Optical Switch 2. *Optical Switch 1 (OSW1)* is an optical add/drop multiplexer (OADM) with two dimensional microelectromechanical systems (2D-MEMS). W incoming lightpaths are switched to M ports. In [59] the authors give an upper bound of 21 FIT for the failure rate of a 2D-MEMS based OADM. Therefore, in an optical network, the failure rate of an OSW1 can be considered as $21 \cdot W \cdot M$. *Optical Switch 2 (OSW2)* is based on 3D-MEMS and wavelength selective optical cross-connects (OXCs) can be considered in this category. Since the 3D-MEMS-based switches have mirrors that are twice the number of inlets, the wavelength selective switch has $2N$ input and output ports. Thus, based on [59], the failure rate of OSW2 can be taken as $21 \cdot 2 \cdot 2N$ FIT.

Digital Switch 1 (DSW1) can operate with opaque OADMs that support W wavelengths. The failure rate for a $4 * 4$ switch is given as 3500 FIT so, assuming that the failure rate is proportional to the number of input channels, the failure rate for a DSW1 is $875 \cdot W$ FIT. *Digital Switch 2 (DSW2)* operates with opaque OXCs and supports $N \cdot W$ channels where N is the number of incoming fibers and W is the number of wavelengths per fiber. By using the same method above, the failure rate for DSW2 is found as $875 \cdot W \cdot N$.

Three types of couplers can be considered, namely $Coupler-1$, $Coupler-2$, and $Coupler-3$. The failure rate of a coupler is considered to be proportional to the number of the outgoing ports. A lower bound (25 FIT) for a coupler is determined in previous studies. Thus, $Coupler1$ is a $1:2$ splitter so the failure rate for $Coupler1$ is 50 FIT. $Coupler2$ is a $1:W/4$ splitter. Therefore it has a failure rate of $25 \cdot W/4$ FIT. Failure rate of $Coupler3$ which is a $1:(N-1)$ splitter can be calculated in a similar way. Here, N is the number of incoming fibers to the OXC. The failure rate of $Coupler3$ is $25 \cdot (N-1)$ FIT. Failure rates for Tunable Transmitter, Fix Transmitter, Tunable Receiver, Fix Receiver are given in [57] based on the previous research. It is also possible to find other values used for the availability of the optical components [60, 61]

Table 2.1: Component Failure Rates. W = Number of wavelengths per fiber, N = Number of incoming fibers

Component	Symbol	Failure Rate (FIT)
MUX/DEMUX	MUX	$25 \cdot \mathrm{W}$
EDFA	EDFA	2850
Optical Switch 1	OSW1	$21 \cdot W \cdot W/4$
Optical Switch 2	OSW2	$21 \cdot 2 \cdot 2N$
Coupler 1	COUP1	$25 \cdot 2$
Coupler 2	COUP2	$25 \cdot W/4$
Coupler 3	COUP3	$25 \cdot (N-1)$
Tunable Transmitter	TTx	745
Tunable Reciever	TRx	470
Fix Transmitter	FTx	186
Fix Reciever	FRx	70
Digital Switch 1	DSW1	$875 \cdot W$
Digital Switch 2	DSW2	$875 \cdot W \cdot N$
Wavelength Blocker	W/B	$50 \cdot W$

In [57], the authors draw the availability of a connection by paying attention to the path length and the number of hops traversed. 40 wavelengths are assumed to be supported, and 310 FIT per kilometer is taken as the link failure rate. To draw a closed formula for connection availability, they define the availability penalty (*AP*) for a system which is given in Equation 2.7 where FR stands for failure rate of the system.

$$AP = 10^{-9} \cdot FR \cdot MTTR \qquad \textbf{(2.7)}$$

The connection availability is derived using the availability penalty for the components along the path, and the closed formula of the connection availability is given in Equation 2.8. $AP_{link-km}$, AP_{add}, AP_{drop}, $AP_{pass_t hr}$, AP_{reg}, and P_{reg} stands for link availability penalty per kilometer, availability penalties due to adding, dropping, passing through, regeneration node operations, and the ratio of the nodes where signal regeneration is required.

$$\begin{aligned} A_c = 1 \ - \ (&AP_{link-km} \cdot D \ + \ AP_{drop} \ + \ AP_{add} \ + \\ &AP_{pass\_thr} \cdot \ulcorner (NH-1) \cdot (1-P_{reg}) \urcorner \ + \ AP_{reg} \cdot \llcorner (NH-1) \cdot P_{reg} \lrcorner) \qquad \textbf{(2.8)} \end{aligned}$$

Based on the assumptions and the formulae given above, availability maps are derived for wavelength selective, select-and-broadcast and opaque *OADMs* and *OXCs*. It is shown that the transparent node architectures outperform the opaque architectures in terms of availability. Moreover, when *OADMs* are used, wavelength selective structure has to be preferred for high availability while wavelength selective and select-and-broadcast architectures lead to the same performance when *OXCs* are used.

In [20], a comparison on analytical and simulation approach for availability analysis of optical transport network is given. Two network architectures are considered, namely passive WDM network (PWN) and automatic switched WDM network (ASWN). In PWN, static cross-connecting is used, and no restoration is allowed. On the other hand, AWSN performs dynamic wavelength path provisioning. Component availability model is based on Markovian ON/OFF process. The network availability is calculated by using a logical transport entities hierarchy. At the bottom of the transport entities hierarchy, wavelength channel exists. On top of the wavelength channel, wavelength path and logical channel exists. At the highest level, there is the logical connection entity. Network availability analysis is performed for no protection, $1+1$ dedicated path protection, and path restoration $(1:m)$ schemes.

Arci et. al [16] study the availability models for the most common protection techniques by giving the relations between the dedicated and shared protection techniques and some network parameters assuming that the RWA has just been employed. The analysis starts with the basic $1:1$ protection scheme, then the numbers of working lightpaths and protection lightpaths are increased ($1 : N$ and $M : N$ protection respectively). These schemes are given in Figure 2.6. For the mesh shared cases, $2 * (1 : 1)$ shared protection and $m * (1 : 1)$ shared protection schemes that are shown in Figure 2.7 are considered. In the book, the difference between reliability and availability is formulated as follows, E_{xy} being a random variable pointing the state of the component xy:

- E_{xy}: xy has never failed up to time $t \Rightarrow P\{E_{xy}\}$:Reliability
- E_{xy}: xy operates at time t independent of the previous events $\Rightarrow P\{E_{xy}\}$: Availability

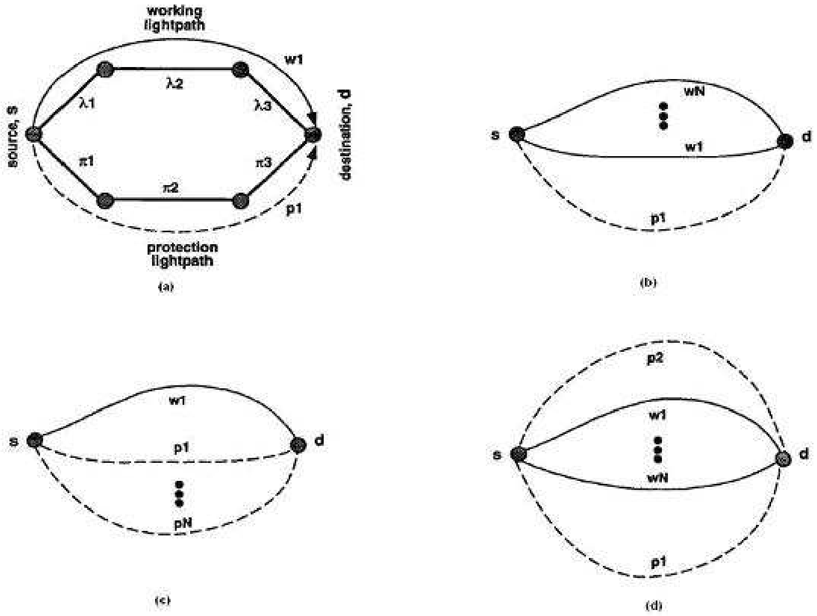


Figure 2.6: Dedicated and Shared Path Protection Schemes for availability analysis (a) 1:1 (b) 1:N (c) N:1 (d) 2:N (Arci, 2003)

In [16], the availability of an entity is represented by A_{xy} where x represents the entity itself, and y represents the index of the element. y stands for the index of the entity while x can be either w or p representing the working or the primary path of the corresponding entitiy respectively. Thus, the analysis starts with A_{wi}, namely the availability of the working path i. The closed form expression of A_{wi} is given in Equation 2.9. As it is seen, a working path is a series of wavelength channels.

$$A_{wi} = \prod_{\forall \lambda_j \in \Lambda_{wi}} A_{\lambda j} \qquad \textbf{(2.9)}$$

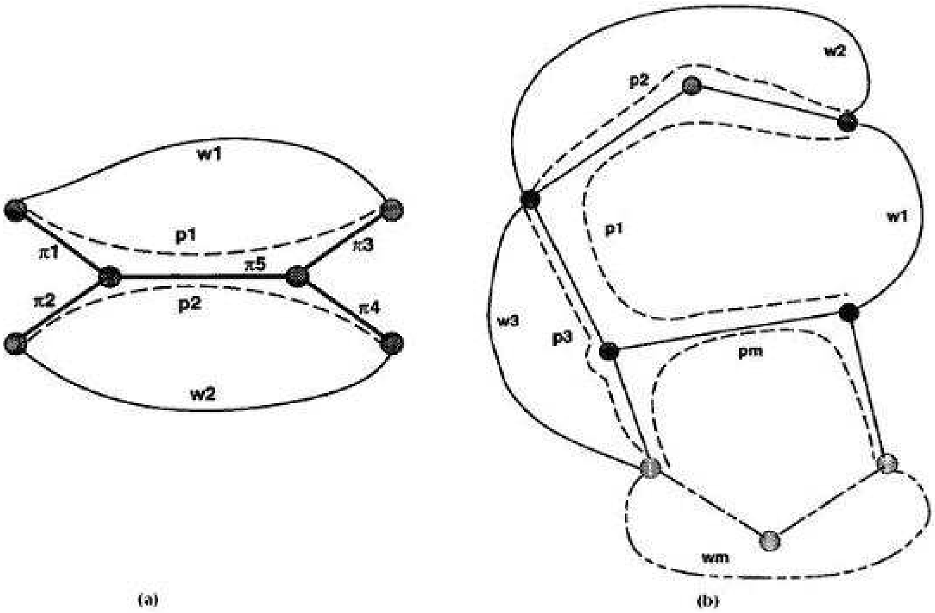


Figure 2.7: Shared Backup Path Protection Schemes for availability analysis (a) 2*(1:1) mesh protection (b) m*(1:1) mesh protection (Arci, 2003)

The open form of the availability of the 1 : 1 system (Figure 2.6.a) is given in Equation 2.10. In the figure, a 1 : 1 system with one connection ($k1$) is given. The system consists of a parallel configuration. Therefore the system is available either the primary path ($w1$) or the protection path ($p1$) works. For 1 : N protection case in Figure 2.6.b, N is taken as 2. The same principle works here with a little difference; at most one of the primary paths can be down and be protected by the protection path. Thus, the availability of the system is formulated in Equation 2.11. Besides this, a general closed form expression is given for a generic number of N in Equation 2.12. If we would like to compute the availability of a single connection i, either its primary path has to work or in case of a failure of its primary paths, all the other primary paths have to work. Then the closed form of a single connection's availability is given in Equation 2.13.

$$A_{11} = A_{k1} = A_{w1} + A_{p1} - A_{w1} \cdot A_{p1} \qquad \textbf{(2.10)}$$

$$A_{12} = A_{w1} \cdot\ A_{w2} + A_{w1} \cdot\ A_{p1} + A_{p1} \cdot\ A_{w2} - 2 \cdot A_{w1} \cdot\ A_{w2}\, A_{p1} \qquad \textbf{(2.11)}$$

$$A_{1N} = (1 - N \cdot A_{p1}) \cdot\ \prod_{j=1}^{N} A_{wj} + \sum_{h=1}^{N} [A_{p1} \cdot \prod_{j=1}^{N} A_{w(j \neq h)}] \qquad \textbf{(2.12)}$$

$$A_{1N}^{ki} = A_{wi} + (1 - A_{wi}) \cdot A_{p1} \cdot \prod_{j=1}^{N} A_{w(j \neq h)} \qquad \textbf{(2.13)}$$

As it is seen in Figure 2.6.c, one connection is protected by M protection paths ($M:1$). In the figure, $M = 2$ so either the working path has to be operating or if it fails, at least one of the protection paths has to work. This condition is formulated in Equation 2.14 for 2:1 DPP. Under these circumstances, for connection $k1$, the generalized form of the availability function is also given in Equation 2.15.

$$A_{21} = A_{w1} + (1 - A_{w1}) \cdot (1 - A_{p1}) \cdot A_{p2} + (1 - A_{w1}) \cdot (1 - A_{p2}) \cdot A_{p1} \qquad \textbf{(2.14)}$$

$$A_{21}^{k1} = A_{w1} + (1 - A_{w1}) \cdot \sum_{i=1}^{m} [\prod_{j=1}^{m} (1 - A_{p(j \neq i)})] \cdot A_i \qquad \textbf{(2.15)}$$

Availability analysis of $M:N$ scheme is the last and the most complicated of the DPP schemes. To keep it simple, it is assumed that M=2 since there are $C(N+2,\ N)$ different cases to be considered for availability analysis. For $2:N$ scheme, three cases should be considered: 1) All the primary paths work, 2) One primary path fails and it is protected by a protection path, and 3) Two primary paths fail and they are protected by the two protection paths. This scenario is formulated in Equation 2.16 to calculate the availability of the $2:N$ protection system.

$$\begin{aligned} A_{M2} = & \prod_{i=1}^{N} A_{wi} + \sum_{i=1}^{N} [(1 - A_{wi}) \cdot (A_{p1} + A_{p2} - A_{p1} \cdot A_{p2}) \cdot \prod_{j=1}^{N} A_{p(j \neq i)}] \\ & + \sum_{i=2}^{N} \sum_{j=1}^{i-1} (1 - A_{wi}) \cdot (1 - A_{wj}) \cdot A_{p1} \cdot A_{p2} \cdot \prod_{k=1}^{N} A_{w(k \neq i,j)} \qquad \textbf{(2.16)} \end{aligned}$$

In [16], the availability of two mesh shared protection schemes are also analyzed. As shown in Figure 2.7, the simplest shared backup path protection (SBPP) scheme is $2 * (1:1)$ mesh protection. To calculate the availability of the system, the cases where at most one connection fails have to be considered. Dual failure case leads to unavailability since the connections share a link on their protection paths. The availability of the system is formulated in Equation 2.17. To draw the availability of a connection (k1) in this scenario, dual failure cases have to be taken into account. In Figure 2.7.a, the πi symbols on the links represent the wavelengths on which the corresponding connection carries its traffic. Connection $k1$ is available if one the following four conditions holds: 1)Both of the primary paths work, 2)Primary paths of both of the connections work. 3)Primary path of $k1$ fails, protection path of $k1$ is activated, primary path of $k2$ fails, and the wavelength ($\pi 2$) on the first link of the protection path fails, 4) Primary path of $k1$ fails, protection path of k1 is activated, primary path of $k2$ fails, the wavelength ($\pi 2$) on the first link of the protection works, and the wavelength ($\pi 4$) on the last link of the protection path fails. Thus, the availability of the connection $k1$ is evaluated in Equation 2.18.

$$A^{mesh}_{2(1:1)} = A_{w1} \cdot A_{w2} \; + \; (1 - A_{w1}) \cdot A_{w2} \cdot A_{p2} + (1 - A_{w2}) \cdot A_{w1} \cdot A_{p1} \qquad \textbf{(2.17)}$$

$$\begin{aligned} A^{k1}_{2(1:1)} = & A_{w1} \; + \; (1 - A_{w1}) A_{p1} \cdot A_{w2} \; + \; (1 - A_{w1}) \cdot A_{p1} \cdot (1 - A_{w2}) \cdot (1 - A_{\pi 2}) \\ & + \; (1 - A_{w1}) \cdot A_{p1} \cdot (1 - A_{w2}) \cdot A_{\pi 2} \cdot (1 - A_{\pi 4}) \end{aligned} \qquad \textbf{(2.18)}$$

In Figure 2.7, $m * (1:1)$ shared mesh protection scenario is illustrated. In the figure, multiple failure cases are discarded to derive the system availability expression [16]. Therefore, system availability is approximated to the formula given in Equation 2.19. For the system to be available, either all of the primary paths have to work or there has to be at most one failed primary path which is recovered by its protection path. For a single connection's point of view, it is available if either its primary path works or the traffic that flows over its failed primary path is recovered by its protection path while the primary paths of the remaining connections are active. This is also formulated in Equation 2.20.

$$A^{mesh}_{m(1:1)} \; \cong \; \prod_{i=1}^{m} A_{wi} \; + \; \sum_{j=1}^{m} (1 - A_{wj}) \cdot A_{pj} \cdot \prod_{h=1}^{m} A_{w(h \neq j)} \qquad \textbf{(2.19)}$$

The analytical availability evaluations given above are compared with the simulation work, and it is shown that this approach is capable of estimating the system and connection availability. It is also shown that, for $M:N$ SBPP scheme, the number of shared paths affect the availability, other than the number of sharing paths. Therefore, the most important availability parameters are proposed to be the connection path length and the number of shared paths for the SBPP [16]. It should be noted that, these analyzes consider only link and wavelength channel failures. The effect of the path length on the availability was also stated in [57].

Another availability analysis approach for SBPP is proposed in [62]. Here, on the contrary of the former analysis, the connection is supposed to have the chance to survive if its working path fails together with one or more working paths in its sharing group. When there are n working path failures in its sharing group, the connection c

$$A^{ki}_{m(1:1)} = A_{wi} + (1 - A_{wi}) \cdot A_{pi} \cdot \prod_{k=1}^{m} A_{w(k \neq i)} \qquad \textbf{(2.20)}$$

is still supposed to get the shared backup channel with a probability of δ as shown in Equation 2.21. As seen in the equation, connection c is said to be available either its working path (A_{wc}) is available or when its working path fails, its backup path is still available (A_{pc}) and in case of n working path failures (ρ_n) in its risk group it has the chance to survive ($\delta_n^{(c)}$).

$$A_c = A_{wc} + (1 - A_{wc}) \cdot A_{pc} \cdot \sum_n \rho_n \cdot \delta_n^{(c)} \qquad \textbf{(2.21)}$$

A comparative study for the analysis of different protection schemes is done in [63]. The related work deals with three protection schemes namely, span protection, path protection and protection cycles. The authors also provide an estimation for the availability optimization potential. One of the major contributions of this work is that it provides a comparison between these three protection methods with respect to availability and redundancy.

Another analytical model for availability calculation under multi-failure assumption with SBPP is presented in [64]. In the proposed scheme, a connection is assumed to be provisioned with a working path and n backup paths. The closed formula for availability calculation of the connection is given in Equation 2.22. The term in the parenthesis refers to the unavailability of the connection where m is the total number of possible failures in the network, P_i is the probability of the $failure - i$ to occur, and U_d^i is the probability of the connection to be unavailable when $failure - i$ occurs.

$$A_c = 1 - (\sum_i^m U_c^i \cdot P_i) \qquad \textbf{(2.22)}$$

Calculation of the term in the parenthesis is done by the proposed algorithm in [64] based on the assumption that the network fault state prtobabilities (P_i) are known in advance. The algorithm attempts to obtain U_c^i values by considering each failure state, all of the working / backup paths of the connections, and the sharing information on the backup links. It is stated that the algorithm can calculate the availability of a connection less than one minute. Thus, the proposed method can be considered to be used for network planning rather than a dynamic environment.

A restoration aware connection availability analysis is introduced in [65]. The physical unavailability of a span is used to obtain the *equaivalent unavailability* of the span which is used to calculate the availability of the connection. Equivalent unavailability is a function of the physical unavailability of the span, physical unavailability of the other spans, and the restorability of the traffic on the span. The unavailability of a connection is the sum of the equivalent unavailability of its working spans. Thus the equivalent unavailability of the working span i is calculated as shown in Equation 2.23 where U_i^{phy} is the physical unavailability of the i^{th} working span, $NT_i/d_{s,t}$ is the probability of non-restorable traffic from s to t, and c_j is 0.5 or 1 based on whether one sequence of dual failure affects the availability of the connection. Once the equivalent unavailability for the spans are obtained, connection unavailability is derived by using Equation 2.24. Based on these two equations, the authors in [65] derive closed and extended formulas with detailed analysis for SBPP under dual failure presumption.

$$U_i^* = U_i^{phy} \cdot \sum_{j \in S, j \neq i} (c_j \cdot U_j^{phy} \cdot NT_i/d_{s,t}) \qquad \textbf{(2.23)}$$

$$U_c = \sum_{i=1}^{n} U_i^* \qquad \textbf{(2.24)}$$

Since p-cycles have been less considered than the mesh protection schemes, there are rare works on availability and p-cycles [17,27,66]. In a recent work [17], unavailability of end-to-end traffic is studied in WDM mesh networks protected by p-cycles. It is shown that, to get the same level of unavailability, shorter primary paths have to be protected by longer p-cycles when compared to the p-cycles that protect the longer primary paths. The availability analysis of p-cycle protection includes four sets of spans as follows for the p-cycle x:

O_x^p: The set of on-cycle spans that are on the working path.
$O_x^{p'}$: The set of on-cycle spans that are not on the working path.
S_x^p: The set of straddling spans that are on the working path.
$S_x^{p'}$: The set of straddling spans that are not on the working path.

The sets given above are considered to draw six dual failure scenarios. Dual failures are represented by x and y. The failure scenarios are given below under six categories:

Category 1: $\{x \in O_x^p \wedge y \,\varepsilon\, O_x^{p'}\}$
Category 2: $\{x \in O_x^p \wedge y \,\varepsilon\, S_x^{p'}\}$
Category 3: $\{x \in O_x^p \wedge y \,\varepsilon\, S_x^p\}$
Category 4: $\{x \in S_x^p \wedge y \,\varepsilon\, O_x^{p'}\}$
Category 5: $\{x \in S_x^p \wedge y \,\varepsilon\, S_x^{p'}\}$
Category 6: $\{x \in S_x^p \wedge y \,\varepsilon\, S_x^p\}$

The authors calculate the unavailability for each category. Each p-cycle is considered as an independent domain so a path consisting of a number of domains has an unavailability value which is the sum of the unavailability value of each domain along the path. Based on these analysis approaches, an ILP formulation is constructed where the objective function is minimizing the total spare capacity. The ILP formulation consists of conventional p-cycle determination constraints other than the objective function and additional constraints. The additional constraints are about the unavailability calculation of the six scenarios and the unavailability calculation of the paths. In this model, there is also a limit for each path which is a constraint for the unavailability of that path to be lower than or equal to the unavailability value specified in SLA. This model introduces low- capacity redundancy and better availability values than a model that limits the length of p-cycles.

2.2.1.2 Markovian Analysis

Another availability analysis method is presented in [67] where the failure process is defined by a Markovian process. The modeling of the failures is based on the dual failure assumption. As seen in Figure 2.8, each state represents a failure state. $State-0$ represents no failure, while $state-i$ represents the failure of $link-i$, and $state-ij$ represents the failure of $link-i$ followed by the failure of $link-j$. Steady state probabilities are represented by the π symbols. When the Markovian equations are solved, the steady state probabilities, π_i and π_{ij} are obtained.

The construction of the balance equations are explained from Equation 2.25 to Equation 2.27. In the equations, λ_i represents the failure probability of $link-i$ which is specified as $1/MTTF_i$. Besides μ_i stands for the repair rate on $link-i$ which is equal to $1/MTTR_i$. In Equation 2.25, λ_T represents the total of all failure probabilities

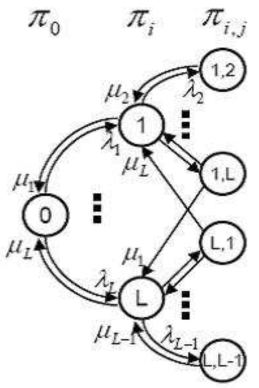


Figure 2.8: Markov modeling for state transition of network failures (Mello, 2005)

on the links in the network. Equation 2.25 stands for the probability of $link-i$ being in the failed state. Next equation (2.26) stands for the conditional probability of dual failure when $link-j$ fails following the failure of $link-j$. The last balance equation (2.27) is to confirm that the probability of the network being in any of the states is one.

$$(\lambda_T - \lambda_i + \mu_i) \cdot \pi_i \;=\; \lambda_i \cdot \pi_0 \;+\; \sum_{j=1, j\neq i}^{L} \mu_j(\pi_{i,j} + \pi_{j,i}) \tag{2.25}$$

$$\pi_{i,j} = \frac{\lambda_j}{\mu_i + \mu_j} \cdot \pi_i \tag{2.26}$$

$$\pi_0 \;+\; \sum_{i=1}^{L} \pi_i \;+\; \sum_{i=1}^{L} \sum_{j=1, j\neq i}^{L} \pi_{i,j} \;=\; 1 \tag{2.27}$$

Obviously, Equation 2.26 can directly be substituted into the equations 2.25 and 2.27. Thus, Equation 2.28 and Equation 2.29 are obtained as follows:

$$\begin{aligned}(\lambda_T - \lambda_i + \mu_i) \cdot \pi_i \;&=\; \lambda_i \cdot \pi_0 \\ &+ \sum_{j=1, j\neq i}^{L} \frac{\lambda_j \cdot \mu_j}{\mu_i + \mu_j} \cdot \pi_i + \frac{\lambda_i \cdot \mu_j}{\mu_i + \mu_j} \cdot \pi_j\end{aligned} \tag{2.28}$$

Once the linear model based on the last two balance equations is solved, steady state probabilities for single link failures (π_i) are obtained. Substituting the π_i values in Equation 2.26 gives the steady state probabilities for dual failure which is represented as $\pi_{i,j}$. Based on the steady state probabilities, availability of a connection is shown in Equation 2.30 where S_c and is the set of connections that share at least one backup resource with $connection-c$ [68]. It is clear that W_c and P_c are the working and the protection paths of $connection-c$ respectively.

$$\pi_0 + \sum_{i=1}^{L}\pi_i + \sum_{i=1}^{L}\sum_{j=1,j\neq i}^{L}\frac{\lambda_j}{\mu_i+\mu_j}\cdot\pi_i = 1 \tag{2.29}$$

$$A_c = 1 - [\sum_{k\in W_c,\ l\in P_c}\pi_{k,l} + \sum_{k\in W_c,\ l\in(P_c\cup S_c)}\pi_{l,k}] \tag{2.30}$$

When connections arrive with differentiated availability requirements, if the availability requirement of a connection can be met by the working path, the connection can be provisioned as unprotected. In this case, the availability estimation changes. As seen in Equation 2.31, an unprotected connection is unavailable if one of the following three conditions hold:

1) One link in its working path fails (first summation term),

2) Dual failure occurs where one of the failures belongs to the connection's working path (second summation term),

3) Dual failure occurs where both of the failures are from the connection's working path (third summation).

$$A_c = 1 - [\sum_{k\in W_c}\pi_k + \sum_{k\in W_c,\ l\in(\overline{W_c})}(\pi_{l,k}+\pi_{k,l}) + \sum_{k,l\in W_c,k\neq l}\pi_k, l] \tag{2.31}$$

In our work, to keep it simple, under non-differentiated availability conditions, we use the availability analysis formula in Equation 2.20. However, in differentiated availability case, the connections arrive with different availability requirements. Therefore, we have to assume more than one failure in the network for a connection to survive so we use the Markovian analysis approach. Since there is no specific availability analysis for overlapping shared segment protection, we propose our own availability analysis method and verify it.

2.2.2 Connection Provisioning and Availability in Optical WDM Networks

Recently, in [11, 69], an availability design scheme is proposed for dedicated and shared protection schemes. The proposed availability design scheme consists of two steps. The first step is *maximum connection availability design* (*MCAD*). In this step, capacity allocation is performed for each connection demand. The second step is *availability – constrained physical resources optimization* (*ACPRO*). *MCAD* starts with an empty network with an infinite number of available fibers. Therefore there is not a physical resource constraint. *MCAD* and *ACPRO* are both designed to work with DPP ($MCAD-DPP$) and SBPP ($MCAD-SBPP$).

$MCAD-DPP$, begins with routing and fiber and wavelength assignment (RFWA) as the resource allocation. However, the topology is represented as a multi-layered graph, such that there exists one arc per WDM channel and W WDM channels are grouped to represent a fiber. The weight of each arc is assigned to the "unavailability (U)" value of the corresponding WDM channel. Then, the DPP connection forms a parallel system with two paths, namely the working path and the protection path with the unavailability values of U_w and U_p respectively. Thus, the unavailability of the DPP connection becomes; $U_c = U_w \cdot U_p$. The problem is reduced to finding a cycle that minimizes U_c in the idle part of the multi-layered graph. First, two-step Dijkstra's algorithm is run to find two link-disjoint paths with the least cost. Then, a set of two link-disjoint paths that satisfies min $\{U_w + U_p\}$ is searched within one step by using the Bhandari's algorithm [70]. The details of the Bhandari's algorithm is given in Appendix-A. The one that leads to the minimum U_c value is selected among the one-step and two-step approaches. Once, all connection demands are provided physical resources, empty fibers are removed from the multi-layered graph.

For the SBPP case, MCAD-SBPP uses a heuristic approach by starting with an idle network and infinite number of physical resources. For each connection request, a working path w_c, is found by applying Dijkstra on the multi-layered graph where the link weights are the WDM channel unavailability values. The connections whose working paths share at least one link with w_c is collected in a list $Y(c)$. The links of w are removed from the multi-layered graph, and a protection path p_c that share no links with the protection paths of the connections in $Y(c)$ is searched. When all the connections are provided physical resources, the empty fibers are removed from the multi-layered graph.

The second step of the availability design (*ACPRO*) covers the resource optimization process based on availability constraint. *ACPRO* is transparent to the protection mechanism employed. The input of *ACPRO* is the output of *MCAD* and a margin value, M which stands for the tolerance rate that the unavailability value of a connection provided by *MCAD* must stay in. After completing the greedy step for resource allocation maximizing the connection availability for each connection request, the fibers are ordered based on the number of wavelengths that are utilized on them. Starting from the least utilized fiber, each fiber is probed once by releasing the connections that pass through it. An alternative routing and fiber and wavelength assignment (RFWA) is searched for each connection. If each released connection can be assigned to a RFWA that leads to an unavailability value which does not exceed the former unavailability with a tolerance factor M, the new configurations are accepted and the empty fibers are removed. The algorithm is given in Appendix-B.

A detailed comparative study for DPP-based availability aware connection provisioning schemes can be found in a recent work in [71].

$CAFES$ $(Compute-A-Feasible-Solution)$ is proposed for connection provisioning in dynamic traffic environment [62]. The input of $CAFES$ is a directed graph such that $G = \{V,\ E,\ C,\ \lambda\}$, the set of vertices $v = \{v_e \mid e \in E\}$, source and destination nodes s, d, and an integer K which stands for the number of alternate path pairs. The algorithm computes the set of K minimal cost paths from s to d; $k \in \{1...K\}$. For each k^{th} trial, the algorithm keeps l_w^k as the working path obtained from the k^{th} minimal cost path. For each of these working paths, a minimal cost backup path is computed as shown in Equation 2.32.

$$C_b(e) = \left\{ \begin{array}{cc} \infty & if\ e \in\ l_w^k \vee\ (\lambda_f^e = 0 \wedge (\exists e' \in l_w, v_e^{e'} = v_e^*)) \\ \varepsilon * C(e) & if\ \forall e' \in l_w, v_e^{e'} < v_e^* \\ C(e) & otherwise \end{array} \right\} \qquad \textbf{(2.32)}$$

In the equation above, λ_f^e is the residual capacity on $link\ e$ in terms of wavelength channels. $C(e)$ is the actual cost of the $link\ e$. ε is a significantly small number close to zero that is multiplied with the cost of the link, if the link is shareable by the connection request from s to d. This operation forces the channel to be shared by the incoming connection. The terms $v_e^{e'}$ and v_e^* are explained by the concept of $conflict\ set$. v_e is the conflict set for $link\ e$. The elements of v_e are the subsets shown as $v_e^{e'}$. Each subset $v_e^{e'}$ stands for the number of working paths utilizing $link\ e'$ that use $link\ e$ as a backup resource. v_e^* is the star closure of v_e, and stands for the maximum number of backup bandwidth (wavelengths) that has to be reserved on $link\ e$ to protect the connections that refer to the conflict set. Upon computing the $k-path$ pairs for the $connection\ c$, the pair that least to minimal total cost is selected, such that $min\{W_c^k + P_c^k\}$.

The link costs may be assigned either to the unavailability value of a single WDM channel on the corresponding link or to the negated logarithm value of a single WDM channel on the link. Negative logarithm approach uses multiplication-to-summation (MTS) technique which is employed by several studies [18, 55, 62]. Equation 2.33 shows the idea behind multiplication-to-summation. Unavailability, which is one's complement of the availability, is additive therefore minimum cost leads to the minimum total value of unavailability values on the links [11,69]. In all of the schemes in this study, we select the working/backup path pair with the least unavailability which is practical and easy to implement.

$$
\begin{aligned}
A_s &= \prod_{i=1}^{n} a_i = a_1 \cdot a_2 \cdot .... \cdot a_n \\
&-logA_s = -log(\prod_{i=1}^{n} a_i) = -(\sum_{i=1}^{n} log(a_i)) = -(log(a_1) + log(a_2) + \\
&.... + log(a_n))
\end{aligned}
\qquad \textbf{(2.33)}
$$

In [62], the authors show that $k = 2$ and $k = 3$ gives the best performance in terms of resource overbuild and blocking probability when the connections arrive with differentiated availability requirements. Therefore in our work, we take $CAFES - k = 3$ as the basis for the proposed provisioning schemes. The backup path search is the same for each candidate working path. However, the working paths are selected as follows:

- w_c^1: Maximum reliable path (*MRP*) where the unavailability values of the WDM channels are used as the link weights
- w_c^2: Maximum reliable path where the link with the minimum unavailability in w_c^1 is deleted from the graph
- w_c^3: Shortest path based on the hop count

In [55], Availability Guaranteed Service Differentiated Provisioning (*AGSDP*) algorithm is proposed to enhance the performance of CAFES. AGSDP consists of five steps before provisioning the connection: 1) Compute the MRP and assign it as the working path of the connection. Compute the availability of MRP. If $A_{MRP} \geqslant A_{SLA}$, set up the connection unprotected. 2) If connection cannot be provisioned unprotected, search for a backup path by using Equation 2.34. The first line in the equation corresponds to the links in the conflict set. The second line forces the connections to share wavelengths by considering the backup utilization of the link where α_e stands for the ratio of the sharing connections to the utilized backup wavelengths on $link\ e$. The third line corresponds to the condition where a new backup channel has to be added for the connection on $link\ e$. Thus, β_e is an updated ratio of α_e. 3) Compute the availability of the connection considering the working/backup paths. If it is not less than the availability requirement, set up the connection. 4) If the availability of the shared backup protected connection does not meet the availability requirement, an idle wavelength is reserved on $link\ e$ so the connection is provisioned by DPP. 5)Calculate the availability of the conenctions traversing $link\ e$ as a backup link. If the availability of any of them is violated, then go back to the previous step.

$$C_b(e) = \left\{ \begin{array}{cc} \infty & if\ e \in\ l_w^k \vee\ (\lambda_f^e = 0 \wedge (\exists e' \in l_w, v_e^{e'} = v_e^*)) \\ \varepsilon \cdot \alpha_e \cdot (-log\ a_e) & shareable\ backup\ wavelength\ pool \\ 1 + \varepsilon \cdot \beta_e \cdot ((-log\ a_e)) & otherwise \end{array} \right\} \tag{2.34}$$

AGSDP is shown to outperform *CAFES* in terms of resource overbuild and availability satisfaction. However, it can perform better than *CAFES* only under light load levels, and it leads to higher blocking probability under moderate and heavy loads due to the tradeoff between resource consumption and availability satisfaction [55].

Holding Time-aware AGSDP ($HT - AGSDP$) is proposed as an adaptation of the fundamental holding time-aware routing scheme, *PHOTO* [72] into AGSDP in [22]. *PHOTO* is based on the assumption that the holding time for each connection request is known at the time of arrival. Upon a connection setup request, working path is searched by using the same strategy in CAFES. However, backup path search considers connection holding times to utilize the shared backup resources more. For each link, each time a link state changes, it updates the offset time (Δ_{τ_k}) between two consecutive link state changes. Here, since a separate link cost is calculated at each time interval, the terms related to the conflict set ($v_e^{e'}$ and v_e^*) are kept per interval such as $v_e^{e'}(\Delta_{\tau_k})$ and $v_e^*(\Delta_{\tau_k})$. At each time interval (link state update Δ_{τ_k}), the link cost is calculated as seen in Equation 2.35. Thus if there is a shareable wavelength on the link during the corresponding interval, the link cost is multiplied by a negligible value ε, otherwise it is kept as it is. For the whole holding time of the connection, each separate cost value is summed and normalized with the total holding time of the connection as seen in

Equation 2.36 where m and t_h are the total number of link state updates (intervals) and the holding time of the connection respectively.

$$C_b(e,\Delta_{\tau_k}) = \left\{ \begin{array}{cc} \infty & if\ e \in\ l_w^k \vee\ (\lambda_f^e = 0 \wedge (\exists e' \in l_w, v_e^{e'}(\Delta_{\tau_k}) = v_e^*(\Delta_{\tau_k}))) \\ \varepsilon \cdot C(e) & shareable\ backup\ wavelength\ pool \\ C(e) & otherwise \end{array} \right\} \quad \textbf{(2.35)}$$

$$C_b(e) = \frac{1}{t_h} \cdot \sum_{k=1}^{m} (\Delta_{\tau_k}) \cdot C_b(e,\Delta_{\tau_k}) \quad \textbf{(2.36)}$$

HT-AGSDP uses the AGSDP algorithm for connection provisioning, but uses cost assignment approach of PHOTO when searching for a backup path for an incoming connection. Thus, the link costs are assigned the availability values of the links and when running the shortest path algorithm, MTS is employed to make the availability values additive as shown in Equation 2.33. The idea behind the holding time-aware schemes is forcing a connection to utilize the shared backup channels that are more utilized during its holding time. The normalization in the Equation 2.36 is explained as follows: As the connection approaches to be permanent, its holding time approaches to infinity. Therefore link costs are not differentiated in that case. PHOTO and HT-AGSDP aims to decrease the resource overbuild when compared to CAFES and AGSDP respectively [22, 72]. In another similar recent work [73], remaining holding time awareness and failure tracks of the connections are used to re-define the SLA requirements of the existing connections to increase the acceptance rate for the future requests.

Another time-aware similar approach for availability-guarantee is also proposed recently in [74]. The proposed scheme uses the fact that the connection's availability requirement varies with its SLA requirement during the holding time. It dynamically adds and releases the backup paths based on the change in the availability requirement of the connection during the holding time.

In [75], the authors propose a heuristic for SLA-constrained sharing. The proposed heuristic algorithm is tested under several provisioning strategies defined in [76] such as most reliable working/backup pair, the working/backup pair that leads to an availability just above a threshold value, the route pair with minimal cost, and iteratively selecting and replacing a route pair among the demands pool. The provisioning strategies set up the connections either as unprotected or by DPP. Upon running each tested provisioning scheme, backup lightpath modification is done based on the proposed algorithm called SLA-Constrained Sharing Algorithm (*SCSA*). The algorithm consists of two main steps: 1) Starting from the lowest number, for each wavelength w on each backup link e, check if wavelength w is shareable by the incoming connection considering the SRLG constraints. If the wavelength is shareable, compute the new availability values for the connections that are protected by the corresponding wavelength. If the availability requirement of any connection is violated, proceed with the next wavelength. 2) If the corresponding wavelength is shareable and it does not lead to any availability violation for the other connections, release the dedicated channel for the connection and assign $wavelength\ w$ as the backup resource for it on $link\ e$. If the connection cannot be assigned on any of the shared wavelengths on $link\ e$, it is left as dedicated protected on the related link.

In [46], a network availability algorithm that considers the network performance is proposed. A new network performance metric (P) is proposed as a function of accepted rate (R) and availability for the incoming requests (A) as follows: $P = R \cdot A$. If the network offers high availability, more resources are required to be allocated to protect the connection, then this leads to high blocking probability. On the other hand, if the network offers low availability, protection can be achieved by fewer backup resources, then the blocking probability will be low. Therefore, in the proposed network availability algorithm, network availability is dynamically modified to force the network performance converge to its best value.

The algorithm works as follows: If the performance value is greater than the last one, the availability offered to the connection requests is modified with the same trend as the last change. Thus, if the last trend was increase, the availability offered is increased, otherwise it is decreased. If the performance value is less than the last one, the availability offered is modified with the reverse of the last trend. This means that the availability is increased if the last trend is decrease, it is decreased if the last trend was increase. The availability adjustment for increase and decrease is given in Equation 2.37. It is also guaranteed that if the availability offered is increased, it does not exceed 1. If A is decreased, according to Equation 2.37, it can get a negative value. Therefore decrease operation can be done if current value of the availability offered is equal to or greater than 0.5. In the equation, N is a big number to decrease the second term to a significantly small number.

$$A^{+} = A \mp \frac{1-A}{N} \tag{2.37}$$

The performance aware network availability algorithm is designed to work with SBPP. The availability of a connection (A_k) is calculated based on the formula in Equation 2.10. If $A_k > A$, the connection request is accepted and the working / backup path pair is assigned to the connection. It should be noted that, if the working path itself, provides the required availability degree, there is no need to search for a protection path. Routing is based on Dijkstra's shortest path algorithm. However, when calculating the working path (W_k), link costs are assigned to links by taking the logarithm of the link availability values. If the set of free wavelengths on a $link\ e$ (λ_f^e) is empty, the cost of this link is assigned to infinity. When calculating the protection path ($P2$), another parameter which is the link-disjoint degree of the primary and the backup paths, ξ, is used to determine the link costs. As it is seen in Eq.2.38, when ξ is small, it is more likely to find a link-disjoint pair for the primary and the protection paths.

$$C_b(e) = \left\{ \begin{array}{cc} -ln(\xi \cdot a_e) & (i,j) \in W_k \\ -ln\ a_e & \lambda_f^{W_k \not\ni e} \neq \varnothing \\ \infty & \lambda_f^{W_k \not\ni e} = \varnothing \end{array} \right\} \tag{2.38}$$

In [58], three routing schemes are proposed that use failure information. Failure Independent Routing (FIR), creates a generic view of the network, and partitions the topology into bi-connected components. For each bi-connected component, disjoint working and backup paths are calculated based on Dijkstra's algorithm with minimum hop count constraint. These disjoint segments are then connected to form the working and backup paths between source and destination. Failure Driven Routing (FDR) constructs the network view by using the span failure state. Therefore, the connection requests are routed over working spans. In Failure-Aware Diverse routing, working path is constructed by considering the span failures. However, backup paths are allowed to be selected by considering the failure impacted spans. Since the probability of multiple (more than 2) simultaneous failures is significantly low [77], it is assumed that the backup path can be repaired until a possible failure of the working path so the connection can still be available.

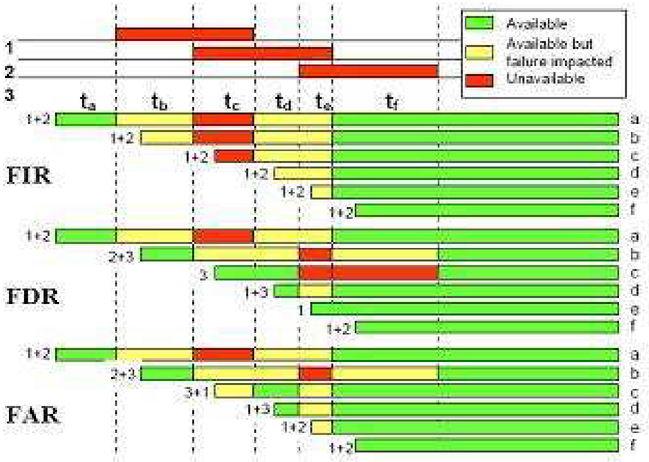


Figure 2.9: Error patterns for failure independent, failure driven, and failure aware routing (Velasco, 2006)

In Figure 2.9, the behavior of these 3 techniques is illustrated. There are three routes (1-3) to be assigned to incoming connection requests, and six connection requests ($a - f$). At time t_a, all of the three paths are available so each policy assigns $route - 1$ as the primary path, $route - 2$ as the backup path. At time t_b, $route - 1$ experiences a span failure, for all of the scenarios (routing schemes), *connection a* is still available but it is failure impacted. At this time interval, if another connection request (*connection b*) arrives, FIR assigns $1 - 2$ since it routes the requests independent of the failure state; FDR routes *connection b* over $route - 2$ and $route - 3$. FAR has to select an available primary path so it routes the request over $route - 2$; it selects the failed path as the backup route unless an available disjoint path is found. Here, $route - 3$ is available therefore FAR selects $route - 3$ as the backup path. At t_c, $route - 2$ also fails and $route - 1$ is expected to be repaired at the end of this timeslot. A new connection request arrives as *connection c*. Since FIR always selects $route - 1$ and $route - 2$ independent of the failure state, *connection c* is unavailable if it is routed based on FIR. FDR attempts to route the primary and the backup path over working paths. Therefore, since $route - 1$ and $route - 2$ are failure impacted, it routes the incoming connection request over $route - 3$. FAR behaves as a compromise between the former routing schemes. Thus, it selects the available route, $route - 3$ as the primary path and $route - 1$ as the backup path. At the end of this time period, $route - 1$ will also be repaired and the connection will be fully available. As it is seen in the figure, the unavailability pattern of the incoming connections are minimum when they are routed based on FAR. The authors show that, as the holding time increases, FAR and FDR outperforms FIR.

However, for holding times varying from 8 hours to 365 days, FAR leads to higher availability of the connections. On the other hand, FDR and FAR schemes increase the blocking probability significantly when compared to FIR, since FIR does not consider the failure state to setup a connection [58]. This routing scheme also can be designed for circuit switched WDM networks where wavelength continuity constraint holds.

There are also distributed approaches for availability-constrained connection provisioning. In [78, 79], a link and resource availability (*LRA*) based connection provisioning algorithm is proposed to work with SBPP. The proposed scheme is not completely distributed but it employs a distributed link-state database in order to inform the nodes on the failure characteristics of the other network components. All nodes are assumed to have wavelength conversion capability. The availability of the links is calculated by deriving a simple graph from the physical configuration of a logical link. Physical link configuration graph (*PLG*) and simplified *PLG* are shown for a simple case in Figure 2.10 where a physical link between two nodes is represented by a simplified *PLG*. In the simplified *PLG*, each physical component is represented as a single component node. The relative positions of the components in the *PLG* have to be the same in the simplified *PLG*. If one or more wavelength channels go through two adjacent component nodes, they are connected by an undirected line, and the lines are tagged with the WDM channel IDs.

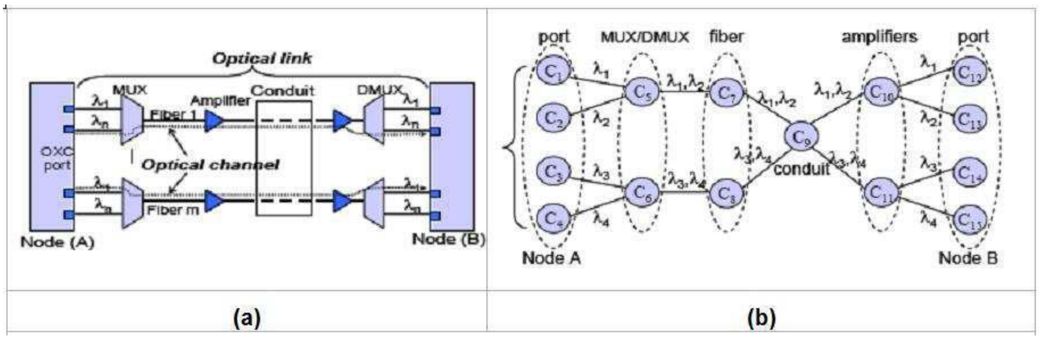


Figure 2.10: Physical link configuration graph and simplified PLG for link and resource availability calculation (Huang, 2004)

To compute the availability parameter of a link (LRA), simplified *PLG* has to be decomposed to consist of *m* independent simple graphs. Decomposition starts with selecting the node with the highest connectivity (C_i). C_i's transparent and C_i's complement *PLGs* are constructed. As a simple example, we consider the simplified PLG in Figure 2.10.b. In the figure, *C*9 is expected to be selected. In order to obtain the transparent graph of $C9$, the component nodes that are connected to the inlets and outlets of $C9$ are to be connected by a directed line that is tagged by the indices of the WDM channels $\lambda_1\lambda_2$ and $\lambda_3\lambda_4$ respectively. In the transparent graph of $C9$, PLG is separated into two distinct graphs. The decomposition goes unless the transparent or complement PLGs of C_i is a simple graph. When PLG decomposition is complete, the LRA parameters of the simple graphs are computed by using the availability values of each component. Hence, LRA value of each link is calculated recursively as given in Equation 2.39, where α_i is the availability value of the i^{th} component.

$$\begin{aligned} &LRA\{PLG^N(C=C_1,...C_N)\} = \\ &\alpha_i \cdot LRA\{LRA\{PLG_t^{n-1}(C=C_1,....C_{N-1})\}\}+ \\ &\quad (1-\alpha_i)\cdot LRA\{LRA\{PLG_c^{n-1}(C=C_1,....C_{N-1})\}\} \end{aligned} \qquad \textbf{(2.39)}$$

When a lightpath of a connection is set up or torn down, *LRA* parameters of all links along the path are updated. The channel used to set up a connection is removed from the simplified *PLG* while the released channel is added to the *PLG* when the connection is torn down. A lightpath is considered as a series of links so the availability of a lightpath is the multiple of the *LRA* values of the links along itself. If the availability requirement of a connection in the SLA is provided by only the working path, a backup path is not required. A connection's availability (A_c) is calculated by using the availability values of its working and backup paths (A_w and A_p respectively) as shown in Equation 2.40. Backup path is selected based on SBPP scheme. In , δ stands for the availability of the shared backup path in case of a multiple failure.

$$A_c = \left\{ \begin{array}{cc} A_w & c: unprotected \\ 1-(1-A_w)\cdot(1-\delta\cdot A_p) & c: working\ and\ backup\ paths \end{array} \right\} \qquad \textbf{(2.40)}$$

When a connection request arrives, the source node computes the primary path which has the maximum LRA factor. If $A_p > SLA_c$ then the connection is setup. Otherwise, a backup path is searched. Backup path search takes the following steps: 1) Compute a temporary *LRA* value, LRA_t, for each link using available resources that are free or reserved by the primary paths that are link-disjoint with the working path of $connection\ c$. 2) For each link on the working path of $connection\ c$, LRA is degraded by a fraction of β which is proportional to the channel availability on the link. Working and backup paths are preferred to be link-disjoint but they are not constrained to. 3) Find a route that has the highest LRA_t product value. If $A_c > SLA_c$, resources are allocated, and for each link in the network *LRA* parameter is updated. However, instead of removing the links that are reserved as the primary paths, *LRAs* of the links on the working path are updated by decreasing with a ratio of β. In [56], the authors propose link state availability design to work with also DPP policy.

Another distributed availability aware connection provisioning framework is recently proposed as destination routing [23, 24]. Each node in the network uses a separate database for three alternate paths to every node. Three alternate paths are selected based on the three minimum costs with respect to the value shown in Equation 2.33. Once a connection request arrives at a source node, the source node prepares and sends three probe messages through the alternate paths to the destination. An intermediate node that receives a probe message updates the message based on the utilization of the wavelengths at its output ports. Routing is done at the destination node based on the collected information from the three probe messages.

Connection provisioning takes three steps in destination routing. At the first step, the destination node tries each of the three candidate paths as the working path for the connection. If any of the paths leads to a greater or equal availability value of the SLA requirement of the arriving connection, the connection is provisioned as unprotected and the nodes from destination to the source node are informed to reconfigure their OXCs. If the first step is not successful, every path out of the three candidates is tried to be assigned as a backup path if there are shareable wavelengths along the path. Each checked path assumes that one of the other two paths will be the working path for the connection. For any working/backup path pair that can be found based on this search criteria, the availability of the connection is calculated, and compared to its SLA requirement. If the calculated availability is not less than the required availability level, the connection is provisioned. If the second step fails to provision the connection, the third step tries three alternate combination of the alternate paths and assigns idle wavelengths along the backup paths, i.e DPP. If any of the DPP solutions satisfies the availability requirement of the connection, the nodes from destination to the source are informed to reconfigure their OXCs and update their local databases.

In [80], a conservative sharing protocol and a preemptive sharing protocol for availability-aware connection provisioning are proposed. Although the schemes are initially proposed to be implemented centralized, their distributed implementations are also outlined by the authors.

Although this study focuses on WDM networks, the next step to extend the availability aware connection provisioning seems to be multi-granular optical networks and Generalized Multi-Protocol Label Switching (*GMPLS*). In [18], the authors propose an availability model for SBPP based on spare capacity availability within $partial\ protection/restorability$ concept for GMPLS networks. This concept can be explained by two different scenarios, subject to the failure pattern set R: First, the working path is partially protected by one or more backup paths where a specific set of failure patterns in R is restorable. Second, the spare capacity allocated along a backup path is a fraction of the bandwidth of the primary path. Thus, the switching node of the backup path switches the specified amount of the working bandwidth (Θ_c) and drops the rest. Four failure patterns are defined due to the effect of the failure on working or protection path and they are as follows: 1) Dual failure occurs, and both of the failures affect both of the working and backup paths where the availability impairment is 100% ($R1$), 2) Either single or dual failure occurs, and only the working path is affected where the availability impairment leads to $(1-\Theta_c)$ ($R2$), 3) Dual failure occurs, the first failure affects neither working nor backup path, but the second failure affects the working path where the availability impairment is approximately $(1-\Theta_c)$ ($R3$), 4) Dual failure occurs and none of the paths is affected where there is no impairment.

The proposed spare capacity reconfiguration model is formulated as an LP model based on failure independent ($FID-SCA$) and failure dependent ($FD-SCA$) concepts. The objective of failure independent spare capacity allocation is minimizing the total spare capacity to be allocated to satisfy the end-to-end availability of the connections. The outputs of the optimization model are the protection level for $connection\ c$ (Θ_c) and the spare capacities to be allocated on each separate link. Since only three failure patterns can affect the availability of a connection, the availability of a connection (A_c) is given by Equation 2.41 where π_r is the probability of the failure pattern r occurs.

$$A_c = 1 - \sum_{r\in R1} \pi_r - \sum_{r\in R2\cup R3} (1-\Theta_c)\cdot\pi_r \qquad \textbf{(2.41)}$$

Failure Dependent Spare Capacity Allocation ($FD-SCA$) has the same objective function with the failure independent SCA. However, Θ_c is modified $\Theta_{c,r}$ to represent the protection level of a *connection c* in case of the failure pattern r. Therefore, the outputs of the optimization model here are the protection level for *connection c* in case of the failure pattern r ($\Theta_{c,r}$) and the spare capacities to be allocated on each separate link. The availability calculation is also modified to include failure dependency as seen in Equation 2.42.

$$A_c = 1 - \sum_{r \in R1} \pi_r - \sum_{r \in R2 \cup R3} (1 - \Theta_{c,r}) \cdot \pi_r \qquad \textbf{(2.42)}$$

Reconfiguration of spare capacity allocation is employed upon the occurrence of a network event which is defined as a specific number of connection setup or release. When *connection c* arrives, its availability (A_c) is calculated by assuming 100% protection level. If it is greater than or equal to the availability requirement specified in SLA, spare capacity reconfiguration is employed. Otherwise, the connection request is blocked. Whenever a network event occurs, if the previous reconfiguration process is finished, the LP model is constructed and solved to update the spare capacities on the links. This theoretical model is validated in the related work [18]. Performance of FID-SCA and FD-SCA is compared with respect to average protection level and spare capacity saving ratio. FID-SCA provides better protection level while FD-SCA outperforms FID-SCA when they are compared with respect to spare capacity saving ratio. A similar work is also done in [81] that focuses on working and spare capacity allocation under dual failure assumption with different failure patterns.

In literature, most of the availability-aware connection provisioning schemes consider DPP and SBPP, and use linear connection availability analysis approaches. Majority of the proposed schemes are centralized rather than distributed. HT-AGSDP or SCSA provide enhancement to the conventional connection provisioning scheme CAFES. However, they do not solve the trade off between all of the performance parameters, namely resource consumption, availability and blocking probability at all load levels. For network planning phase, the two-step approach MCAD/ACPRO seems to perform well and efficient to guarantee high connection availability and degraded resource consumption. Most of the works deal with the nodes that have full wavelength conversion capability since optimal working / backup path pair search problem is shown to be NP-Complete [82]. Although it is rare today, there are some works like

FD/FID-SCA and FAR that consider connection availability GMPLS networks other than optical WDM networks.

3. AVAILABILITY - AWARE DESIGN AND CONNECTION PROVISIONING FOR NETWORK PLANNING

3.1 Network Planning Under Static Demand

In [11], the authors propose a two-step design approach for availability-constrained network planning under static traffic. This scheme is explained in detail in Chapter 2. In this work, we use this scheme as a basis for our proposed provisioning scheme. The first step is greedy, and it tries to provision maximum connection availability for each connection request. It starts with an empty and over-provisioned network. By using a multi-layered graph model, the working path of each connection is first routed over the MRP which leads to minimum unavailability where the cost at each hop is assigned to the unavailability of the corresponding wavelength channel. To find the backup path, the links of the working path are deleted while each arc related to wavelength channel is assigned a cost as shown in Equation 3.1 where U_i is the actual unavailability value of channel-i on the related link, $c(i)$ is the number of connections whose either working or backup paths pass through wavelength channel-i, w_k and p_k are the working and the backup paths of connection-k respectively.

$$C_b(i) = \left\{ \begin{array}{cc} U_i & if\ c(i) = 0 \\ 0 & if\ c(i) > 0\ \wedge \exists k, i \in p_k \\ \infty & otherwise \end{array} \right\} \qquad \textbf{(3.1)}$$

In our work, we implement this scheme as follows: Once the wavelength is assigned for each hop, their shareability is checked. If the wavelength is being used by one or more connections that are in S_c, another shareable wavelength is searched. If another shareable wavelength cannot be found on the same fiber, a new free wavelength is added. The greedy step aims to maximize the connection availability for each connection request. After this step, the fibers are ordered based on the number of wavelengths that are utilized on them. Starting from the least utilized fiber, each fiber is probed once by releasing the connections that pass through it. An alternative routing and fiber and wavelength assignment (RFWA) is searched for each connection. If each released connection can be assigned to a RFWA that leads to an unavailability value which does not exceed the former unavailability with a tolerance factor M, the new configurations are accepted and the empty fibers are removed. In this second step, to obtain better availability, we assign the backup path of the connections first to shared channels, then a posterior search is done on the assigned fiber for a free wavelength. If there is a free wavelength, the backup path of the connection is assigned to that free wavelength. It is obvious that this posteriori search in the second step will increase the utilized channels when compared to previously proposed ACPRO scheme [11], and it will also decrease unavailability. The details of this MCAD-ACPRO scheme is explained in Chapter 2 and Appendix-A.

In [11], it is assumed that the nodes are nearly-perfect hence the failures correspond to WDM channel unavailability. The unavailability of a WDM *channel i* is calculated as given in Equation 3.2 where U_{tx} is the unavailability of a transponder, a multiplexer or a booster ($U_{tx} = U_{transp} + U_{mux} + U_{booster}$); U_{rx} is the unavailability of a pre-amplifier, demultiplexer, and amplified receiver ($U_{rx} = U_{pre} + U_{demux} + U_{amp-rcv}$); U_{span} is the unavailability of the cable span; L_{span} is the distance between two neighbor amplifiers. The unavailability values used in this study are given in Table 3.1, and they are taken from [11].

$$U_i = U_{tx} + U_{rx} + [round(\frac{L}{L_{span}}) - 1] \cdot U_{span} \qquad \textbf{(3.2)}$$

3.1.1 Dynamic Sharing

In [83], we propose a connection provisioning scheme with dynamic sharing degree which is built on top of the two step provisioning approach, MCAD/ACPRO that is explained in Chapter 2. Here, we attempt to provision the arriving connection requests by arranging the sharing degree per channel dynamically. To achieve this, we define a tradeoff function T as seen in Equation 3.3 for the i^{th} arranging period where RO and U are the resource overbuild and average unavailability per connection respectively. Resource overbuild stands for the ratio between the backup channels and the working channels. As pointed in the previous studies, there exists a tradeoff between availability

Table 3.1: Component Availability Values for WDM Networks

Transmitter			
Component	**MTTF (khour)**	**MTTR (hour)**	**A**
Transponder	196	2	0.999990
Multiplexer	606	2	0.999997
Booster	211	2	0.999991
Receiver			
Component	**MTTF (khour)**	**MTTR (hour)**	**A**
Pre-amplifier	370	2	0.999995
De-multiplexer	279	2	0.999993
Amp. Receiver	210	2	0.999990
Terrestrial Link L_{span}=100 km			
Component	**MTTF (khour)**	**MTTR (hour)**	**A**
Amplifier	211	2	0.999991
Submarine Link L_{span}=57 km			
Component	**MTTF (khour)**	**MTTR (hour)**	**A**
Amplifier	$20 \cdot 10^3$	336	0.999983

and resource requirement which was stated for SBPP in [69, 84–86], and for DPP in [87].

$$T(i) = RO(i) \cdot U(i) \tag{3.3}$$

The value of this tradeoff function is to be minimized. To achieve this, we construct a function, $UpdateTradeoff()$ which runs upon n connection arrivals. The tradeoff update approach is derived from the network availability arrangement in [46]. However, we aim to arrange the shareability on the channels. We set an upper bound ($UPPERBOUND$) for the maximum sharing degree in order to avoid maximum sharing degree ($S(n)$) grow unnecessarily. In the simulations, we set this value to eight. We start the greedy provisioning step by setting $S(0)$ and $T(0)$ to four and zero respectively. In our work, we set n equal to ten. $UpdateTradeoff()$ function is shown in Appendix-C where we give information on the simulation environment.

Working path of each connection is routed over the most reliable path. For the backup path, the cost of each arc is arranged as given in Equation 3.4 where K is some large value. In our simulations, we set the value of K to 30 empirically. The reason for this modification is forcing the connections to select the less-shared backup channels among the shared ones. This enforcement causes the unavailability to decrease as expected from Equation 3.3.

$$C_b^{dynamicShare}(i) = \left\{ \begin{array}{cc} U_i & if\ c(i) = 0 \\ U_i \cdot /K & if\ c(i) > 0\ \wedge \exists k, i \in p_k \\ \infty & otherwise \end{array} \right\} \tag{3.4}$$

After provisioning all the connections with maximum connection availability design, we remove all of the empty fibers, and start the second step (resource optimization step explained in 2.2.2). We also aim to obtain a better availability in the second step by setting the unavailability tolerance to one. In the second step, for each released connection, we search the maximum reliable path as the working path. For the backup path, we employ routing on a single-layered graph. Apart from the previous approach, each arc represents the unavailability value of the one channel on the corresponding link, and the arcs that belong to the working path of that connection are temporarily disabled before searching the backup route. Whenever a backup route is found, the first free channel on the corresponding link is assigned to every hop of that route. If a new channel cannot be added, another backup channel which satisfies the shareability requirement is searched. This search operation can be completed in $O(W)$ time. The global sharing degree parameter is not modified in this step since a few RFWA configurations are expected to change. For each probed fiber, if each reconfigured connection can be offered an unavailability level equal to or less than the previous one, the reconfiguration for the RFWA of the connections are accepted.

3.1.2 Performance Evaluation

In our simulations, we use the channel availability model and the corresponding MTTF and MTTR values in Table 3.1 to obtain unavailability values for the arcs. It should also be noted that a channel failure corresponds to a link failure at the same time. Therefore a WDM channel is considered as a serial system consisting of a transmitter (t_x), a receiver (r_x), and an amplifier (amp). Then, the unavailability of the i^{th} WDM channel is calculated as given in Equation 3.2 where L_{span} is a function whose value increases with the length of the fiber and takes lower values for terrestrial links, higher values for submarine links. We assume that all nodes have wavelength conversion capability. We run our simulations for $W \in \{2,4,8,16,32\}$ where W is the number of wavelengths per fiber. We first employ the NSFNET topology consisting of all terrestrial links as seen in Figure C.2 and the static traffic demand matrix in [88] where 360 bidirectional connection demands are to be provisioned. In the figures, we illustrate the results taken for the first and second step provisioning of the dynamic sharing degree approach, and the two-step approach discussed in MCAD and ACPRO, respectively. The availability tolerance is set to one for trying to achieve better availability in the second step of provisioning. We represent the first and the second step of our proposed approach as $Dynamic-Sharing-Step-1$ and $Dynamic-Sharing-Step-2$ respectively. To interpret the results better, we also illustrate the performance of DPP by using the two-step provisioning approach in [11]. In DPP, the connections are provisioned by running Dijkstra's and Bhandari's link-disjoint path algorithms [70]. The path pair that gives the less unavailability value is selected as the working and backup path pair. In [69], it is shown that this path pair leads to the optimum value for the unavailability obtained by the link-disjoint path pairs. Therefore, also in our simulation results, DPP provides an upper bound for channel consumption and a lower bound for average unavailability per connection.

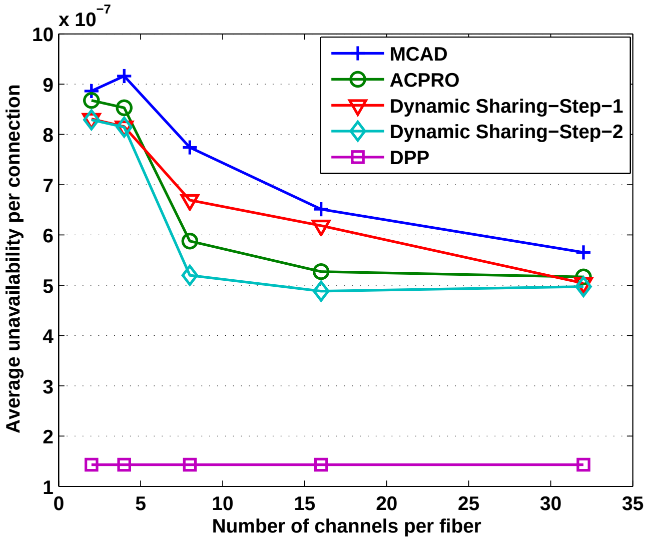


Figure 3.1: Average unavailability per connection under NSFNET

In Figure 3.1, the unavailability per connection is shown for the first and the second step of connection provisioning when different approaches are employed under the NSFNET topology. Figure 3.2 shows the total number of utilized channels by the connection provisioning approaches. To support the results in Figure 3.2, Figure 3.3 illustrates the decrease in WDM channels in terms of percentage with respect to the total WDM channels utilized by DPP. As it is seen from the figures, $Dynamic-Sharing-Step-2$ leads to a decreased unavailability due to spreading the sharing on the backup channels and forcing the connections to select backup channels that are less utilized. When the number of wavelengths per fiber is 32, the dynamic-sharing scheme has almost similar performance with the former ones because there are several free channels to use in the backup paths and the RFWA schemes start getting closer to the DDP scheme. However, the aim of decreasing unavailability with the dynamic-sharing idea increases the number of utilized channels when compared to the conventional two-step provisioning approach.

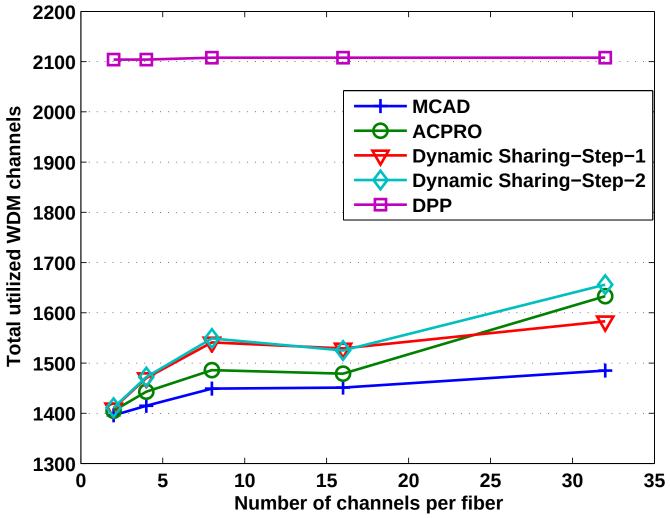


Figure 3.2: Total number of utilized WDM channels under NSFNET

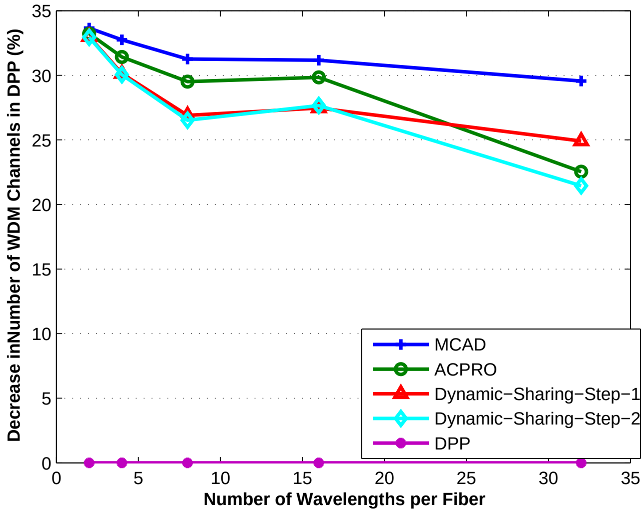


Figure 3.3: Decrease in WDM channels for DPP under NSFNET

In Figure 3.2 and Figure 3.3, it is also seen that this increase in channel consumption is not as much as the difference between the utilized channels by the SBPP provisioning schemes and DPP scheme. Therefore we can still say that the proposed scheme attempts to provide a compromise between resource consumption and connection unavailability. It is also obvious that, $Dynamic-Sharing-Step-2$ is successful since it starts with the RFWA configuration obtained by $Dynamic-Sharing-Step-1$ which provisions the arriving connections so that the average unavailability per connection is significantly decreased in comparison to the first step of the former provisioning approach.

Since the topology change may have effect on the availability performance of the network [89], We also evaluate the performance of the proposed scheme by generating five static traffic matrices in which 400 unidirectional connection demands are uniformly distributed among the nodes of 28-node EON topology in [90] which is also shown in Figure C.3. We generate five uniformly distributed demand matrices since we could not notice a realistic traffic demand matrix for this 28-node EON topology. We regard the links between Glasgow-Amsterdam, London-Dublin, London-Paris, Oslo-Copenhagen, and Rome-Athens as unidirectional submarine links for each direction. The unavailability of the WDM channels is higher in submarine links than the terrestrial links. The route selection in connection provisioning is affected by the difference between terrestrial and submarine links in terms of availability.

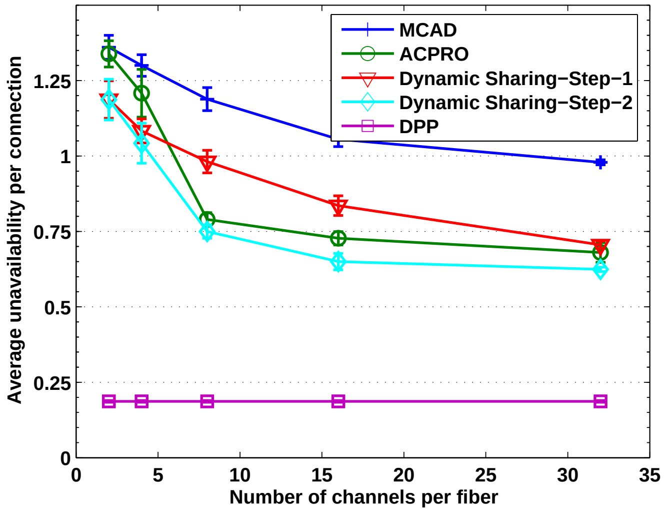


Figure 3.4: Average unavailability per connection under EON

In Figure 3.4 and Figure 3.5, we present the average of the results obtained by those five static traffic matrices and 90% confidence intervals obtained by the results. The figures show the average unavailability per connection and total utilized number of channels respectively. The average unavailability per connection increases with the

EON topology for each scheme since larger hop counts, and the effect of submarine links occur. The proposed scheme gives better performance in 28-node EON topology with a significant decrease achieved in unavailability in the first greedy step. In the second step a less decrease can be obtained in terms of unavailability but it still offers better availability to the incoming connections. The results referring to channel consumption are very similar to those obtained when NSFNET topology is employed. We can still observe that the proposed scheme does not consume as many channel as the dedicated path protection does. Figure 3.6 also supports the results in Figure 3.6 that shows the decrease in the total number of utilized channels in terms of percentage with respect to DPP.

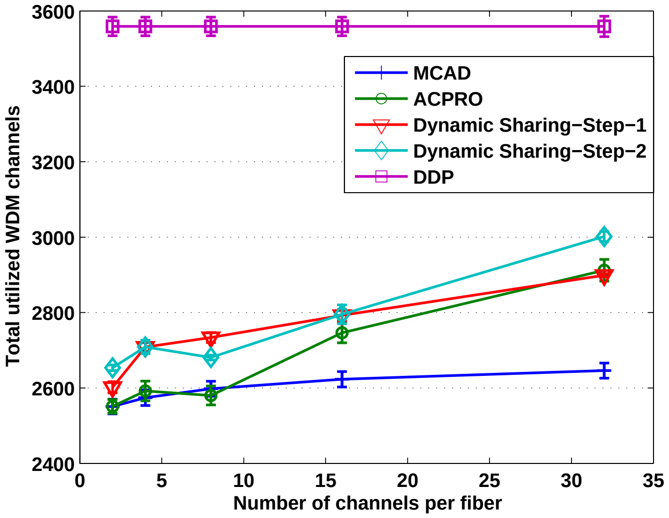


Figure 3.5: Total number of utilized WDM channels under EON

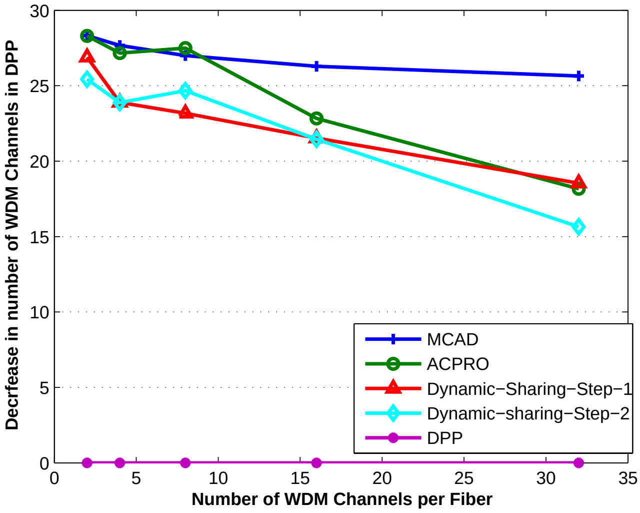


Figure 3.6: Decrease in WDM channels for DPP under EON

3.2 Network Planning Under Dynamic Demand

In this section, we focus on dynamic traffic environment, and propose two connection provisioning algorithms that attempt to offer better availability to the connection requests while keeping the resource overbuild in a feasible range [91]. The first provisioning approach is based on a heuristic. It modifies the feasible sharing degree for the links based on the current average unavailability and resource overbuild. The second scheme is based on an ILP model where each link is determined to have a feasible sharing degree for the channels in it. We evaluate our provisioning schemes under dynamic traffic. The simulation results under 14-node NSFNET and 28-node EON topologies show that the proposed schemes improve the performance of conventional availability aware provisioning scheme CAFES, without violating the resource overbuild of shared backup path protection. The simulation results that belong to the ILP model show that, the optimized performance to solve the tradeoff between availability and resource overbuild is obtained when maximum sharing degree mostly takes values of two and three. In Section 2.2.2 we present a conventional connection provisioning approach, namely Compute-a-Feasible-solution (CAFES). In this section, in 3.2.1 and 3.2.2, we present our proposed connection provisioning schemes, namely Global Shareability Surveillance (GSS) and Link-By-Link Shareability Surveillance (LSS). In 3.2.3, we evaluate the performance of the these schemes with respect to average connection availability and resource overbuild, and compare them to CAFES.

3.2.1 Global Shareability Surveillance (GSS)

To enhance the performance of CAFES, we propose a dynamic shareability heuristic, namely $Global\ Shareability\ Surveillance\ (GSS)$ for the dynamic environment. We provision the arriving connection requests by arranging the feasible sharing degree for the channels dynamically. To achieve this, we use the trade-off function T shown in Equation 3.3 for the i^th arranging period where RO and U are the resource overbuild and average unavailability per connection respectively. Resource overbuild stands for the ratio of the backup channels to the working channels.

GSS determines a global feasible sharing degree ($SHAREABLE$) for the network by using the $UpdateTradeoff()$ function given in Appendix C. Upon arrival of each N connection requests, $UpdateTradeoff()$ function runs, and updates the average sharing degree for the network. It attempts to minimize the $T(i)$ value in Equation 3.3. Therefore, if currently calculated $T(i)$ is greater than previously calculated value, it reverses the action taken on the global sharing degree; i.e, increase global sharing degree if it was decreased in the last period and vice versa. If currently calculated $T(i)$ is less than the previously calculated value, the last action on the global sharing degree is kept; i.e decrement if it was decremented previously and vice versa. The working and backup paths are calculated the same way as described for CAFES. However, links costs are assigned as shown in Equation 3.5 where $B(\lambda_k)$ is the total number of connections sharing wavelength λ_k as a backup resource.

$$C_b(e)^{GSS} = \left\{ \begin{array}{cc} \infty & if\ e \in w_i \vee \forall w \in b(\exists conn_k | e \in b_k \wedge (\exists l | l \in w_k \wedge l \in w_i)) \\ \varepsilon \cdot C_b(e) & if\ w_i \not\supseteq e \wedge \\ & (\exists conn_j | e \in b_j \wedge (\exists \lambda_k \in e(B(\lambda_k) < SHAREABLE))) \\ C_e & otherwise \end{array} \right\} \quad \textbf{(3.5)}$$

The backup paths of the connection requests are routed over the links using the cost metric above and assigned to the wavelength that has the minimum $B(\lambda_k)$ value. If that wavelength is not shareable due to being assigned to another connection whose working path has at least one common link with $connection\ i$, a new wavelength is reserved on the link. Here, we set N to be equal to 100. By this dynamic shareability approach, we aim to spread the sharing of backup resources between the backup channels to overload a few number of backup channels.

3.2.2 Link-By-Link Shareability-Surveillance (LSS)

In order to offer better availability per connection and avoid shared-backup protection violation, we modify the GSS by adapting an ILP, and call this scheme $Link\ by\ Link\ Shareability\ Surveillance$ (LSS). Here, we assign separate sharing degrees (SD_i) for each link. We set the objective function to present the tradeoff between resource overbuild and unavailability per connection. In every M connection arrivals, the shareability arrangement algorithm takes the snapshot of the current configuration in the network. Using the current configuration, it determines the sharing degree per channel on each link.

In the ILP model, *RD* is the backup channel gain, SD_j is the sharing degree per channel on $link - j$, and U_total is the total unavailability of the active connections. Besides these, S_{AVG} is the average sharing degree for one channel per link, *C* stands for the set of currently active connections, and *B* stands for the set of backup links. The other variables used in the model are H, *A*, and $U(i)$ that represent the total backup hop counts of all active connections, average connection availability, and the unavailability of $connection\ i$ respectively.

In LSS, the tradeoff between availability and resource consumption is considered again. However, as seen in Equation 3.6, the tradeoff function is modified and called T_{LSS}. According to T_{LSS}, as the backup channel gain (*RD*) increases, the amount of backup resources to protect the connections decreases where the network tends to offer less availability per connection (*A*). On the other hand, when backup channel gain is low, more backup resources are required to protect the connections where higher availability is offered for each connection. Here, it is worth noting that the clear definition for backup channel gain is given in the explanation of the ILP model.

$$T_{LSS} = RD \cdot A \tag{3.6}$$

The tradeoff function in Equation 3.6 is non-linear. Therefore, we derive an approximation by using the previous values of *RD* and *A*, $RD'$and A' respectively. Thus, the objective function for T_{LSS} is re-defined as given in the ILP model below. Each time the ILP is executed, the *RD* and *A* values are saved to be used as $RD'$and A' in the next optimization.

As seen in the first constraint of the ILP model in Equation 3.8, *A* is calculated by taking the average of one's complement of the total unavailability (U_{total}). The total unavailability is calculated by taking the sum of all active connections' unavailability ($U(i)$). The first product of $U(i)$ is the unavailability of the working path of the connection as seen in Equation 3.9. However, to present the effect of shareability in terms of availability impairment, we increase the unavailability of each $link\ j$ along the backup path of the $connection\ i$ by the sharing degree per channel on the corresponding link (SD_j) as shown in Equation 3.10. The average sharing degree

Objective

$$minRD' \cdot A \; + \; RD \cdot A' \qquad \textbf{(3.7)}$$

Subject To

$$A = \frac{1}{|C|} \cdot (1 - U_{total}) \qquad \textbf{(3.8)}$$

$$U_{total} = \sum_{c \in C} U(c) \qquad \textbf{(3.9)}$$

$$U_c = (\sum_{i \in w_c} U_{\lambda_i}) \cdot (\sum_{j \in B_c} U_{\lambda_j} \cdot SD_j) \quad \forall c \in C \qquad \textbf{(3.10)}$$

$$S_{AVG} = \frac{\sum SD_j}{|B|} \quad \forall j \in B \qquad \textbf{(3.11)}$$

$$RD = |B| \cdot S_{AVG} \; - \; H_b \cdot C \qquad \textbf{(3.12)}$$

$$2 \leq SD_j \leq UPLIMIT \quad \forall j \in B \qquad \textbf{(3.13)}$$

$$RD \geq 0 \qquad \textbf{(3.14)}$$

(S_{AVG}) is calculated by dividing the sum of sharing degrees by the number of backup links Equation 3.11. The backup channel gain (*RD*) stands for the number of idle channels if the currently active connections were re-configured based on the SD_j values to be calculated Equation 3.12. In Equation 3.13, the sharing degrees for each link are limited by the lower bound of two and the upper bound of $UPLIMIT$ which is set to eight in this work. Equation 3.14 stands for the positivity constraint for the resource gain.

Following the arrival of *M* connections, the ILP model runs to update the sharing degrees (SD_j) of the links. For a connection, the working path is found the same as in CAFES. For the backup path, the path with the minimum cost is selected where the link costs are obtained as in Equation 3.15. The second line in the equation prevents resource overbuild due to longer path selection. The cost of the link is decreased but the amount of decrease is aimed to be kept in a feasible range.

$$C_b(e)^{LSS} = \left\{ \begin{array}{cc} \infty & if\ e \in w_i \vee \forall w \in b(\exists conn_k | e \in b_k \wedge (\exists l | l \in w_k \wedge l \in w_i)) \\ \frac{C_b(e)}{SD_e} & if\ w_i \not\supseteq e \wedge \\ & (\exists conn_j | e \in b_j \wedge (\exists \lambda_k \in e(B(\lambda_k) < SD_e))) \\ C_e & otherwise \end{array} \right\} \quad \textbf{(3.15)}$$

3.2.3 Performance Evaluation

We run our simulations by using the simulation environment developed by Visual C++ and CPLEX [92] as explained in Appendix C. We use the channel availability model and the corresponding MTTF and MTTR values in Table 3.1 to obtain the unavailability of each channel. We deploy the 14-node NSFNET topology in Figure C.2 and 28-node European Optical Network (EON) in Figure C.3. Each fiber is assumed to have 16 wavelength channels. The connections arrive with a Poisson arrival rate, λ per second. The average connection holding time (μ) is set to 1 second, to be coherent with the previous studies. To let GSS work more efficient and relaxed, we force it to update the $TRADEOFF$ value ($T(i)$) once in every hundred connection arrivals. For T_{LSS}, we update the link sharing degrees in every thousand connection arrivals. We run our simulations for 10^5 connection arrivals. $UPLIMIT$ is taken as eight to prevent unnecessary growth of sharing degree as in 3.1. We run our simulations five times for each point in the graph and present 90% confidence interval here. We compare the performance of GSS and LSS with CAFES which is a conventional reliable connection provisioning scheme in terms of average unavailability per connection and resource overbuild. Here, we use CAFES-k=3 where three different working/backup path pairs are searched and the connection is provisioned by one of those candidates.

In Figure 3.7, the average unavailability per connection offered by the network is shown under NSFNET. In the figure, *GSS* leads to a slight improvement in the performance of $CAFES$ due to spreading the resource sharing among the backup channels. On the other hand, *LSS* improves the performance of $CAFES$ significantly with lower average unavailability offering for the incoming connections. The reason of this significant improvement is closely related to using separate sharing degree for the links. The output of the optimization shows that most of the channels are forced

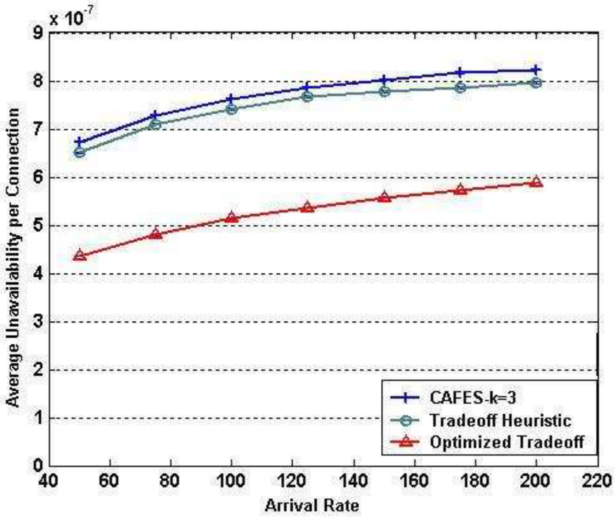


Figure 3.7: Average unavailability per connection of GSS and LSS under NSFNET

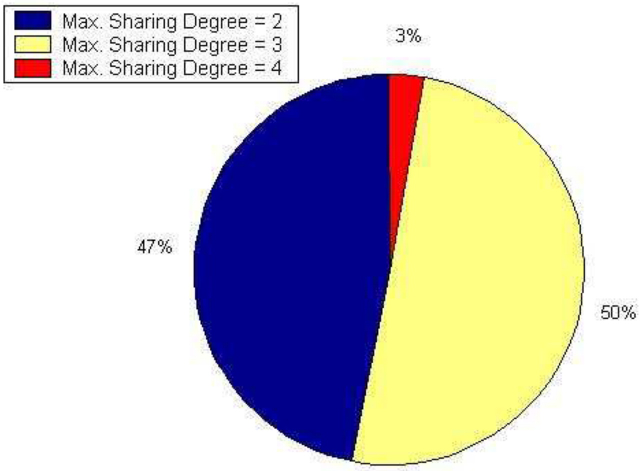


Figure 3.8: Maximum sharing degree probability with LSS at arrival rate 200

by the model to have sharing degree of two and three and a very little portion of the channels to have sharing degree of four as seen in Figure 3.8. Hence, the availability degradation due to sharing is assumed to be fair among the channels, and a lower unavailability value is obtained per connection.

In Figure 3.9, the connection provisioning schemes are compared in terms of resource overbuild. Our proposed schemes cause a slight increase in resource overbuild to offer better availability to the connections. However, it is obvious that the slight increase in the resource overbuild does not violate shared backup protection by becoming similar to the dedicated path protection. Moreover, the increase in the resource overbuild is kept in one unit of magnitude.

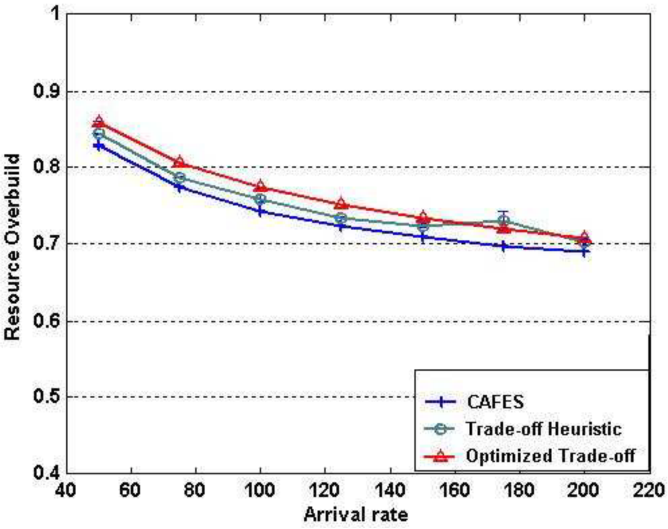


Figure 3.9: Average resource overbuild of GSS and LSS under NSFNET

We also run the same simulations under 28-node EON topology, and obtained very similar results to those taken under NSFNET in terms of average unavailability per connection and average resource overbuild respectively. As seen in Figure 3.10, LSS gives better results in terms of unavailability under EON. The result of this behavior is that a greater portion of the channels are assigned sharing degree of two when compared to the case where NSFNET topology is used. This is an expected output since the nodal degree distribution is non-uniform in the EON topology.

Figure 3.11 illustrates the comparison of the three connection provisioning schemes with respect to resource overbuild. The results are very similar to those obtained under NSFNET topology. The proposed schemes distribute sharing among the channels so

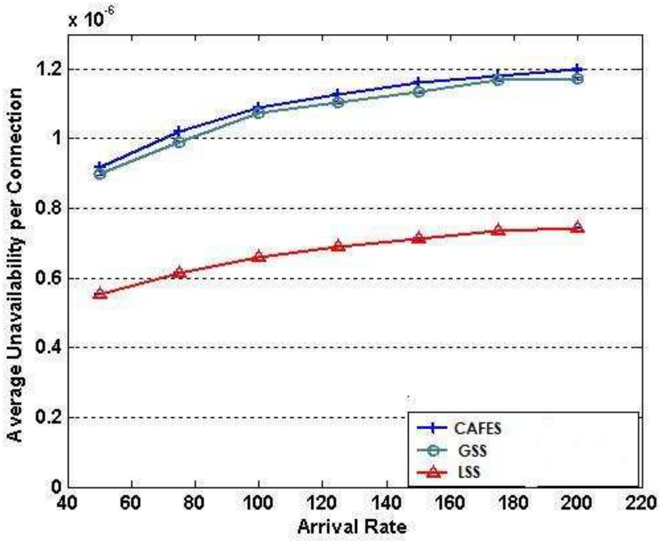


Figure 3.10: Average unavailability per connection of GSS and LSS under EON

they consume more resources compared to CAFES. However, the increase in resource overbuild is still kept within one unit of magnitude.

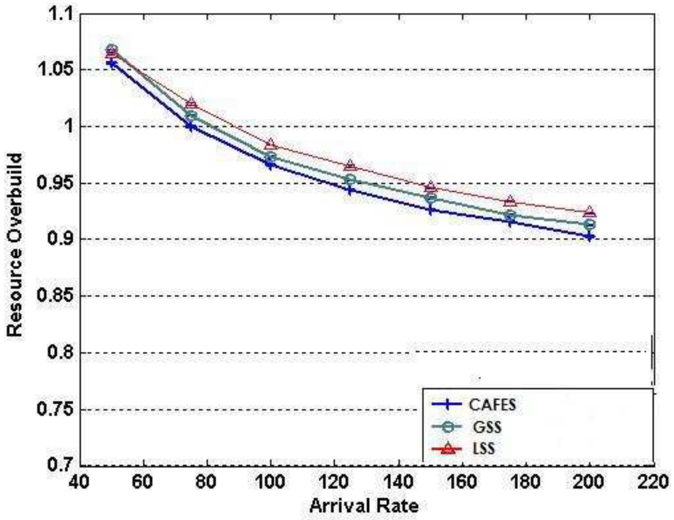


Figure 3.11: Average resource overbuild of GSS and LSS under EON

In summary, under static traffic, the simulation results show that our proposed provisioning scheme with dynamic shareability introduces a compromise between resource consumption and average unavailability per connection. On the other hand, under dynamic traffic, the trade-off heuristic (GSS) leads to a slight improvement in terms of availability while optimized sharing degree assignment (LSS) introduces a significant enhancement due to spreading the sharing fairly among the channels. We also show that, the increase in resource overbuild introduced by the proposed schemes is kept in a feasible margin at each load level.

4. DIFFERENTIATED AVAILABILITY-AWARE CONNECTION PROVISIONING

This chapter presents two adaptive differentiated availability-aware connection provisioning schemes, namely Global Differentiated Availability-Aware Provisioning (GDAP) and Link-By-Link Differentiated Availability-Aware Provisioning (LBL-DAP) in detail [93,94]. GDAP and LBL-DAP are designed to work under SBPP and differentiated availability requirements. The aim of both schemes is monitoring the status of the network and determining feasible global/local sharing degrees for the links and availability classes. G-DAP attempts to specify a global sharing degree on the links for each availability class. To achieve this target, G-DAP uses the shareability arrangement heuristic which was presented in Appendix-C. LBL-DAP is derived from G-DAP, however, it performs the status monitoring in a link-by-link manner. The output of LBL-DAP scheme contains three sets of sharing degree values where each set corresponds to an availability class. Each set keeps the sharing degree of each link for that class. LBL-DAP constructs and solves an ILP model periodically to obtain these sets. [92]

We evaluate the performance of these schemes under the 14-node NSFNET topology (Figure C.2) and the 28-node EON topology (Figure C.3) in terms of blocking probability, average unavailability per connection, average resource overbuild. We show that the proposed schemes enhance the performance of the conventional scheme, CAFES, under both topologies in terms of blocking probability and connection availability. Moreover, LBL-DAP leads to a significant enhancement in resource overbuild at each load level. G-DAP performs almost the same as CAFES under heavy loads while for the light load levels, it introduces a slight increase in resource overbuild. At the end of the chapter, we also present a comparative analysis on the protection schemes based on provisioning by giving the percentage of unprotected,dedicated, and shared connections for each scheme. Moreover, the results showing the percentage of connections blocked due to availability requirements and resource limitations are given and discussed.

4.1 Connection Availability Analysis Method Used

To guarantee that the proposed schemes are robust to dual failure, we use a matrix based availability analysis method to consider more than a single failure. In [67], the authors propose a matrix-based unavailability estimation method for SBPP. As we also explain in 2.2.1.2, the proposed method is based on a Markov-chain model and considers dual failure. Each node in the Markov-chain stands for the state of failure in the network. Thus, π_i stands for the steady-state failure probability of the $link\ i$ while π_{ij} stands for the steady-state probability for the failure of $link\ i$ followed by the failure of $link\ j$. When the Markovian equations are solved, the steady state probabilities, π_i and π_{ij} are obtained. The detailed information on the construction and solution of the Markovian equations exists in [67] and in Section 2.2.1.2. Here, we present the availability estimation formulae that are derived from the solution of this model. Based on the steady state probabilities, availability of a connection is shown in Equation 2.30.

We allow the connections that have common links in their working paths to share the backup resources unless their availability requirements are not violated. As seen in Equation 4.1, we add one more term in the parenthesis different from the work in [67] where W_{sc} is the set of working links of the connections in S_c. The terms in the parenthesis stand for the unavailability of the connection. Hence, a protected connection is unavailable due to one of the three reasons: 1) A link from its working path fails followed by the failure of a link in its backup path (1^{st} summation term), 2) A failure in its backup path or working path of any connection in S_c (2^{nd} summation term), 3) A single working link which is common with any other connection in S_c fails (3^{rd} summation term).

$$A_c = 1 - [\sum_{k \in W_c \wedge l \in B_c} \pi_{kl} + \sum_{k \in W_c, l \in (B_c \cup S_c)} \pi_{lk} + \sum_{k \in (W_c \cap W_{sc})} \pi_k] \quad \textbf{(4.1)}$$

If the availability requirement of a connection can be met by the working path, the connection does not require a backup path, thus, it can be provisioned as unprotected. In this case, the availability estimation changes. As shown in Equation 2.31, an unprotected connection is unavailable if one of the following three conditions hold:

1) Single failure occurs in the working path (first summation), 2) Dual failure occurs where one of the failed links exists in the connection's working path (second summation), 3) Dual failure occurs where both of the failed links are in the working path of the connection(third summation).

4.2 CAFES and Differentiated Availability

In [62], the conventional reliable service provisioning method, namely Compute-A-Feasible-Solution (CAFES) is presented. As explained in 2.2.2, a number of candidate path pairs are searched as the working and the backup paths. The path pair that leads to the highest availability (or lowest unavailability) is selected. The authors show that the performance with respect to resource consumption and acceptance rate does not change significantly by setting the number of candidate path pairs beyond two. Therefore, we search for three alternative working paths for the path pairs based on different criteria. Three alternative working paths are selected by the following criteria: 1) The path with the minimum cost with respect to the link cost assignment (most reliable path (MRP) in this case), 2) The path with the minimum cost after removing the link in Route-1 with the highest availability, 3) Shortest hop count. In 1 and 2, we assign channel unavailability values on the links as the link costs due to the additive property of unavailability. For backup path searching, link costs are arranged as shown in Equation 4.2 where $\lambda_s(e)$, $\lambda_f(e)$, and $C_b^{old}(e)$ are the total spare and free capacities on $link\ e$, and the link cost that is assigned while searching for a working path, respectively. It is worth noting that spare capacity stands for the wavelengths that are utilized as backup resources by the other connections while free capacity corresponds to unutilized WDM channels. $C_b^{old}(e)$ stands for the link cost used while searching the working path.

$$C_b^{new(CAFES)}(e) = \left\{ \begin{array}{cc} \infty & if\ e \in W_c \vee (\lambda_s(e) + \lambda_f(e) = 0) \\ \varepsilon \cdot C_b^{old}(e) & if\ \lambda_s(e) > 0 \\ C_b^{old}(e) & otherwise \end{array} \right\} \qquad \textbf{(4.2)}$$

In the backup path search step, the link cost is assigned to infinity due to two reasons: 1) It has neither free nor spare wavelengths, 2) It belongs to the working path of the connection. If there is a spare wavelength on the link, then its former cost is degraded by a negligible value, ε which we set to 10^{-5} in this work to force the channel to be shared by the incoming connections. If none of these two conditions holds, then the former cost value of the link is kept. To avoid increase in the resource overbuild, we stop CAFES if MRP in the working paths satisfies the SLA requirements. Thus, the connection is provisioned as unprotected.

Wavelength assignment follows the working and backup path selection. Wavelengths are selected as first-fit assignment based on the criteria of not violating the availability requirement of any active connection. If a wavelength selection without violating the availability requirements of the connections cannot be found, a free wavelength is searched on the link. If those two wavelength assignment attempts both fail, the connection is blocked. Moreover, once an RWA configuration is selected for a connection, the connection availability is re-calculated. If the calculated connection availability does not meet the availability requirement specified in the SLA, the connection is blocked. Hence, a connection can be blocked due to one of the following two reasons: 1) Resource limitation, 2) Availability requirement in the SLA.

4.3 Global Differentiated Availability-Aware Connection Provisioning (G-DAP)

In this section, we present a new availability aware connection provisioning scheme that enhances the performance of CAFES. The new provisioning scheme was first presented in [93], and it is called Global Differentiated Availability-Aware Provisioning ($G-DAP$). G-DAP can be considered as an adapted version of GSS which was presented in Chapter 3, and it works under differentiated availability requirement case. G-DAP attempts to monitor the network status, and predict a feasible sharing degree, S_k for each class on the links. Determination of the sharing degree for the k^{th} availability class is done by running a heuristic function, $UpdateTradeoffDiff()$ periodically. The heuristic is a modified version of the $UpdateTradeoff()$ heuristic which was defined in Chapter 3 and Appendix-C. The heuristic, $UpdateTradeoffDiff()$ works with different availability classes. The main input of the heuristic is the $tradeoff$ function ($T(k)^n$) for each availability class as shown in Equation 4.3 where $T(k)^n$, $RO(n-1)$, $A^k_{(n-1)}$ are the tradeoff values for the connections of $class-k$ calculated for the next (n^{th}) period, resource overbuild calculated at the end of the last period ($(n-1)^{th}$), and the average availability value for the active connections of $class-k$ at the end of the last period ($(n-1)^{th}$) respectively.

Resource overbuild (*RO*) stands for the ratio of the backup resources (channels) to the working resources (channels) in the network.

$$T(k)^n = RO_{(n-1)} \cdot (1 - A^k_{(n-1)}) \qquad \textbf{(4.3)}$$

This tradeoff function has the same aim as the tradeoff function defined for GSS. However, here the tradeoff is kept per-class basis. As the resource overbuild increases, more backup resources are utilized to protect the connections so the unavailability $(1 - A^k)$ for a class decreases, and vice versa. Hence, the so called $UpdateTradeoffDiff()$ heuristic function has to minimize this tradeoff value. A period consists of N connection arrivals as in GSS. At the end of the period, the heuristic runs. The heuristic pseudocode can be found in Appendix-C. Here, we adapt the performance maximization idea behind [46] to tradeoff minimization concept.

$UpdateTradeoffDiff()$ function runs following the arrival of every N connections. For each availability class, the heuristic calculates the corresponding tradeoff value. If the tradeoff value for the related class ($T(k)^n$) is less than the previous tradeoff value for the same class, the sharing degree for $class - k$ is updated by taking the same previous action; i.e if the previous step was decrementing, decrement sharing degree for the class, if it was incrementing, increment the sharing degree for the related class. Conversely, if the tradeoff value for the related availability class is greater than its previous value, the sharing degree for the related class is updated by taking the reverse of the previous action on it. It is worth noting that, update on S_k is limited by a value of UPLIMIT from above and by DOWNLIMIT from below. Besides this, sharing degree for an availability class S_k is not a strict sharing degree, but a determined feasible shareability value for the corresponding class.

In order to handle RWA configuration, for each link, G-DAP assigns a cost metric that corresponds to the tradeoff value on the link. The cost metric is shown in Equation 4.4 where $C^w(e)$ is the cost assigned to $link\ e$ for the working path search, A_e is the availability of one WDM channel in $link\ e$, and $\lambda_w(e)$ and $\lambda_w(e)$ are the working and the spare capacities on $link\ e$ respectively.

$$C^w(e) = \frac{\lambda_s(e) + \varepsilon}{\lambda_w(e) + \varepsilon} \cdot (1 - A_e) \qquad \textbf{(4.4)}$$

For backup RWA selection for a connection from the $availability\ class-k$, G-DAP modifies the link costs based on the sharing degree values for $class-k$ obtained from the tradeoff update heuristic as shown in Equation 4.5 where w is a wavelength channel on the $link\ e$ and $\lambda(w)$ is the number of connections that share $channel\ w$ as a backup resource. Thus, a link is removed from the topology by setting its cost to infinity if one of the following two conditions holds: 1) The link does not have any spare or free channels, 2) It is used in the working path of the connection. If the link has at least one spare channel that is shared by a number of connections less than the feasible sharing degree for the incoming connections class, the cost of the link is degraded by the sharing degree of that class to force the channel to be shared. Otherwise, the link cost is left as it is.

$$C_b^{new(G-DAP)}(e) = \left\{ \begin{array}{cc} \infty & if\ e \in W_c \vee (\lambda_s(e) + \lambda_f(e) = 0) \\ \frac{1}{S_k} \cdot C_b^{old}(e) & if\ \lambda_s(e) > 0 \wedge \exists w \in e : \lambda(w) < S_k \\ C_b^{old}(e) & otherwise \end{array} \right\} \quad \textbf{(4.5)}$$

Wavelength assignment for the backup path follows the backup route selection. On each link, spare wavelengths are sorted with respect to the $\lambda(w)$ values in increasing order. The sorted spare wavelengths set is checked starting from the least $\lambda(w)$ value in terms of availability violation. If any spare wavelength does not violate the availability requirements of the currently active connections and the incoming connection, the wavelength is reserved on that link. If none of the spare wavelengths can be reserved as the backup wavelength on that link, a free channel is tried. In case of an unsuccessful spare or free wavelength assignment on that link for the incoming connection, the attempt for the corresponding working/backup path pair is blocked. Following the blocking of the working/backup lightpath assignment attempt, the reserved backup channels in the previous hops and the RWA configuration for the corresponding working path are deallocated for the connection.

The RWA configurations for the three alternative working / backup lightpath pairs are collected. If there is no RWA configuration collected, the connection is discarded due to "resource limitation". Otherwise, another check is done on availability satisfaction. If any of the candidate lightpath pairs does not meet the availability requirement of the connection, the corresponding RWA is deallocated. After this removal process, if there is no path pair collected, the connection is blocked due to "availability requirement".

Otherwise, for each alternative pair k, a resource consumption metric (RCM_k) is calculated as seen in Equation 4.6. RCM_k is the product of the relative resource consumption calculation and the unavailability of the corresponding $connection\ c$ when k^th RWA configuration is used. The second term is seen clearly in the equation as $(1-A_{c(k)})$. The relative resource consumption calculation is the sum of working channels and the number of backup channels divided by the average actual sharing degree along the path. Since the actual average sharing degree on each link is summed and divided by the number of backup links along the path, the numerator of RCM_k has another $Hops_k^{(b)}$ as a factor which introduces a square operation on the related parameter.

$$RCM_k = [Hops_{c(k)}^{(w)} + \frac{[Hops_k^{(b)}]^2}{\sum_{e \in B_c}(\frac{1}{\lambda_s(e)} \cdot \sum_{w \in e} \lambda(w))}] \cdot (1 - A_{c(k)}) \qquad \textbf{(4.6)}$$

RCM_k is used if there are more than one working/backup lightpath candidate for the incoming connection, and the one that leads to the minimum RCM_k value is selected as the RFWA configuration for $connection\ c$. G-DAP runs in $O(W \cdot L)$ time for the link cost arrangement which is the same as in CAFES where L and W are the number links and the number of wavelengths per link, respectively. When assigning wavelengths on the selected routes, G-DAP checks each wavelength on each link. In the wavelength assignment phase, the channels are first grouped as working, spare and free channels. Hence, searching for a spare channel takes $O(W)$ time in the worst case.

4.4 Link-By-Link Differentiated Availability-Aware Connection Provisioning (LBL-DAP)

Based on the results obtained in Chapter 3 under GSS and LSS, it seems possible to adapt and modify LSS into differentiated availability-aware environment, and enhance the performance of G-DAP. For this reason, we construct a more detailed provisioning model, namely $Link-By-Link\ Differentiated\ availability-Aware\ Connection\ Provisioning\ (LBL-DAP)$ which monitors the status and adapts the sharing degrees of each availability class in link-by-link manner. Thus, in LBL-DAP, S_k is modified to represent the sharing degree for $class-k$ on the $link\ l$, and evolves to $S_k^{(l)}$. Similar to G-DAP, LBL-DAP takes the snapshot of the network, and determines these values by running an ILP model periodically. Thus, it is an enhanced version of G-DAP and an adapted version of LSS to differentiated availability-aware service provisioning. Here, we use the metric, *resource gain* that is used in LSS but here, it is modified to work under differentiated services. We define *resource gain* as the possible idle capacity gained after forming lightpaths based on the obtained $S_k^{(l)}$ values. Thus, a contradiction exists between resource gain and connection availability. Increase in resource gain leads to increase in sharing degree; high sharing degree leads to less connection availability. Resource gain concept is first defined in LSS (Chapter 3) for availability-aware network planning without availability class differentiation. The new tradeoff function for $class-k$ in LBL-DAP is constructed in terms of resource gain and availability of class-k as shown in Equation 4.7.

$$Tradeoff_{(k)}^{LBL-DAP} = RG_k \cdot A_k \tag{4.7}$$

To make the ILP model clear and explain how $S_{(l)}^{k}$ is obtained, we define below the variables and the related parameters used in the model:

RG_k:	Resource gain for $class-k$
A_c:	Availability approximation of $connection\ c$
$A^{(k)}$:	Average availability approximation for the connections in $class-k$
$S_{avg}^{(k)}$:	Average sharing degree for $class-k$
$l_c^{(k)}$:	Set of connections from $class-k$ on $link\ l$
SC_l:	Number of spare wavelengths on $link\ l$
L_b:	Set of backup links
$Hops_k$:	Total number of backup links of the connections of $class-k$
$C^{(k)}$:	Set of connections of $class-k$
$S_l^{(k)}$:	Feasible sharing degree of $class-k$ on $link\ l$
ρ_l:	Number of connections using the backup link l

The formulae between Equation 4.8 and Equation 4.16 forms the ILP model to obtain the feasible sharing degrees on each link per availability class. It is worth to note that the tradeoff function in Equation 4.7 is non-linear so it cannot be used in the ILP model as it is. Therefore, we make an approximation by differentiating the tradeoff function by using the previous values of its dependent variables resource gain and availability. The differentiated form of the tradeoff function contributes the ILP model as the objective function as seen in Equation 4.8. We use the values of the resource gain($RG_k^{'}$) and the average availability in the last period ($A^{'(k)}$) where RG_k and A_k

stand for the resource gain and the average availability for the connections of $class-k$ respectively.

The first constraint in Equation 4.9 is the calculation of availability of each $connection\ c$ from the $class-k$. As seen in the formulation, we make another approximation in the availability calculation in order to include the feasible sharing degrees on the related links. The terms after the availability (A_c) stand for the unavailability of $connection\ c$. According to the approximation, $connection\ c$ is unavailable if one of the two conditions holds: 1) A link from its working path fails followed by a backup path fail, 2)A link from the backup path fails followed by the failure of a link from the working path. However, these two conditions reflect the nature of a connection provisioned with DPP. Therefore, to include the sharing and possible unavailability property of SBPP, in the summations, we include each backup link with a contribution to the unavailability of a $connection\ c$ of $class\ k$ proportional to the sharing degree of $class\ k$ on it. The next two constraints in Equations 4.10-4.11 are straightforward that they represent the average availability (modified) per each availability class and average sharing degree per class respectively. Equation 4.12 introduces a capacity-related constraint. It guarantees that, with the obtained sharing degree $S_l^{(k)}$, the $link\ l$ is capable of handling all of the active connections of $class\ k$ that are using the channels on the link as backup resources. Resource gain for the availability $class\ k$ is defined in Equation 4.13. As seen in the formula, resource gain concept is the same as the one used in LSS with a difference of differentiated availability services support. Equation 4.14 aims to force the links with equal backup utilizations to have equal sharing degrees for each class. Equations 4.15 and Equation 4.16 stand for the boundary constraints of the model. The former bounds the sharing degrees by using $UPLIMIT$ and $DOWNLIMIT$ while the latter guarantees that the resource gain always has a non-negative value.

Since running ILP may take time until getting a feasible solution, LBL-DAP runs ILP to update the feasible sharing degrees on the links for the classes $S_l^{(k)}$ following the arrival of every N connections. The outputs of the ILP optimization model are used to update the link costs for backup route selection for the incoming connections. Working and backup lightpath search and assignment strategy is the same as in G-DAP. However, in backup route search, link costs include the feasible sharing degrees for

$$Obj.\ min\ \sum_k RG_k^{'} \cdot A^{(k)}\ +\ RG_k \cdot A^{'(k)} \quad k=1,2,3 \tag{4.8}$$

$$SubjectTo$$

$$A_c + \sum_{p\varepsilon W_c, b\varepsilon B_c} \pi_{pb} \cdot S_k^{(b)} + \sum_{p\varepsilon W_c, b\varepsilon B_c} \pi_{bp} \cdot S_k^{(b)} = 1 \forall\ c,k \mid c\varepsilon C^{(k)} \tag{4.9}$$

$$A^{(k)} = \frac{1}{|C^{(k)}|} \cdot \sum_c A_c, \quad \forall\ k \tag{4.10}$$

$$S_{avg}^{(k)} = \frac{1}{|L_b|} \cdot \sum_{l\varepsilon L_b} S_l^{(k)}, \quad \forall\ k \tag{4.11}$$

$$SC_l \cdot S_l^{(k)} \geq |l_c^{(k)}|, \quad \forall\ k \tag{4.12}$$

$$|L_b| \cdot S_{avg}^k - Hops_k \cdot |C^{(k)}| = RG_k, \qquad \forall\ k \tag{4.13}$$

$$S_l^{(k)} = S_m^{(k)}, \qquad \forall\ l, m\varepsilon L_b \mid \frac{\rho_l}{SC_l} = \frac{\rho_m}{SC_m} \tag{4.14}$$

$$DONWLIMIT \leq S_k^{(b)} \leq UPLIMIT \qquad \forall\ k,l \tag{4.15}$$

$$RG_k\ \geq\ 0, \qquad \forall\ k \tag{4.16}$$

the availability class of the incoming connections in their costs. The link costs are shown in Equation 4.17. For backup path search of an incoming connection from $class-k$, a link is temporarily removed from the physical topology by assigning its cost to infinity if one of the following two conditions holds: 1)$link\ e$ has neither free nor spare wavelengths, 2) It is used in the working path of the incoming connection. If link-e has at least one spare channel that is utilized by a number of connections less than the feasible sharing degree for the corresponding class on $link\ e$ ($S_k^{(e)}$) as a backup resource, the link is assigned the cost $\frac{1}{S_k^{(e)} \cdot \lambda_s(e)}$ where $\lambda_s(e)$ is the spare capacity on the link e. By this modification on its cost, $link\ e$ becomes preferable as a shared backup resource for the incoming connections. If this second condition does not hold, then the link cost has to be assigned a value that significantly greater than the link cost of a preferably shareable link, but significantly less than INFINITY, so it is assigned to the value of DOWNLIMIT.

LBL-DAP has similar properties with G-DAP in terms of running time. It also runs in $O(W.L)$ time for link cost assignment. Since the working and backup RWA strategy is

$$C_e^{new(LBL-DAP)} = \left\{ \begin{array}{cc} \infty & e\varepsilon\, W_c \vee\ \lambda_s(e)+\lambda_f(e)=0 \\ \frac{1}{S_k^{(e)}\cdot\lambda_s(e)} & \lambda_s(e)>0 \wedge \exists w\varepsilon e: \lambda(w) < S_k^{(e)} \\ DOWNLIMIT & else \end{array} \right\} \quad \textbf{(4.17)}$$

the same as G-DAp except the link costs, searching for a spare channel with LBL-DAP can be completed in $O(W)$ for the worst case. However, LBL-DAP introduces an overhead which comes from the ILP optimization. It runs periodically. Moreover, as we mention in the performance evaluation section, the slowest optimization phase takes at most the average holding time of one connection, and majority of the optimization runs end within few milliseconds which corresponds to one hundredth of a the average connection holding time.

4.5 Performance Evaluation

We run our simulations on a P4 with 3.00GHz CPU and 3.50GB memory space using Visual C++. The ILP model in LBL-DAP is solved by the help of CPLEX 9.0 [92]. We generate the arrival of the connection requests with respect to Poisson model, and the connection holding times are negative exponentially distributed by normalizing the average holding time to 1s. There are 16 wavelength channels on each link, and it is assumed that all the nodes have wavelength conversion capability. In the figures, we present the average of five runs with 90% confidence intervals. Our simulation results are taken under the 14-node NSFNET topology in Figure C.2 and the 28-node EON topology in Figure C.3. We warm up the network with thirty thousand connection requests and then collect the results for the next thirty thousand connection requests. The running duration for the tradeoff update heuristic in G-DAP, and the ILP model in LBL-DAP is set to the arrival of every one thousand connections. For LBL-DAP to obtain the $S_k^{(l)}$ values, the ILP runs in a few milliseconds and it is bounded by 1s which is the average connection holding time. There are five availability classes, which require availability levels of 0.98, 0.99, 0.999, 0.9999, 0.99999. We collect the results for 50000 connection arrivals after a warm up duration. To make it similar to a realistic environment, the connections are first distributed uniformly among the availability classes, and then the corresponding portions for the classes are made to be heterogeneous so that there exist less number of connections from the highest availability classes, and the majority of the connections are from the moderate availability classes. Therefore, *class* 1, *class* 2, *class* 3, *class* 4, *class* 5 form 12%, 25%, 32%, 23%, and 8% of the incoming connection requests respectively. To be able to handle these availability requests, the availability values of the fiber links are evenly distributed on the following set {0.999, 0.9999, 0.99999}. Failure rates and their corresponding 1/MTTF values are obtained from the assigned link availability values. We use the formula in Equation 1.1 to obtain these parameters.

Since we obtain similar behavior when we apply uniform incoming requests, we do not present them in these section but the results obtained under uniform connection distribution among the availability classes in Appendix-E.

4.5.1 Results Taken Under NSFNET

The first part of performance evaluation consists of the results taken under the NSFNET topology. In the NSFNET topology, we set the $MTTR$ to 12 hours [68].

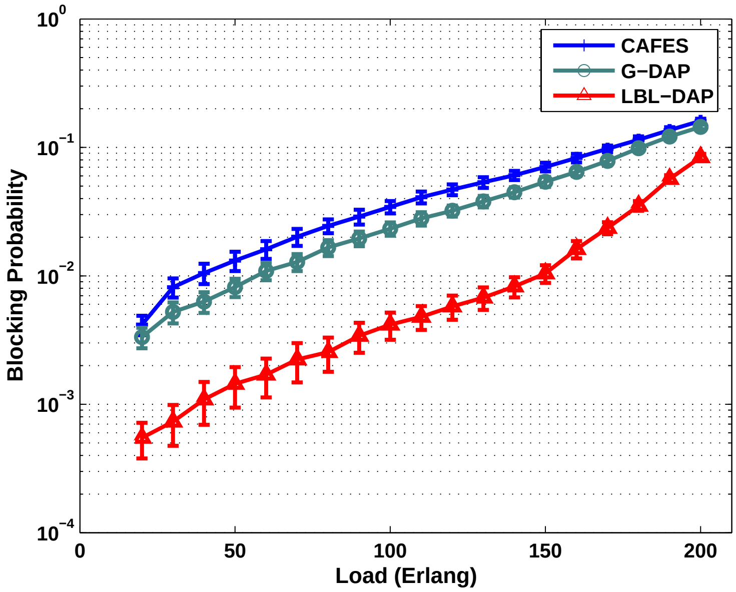


Figure 4.1: Blocking probability of LBL-DAP and G-DAP per connection under NSFNET

In Figure 4.1, the conventional availability aware connection provisioning scheme, CAFES and the adaptive differentiated availability aware connection provisioning schemes are compared in terms of connection blocking probability. The line with the highest blocking probability represents the results obtained by running CAFES. As seen from the figure, the adaptive differentiated schemes decrease the blocking probability significantly. The reason of this behavior is that G-DAP and LBL-DAP select the backup links by considering both the WDM channel availability on the links and the feasible sharing degree for the availability class of the incoming connection. Moreover, LBL-DAP considers the feasible sharing degree for the availability class of an incoming connection on each link separately. Therefore, LBL-DAP performs better than G-DAP in terms of blocking probability due to this link-by-link per-class shareability monitoring.

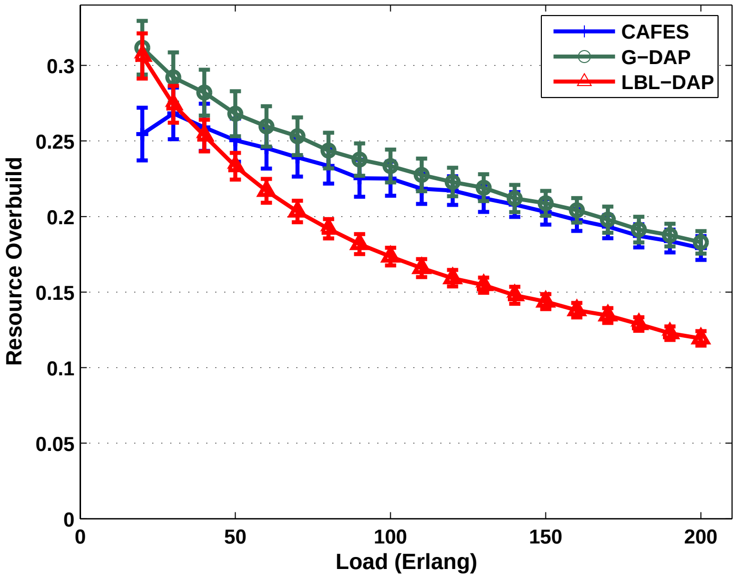


Figure 4.2: Resource overbuild with LBL-DAP and G-DAP under NSFNET

In Figure 4.2, the three techniques are compared in terms of average resource overbuild. Resource overbuild stands for the ratio of the number of backup channels to the number of working channels. In each case, resource overbuild decreases as load gets heavier. The reason of this behavior is that, as the load gets heavier, the connections tend to share the backup resources more. Although G-DAP leads to a slight increase in resource overbuild, it starts to perform almost the same as CAFES under heavy load levels. Moreover, the network experiences approximately one unit of decrease in resource overbuild when LBL-DAP is employed under light and moderate loads. Since LBL-DAP attempts to control the sharing degree for each availability class on each link separately, it achieves to control the utilization of backup resources. Using ILP also has an important effect on this achievement. Once, a feasible shareability is determined for the WDM channels on a link, the determined value is projected on the link cost for the backup search for the incoming connections. The link costs avoid selecting longer backup paths due to the decreasing the original cost at backup routing phase.

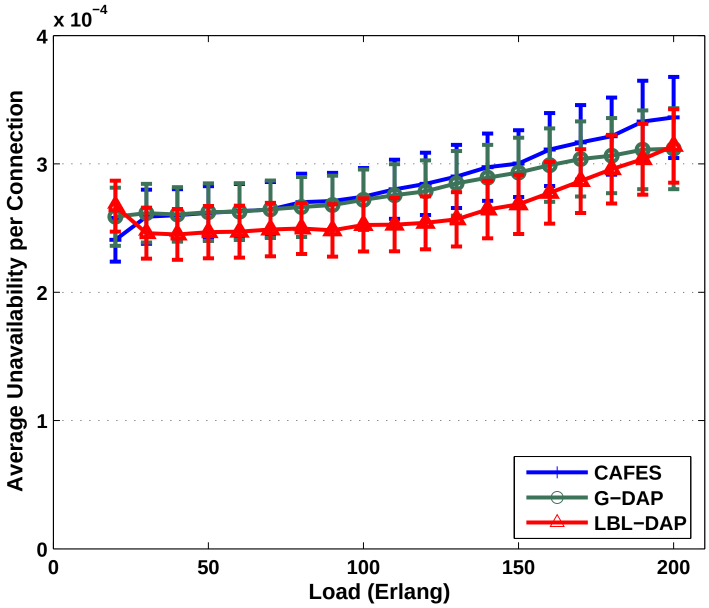


Figure 4.3: Average unavailability per connection with LBL-DAP and G-DAP under NSFNET

Although the adaptive schemes G-DAP and LBL-DAP decrease the connection blocking probability and consider resource overbuild, they do not violate the average unavailability per connection as seen in Figure 4.3. Moreover, a slight decrease is also experienced by running LBL-DAP where G-DAP also tends to decrease unavailability under heavy loads. It can be explained by the adaptive schemes' considering the tradeoff between backup resource utilization and the unavailability. Due to this consideration, while searching the backup lightpaths, G-DAP and LBL-DAP arrange the link costs by using the feasible sharing degree that is the output of an ILP model or a heuristic that uses this tradeoff. Thus, rather than creating stacks of sharing groups on the links, distributing the sharing groups in the network adaptively, keeps the unavailability per connection equal to or lower than the conventional provisioning scheme CAFES.

A connection is blocked due to one of the following two reasons : 1) Resource limitation 2) Availability dissatisfaction with respect to SLA. In Figure 4.4, we show the percentage of the blocked connections due to availability requirement. As seen in Figure 4.1, beyond the load level of 150 Erlang, blocking probability of LBL-DAP starts to increase sharply. The reason for the increase is the lack of available resources

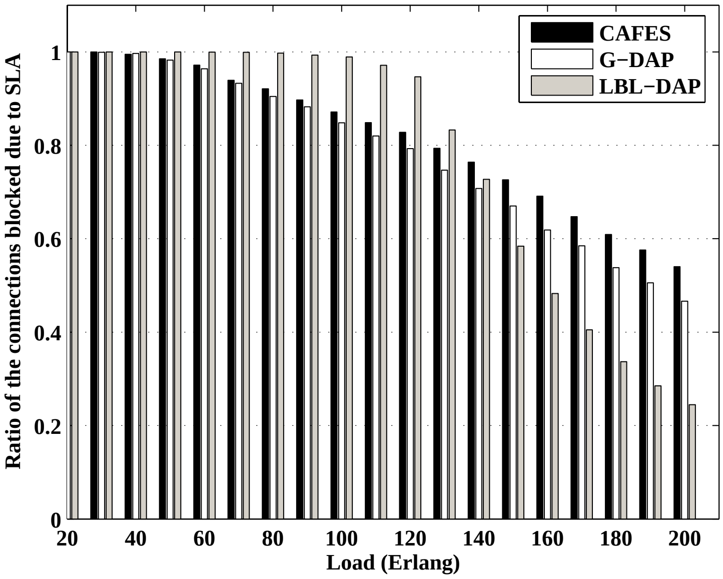


Figure 4.4: Ratio of blocked connections due to SLA requirement with LBL-DAP, G-DAP, and CAFES under NSFNET

to protect the connections. Under light and moderate load levels, LBL-DAP utilizes the resources efficiently so a greater amount of the blocked connections are dropped due to SLA requirement. Moreover, the overall blocking probability for LBL-DAP is also significantly low, and as it is seen in Figure 4.5, majority of the blocked connections are from $class-5$ which requires the highest availability level while $class-4$ and $class-3$ contribute the overall blocking probability with negligible blocking ratios. On the other hand, G-DAP blocks less amount of connections due to SLA requirement when compared to CAFES starting from 50 Erlang network load level. As seen in Figure 4.3, G-DAP introduces better availability per connection when compared to CAFES. This behavior of G-DAP causes a decrease in the amount of connections blocked due to SLA. Since $class-3$ and $class-4$ also contribute the overall blocking probability in CAFES and G-DAP, unavailability per connection can be regarded as the key factor that affects the ratio of the connections blocked due to SLA requirements.

Except the conditions where the load is so heavy that the protection resources are not sufficient, we can say that majority of the connections are blocked due to availability requirement of a connection that is specified in the SLA as seen in Figure 4.12. Indeed, the major contribution to the overall blocking probability is expected to come from the highest SLA class which is $class-5$ in this work. This situation can also be observed in Figure 4.5. The figure shows that the higher the availability requirement

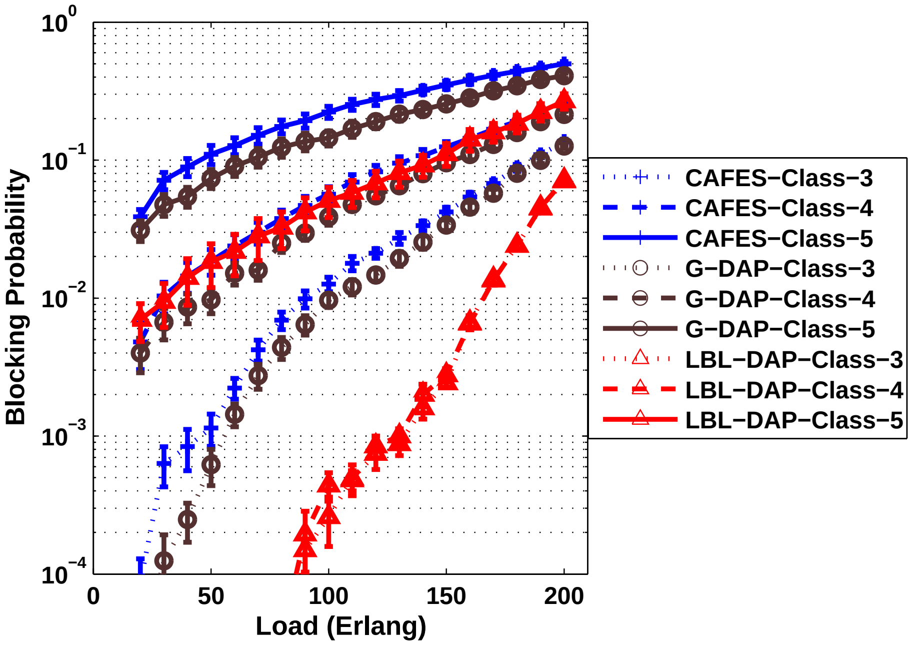


Figure 4.5: Blocking probabilities per each availability class with LBL-DAP, G-DAP, and CAFES under NSFNET

the more contribution to the blocking probability. $class-1$ and $class-2$ require the least availability levels which means provisioning by the fiber link availabilities even without protection. Therefore, blocking probability of these two classes is almost zero. For each SLA class, the proposed connection provisioning schemes lead to lower blocking probabilities when compared to CAFES. The behavior of the schemes for each class is the same as it is in overall blocking probability. The order for blocking probability among the schemes is the same as their order for the overall blocking probability. As it is stated before, blocking probability obtained by LBL-DAP for $class-3$ and $class-4$ is significantly lower than those obtained by CAFES and G-DAP. Therefore, LBL-DAP outperforms CAFES and also G-DAP in terms of overall blocking probability.

In Figure 4.6, we illustrate the distribution of the protection types at the time of provisioning for the incoming connections from $class-3$, $class-4$, and $class-5$. $class3$ requires the least availability level among these SLA classes. Since the connections from $class-3$ require less availability, their availability requirements are more likely to be met by a primary path. Thus, as seen in the figure, at least 70% of the $class-3$ connections are provisioned with only a primary path, i.e unprotected. The portions for the *class* 3 and *class* 4 connections are more under G-DAP than those

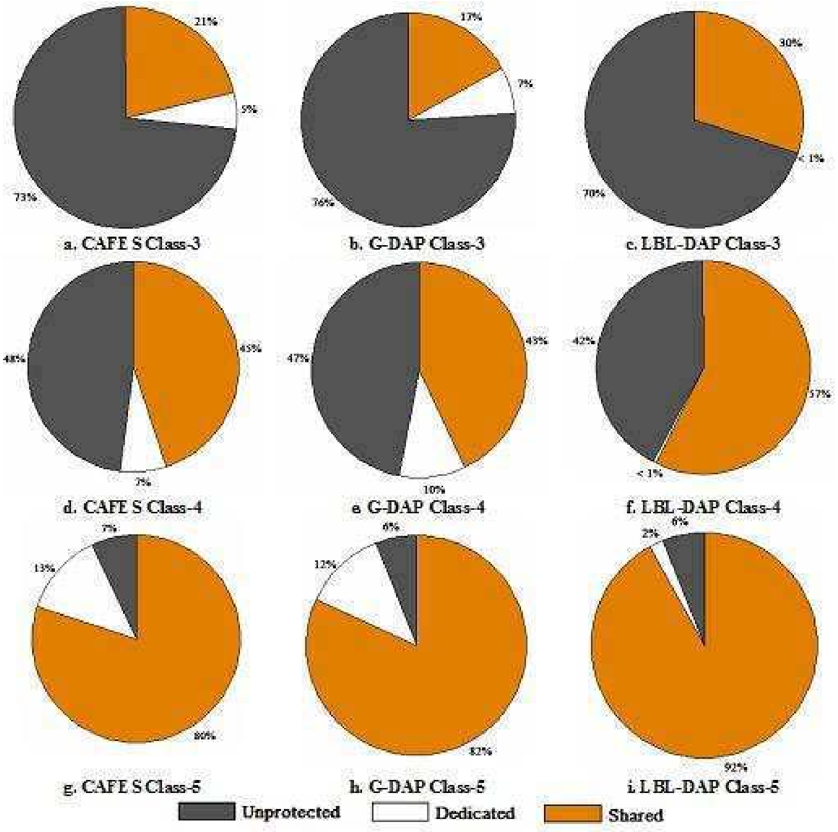

a. CAFE S Class-3
b. G-DAP Class-3
c. LBL-DAP Class-3
d. CAFE S Class-4
e G-DAP Class-4
f. LBL -DAP Class-4
g. CAFE S Class-5
h. G-DAP Class-5
i. LBL-DAP Class-5

Figure 4.6: Distribution of protection types when provisioning the connections under NSFNET

under CAFES.This introduces the slight increase in resource overbuild in Fig.4.2. On the other hand, for *class* 5 connections, G-DAP provisions less dedicated connections than CAFES does. Therefore under heavy loads its performance is close to that of CAFES in terms of resource overbuild, and the slight increase in resource overbuild under light load levels is not as significant as the decrease lead by LBL-DAP. The highest portion for the shared provisioned connections is obtained under LBL-DAP. Moreover, as an explanation to the significant decrease in resource overbuild, for each SLA class, LBL-DAP provisions less amount of dedicated connections compared to G-DAP and CAFES. For $class - 5$ connections, the amount of initially dedicated provisioned connections is 2% under LBL-DAP while this ratio is 13% and 12% under CAFES and G-DAP respectively. For instance, 92% of the $class - 5$ connections are provisioned shared by LBL-DAP, while this ratio is 80% and 81% under CAFES and G-DAP respectively. These two phenomena let LBL-DAP keep the resource overbuild below CAFES under moderate and heavy loads as shown in Figure 4.2.

4.5.2 Results Taken Under 28-node EON

The second part of our simulations are run by employing the 28-node European Optical Network (EON) topology in Figure C.3. The fiber lengths are taken as the distances between the cities. MTTR values are taken to be 20 hours. 1/MTTF values and the failure rates on the fiber links are calculated by using the same approach for NSFNET.

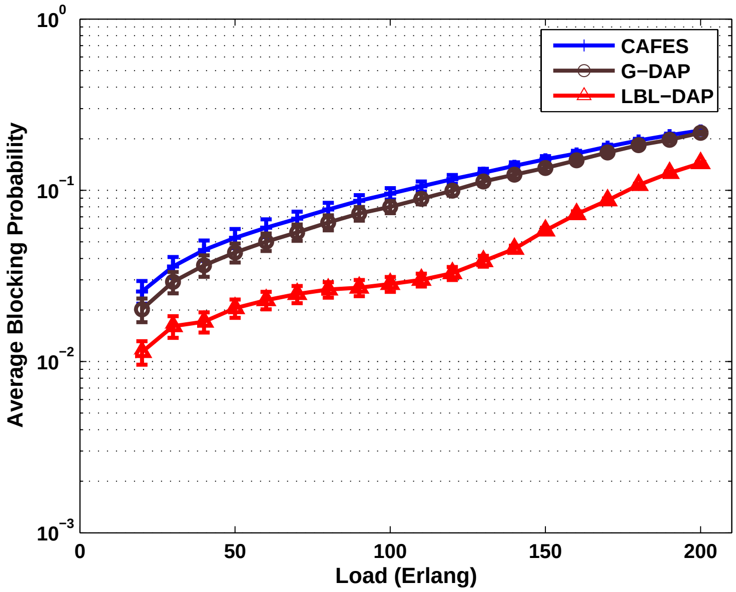


Figure 4.7: Blocking probability of LBL-DAP and G-DAP per connection under EON

In Figure 4.7, the three schemes are compared with respect to the overall connection blocking probability. Here, topology used, EON, is larger, and the nodal degree distribution is not as uniform as in NSFNET, the blocking probabilities obtained here are higher in three of the schemes. However, G-DAP and LBL-DAP still lead to an enhanced acceptance rate in comparison to the conventional reliable connection provisioning scheme CAFES. When the two adaptive schemes are compared to each other, it seems that, due to the advantage of considering the feasible sharing degrees for each class link-by-link by using the tradeoff minimization, LBL-DAP still performs better than G-DAP as under the NSFNET topology. However, the difference between LBL-DAP and G-DAP lines is slightly closer to each other compared to that under the NSFNET topology. Besides this, the actual values of the blocking probabilities are also higher than those taken under NSFNET. The reason of this observation is the non-uniform nodal degree distribution and the greater size of the EON topology in comparison to the NSFNET. As seen in Figure C.3, the nodal degrees vary from two to five so some of the links have to be overloaded. As a result, determining a global sharing degree for each class and assigning appropriate link costs gets closer to setting negligible costs to the shareable links as the load gets heavier and the network starts suffering from available resources. As a supplementary result to the overall blocking probability is thought to be the per-class blocking probability experiment which is shown in Figure 4.8. Similar to the per-class blocking probabilities under NSFNET, the major contribution to the overall blocking probability comes from the connections of $class-5$, and the difference between G-DAP and LBL-DAP results for $class-5$ are less than those obtained under the NSFNET. However, under LBL-DAP, $class-4$ and $class-3$ connections still experience significantly low blocking probability compared to those under CAFES and G-DAP.

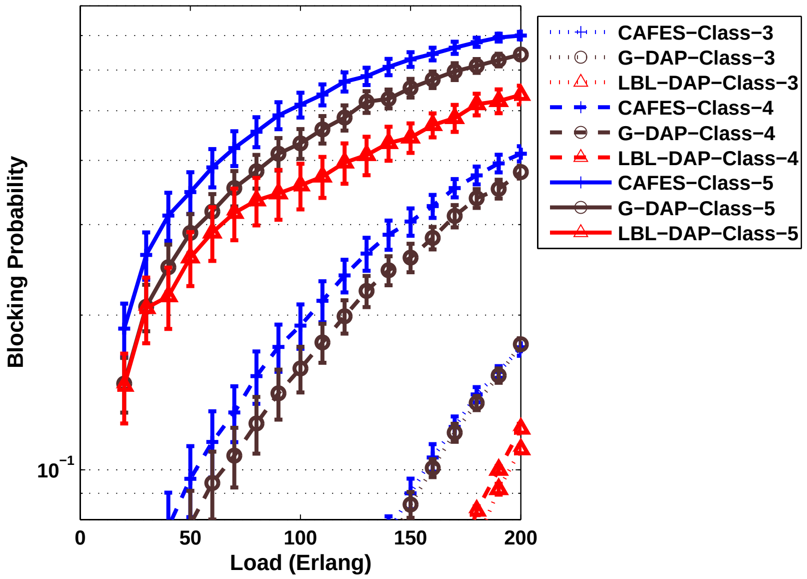


Figure 4.8: Blocking probabilities per each availability class with LBL-DAP, G-DAP, and CAFES under EON

In Figure 4.9, availability aware provisioning schemes are compared in terms of average resource overbuild under 28-node EON. Similar to the results taken under the NSFNET topology, LBL-DAP lead to a significant decrease in resource overbuild. Moreover, G-DAP does not introduce an increase to CAFES in resource overbuild. Thus, here, the adaptive techniques relatively utilize less amount of backup resources to protect the working resources. Moreover, the decrease in the resource overbuild is sharper here when compared with the results under the NSFNET topology. The reason of this behavior lies in the following points: 1) The connectivity of the EON is heterogeneous, 2) The links in the topology are shorter than NSFNET so short fibers have high availability, 3) The lightpaths consist of shorter hops, 4) The ratio of the shared connections is increased.

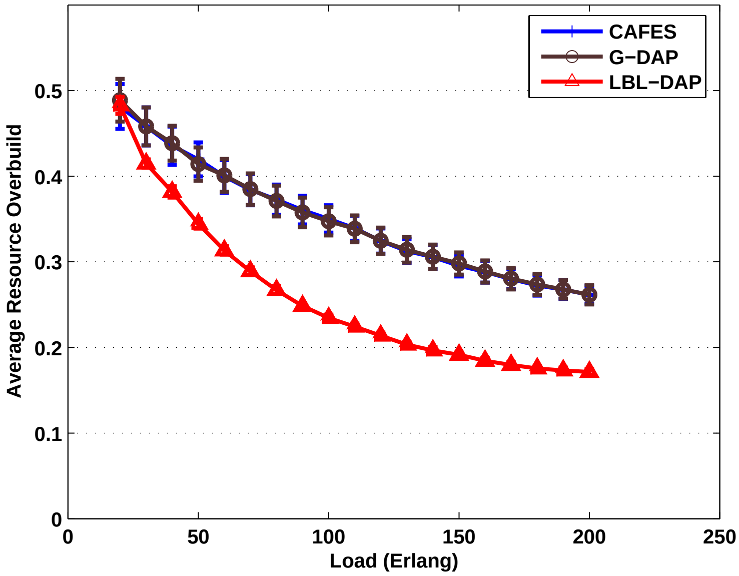


Figure 4.9: Resource Overbuild with LBL-DAP and G-DAP under EON

In Figure 4.10, we present the distribution of the protection schemes for the $class-4$ and $class-5$ connections under G-DAP and LBL-DAP. For both of the SLA classes, LBL-DAP provisions more amount of shared connections compared to G-DAP. Besides this, LBL-DAP provisions less amount of connections with dedicated path protection for both of the classes. Thus, backup resource consumption of LBL-DAP is quite less than G-DAP which confirms the result illustrated in Figure 4.9.

The following results present the average unavailability per connection for CAFES, G-DAP, and LBL-DAP under 28-node EON topology. In Figure 4.11, it seems that, all of the three schemes lead to almost close unavailability levels. However, similar to the results under the NSFNET topology, LBL-DAP leads to a degraded unavailability, and as the load level goes beyond 100 Erlangs, G-DAP introduces a slight decrease in average unavailability per connection. As in the performance evaluation part under the NSFNET, the corresponding figure shows that the adaptive connection provisioning schemes do not cause any availability degradation on the conventional

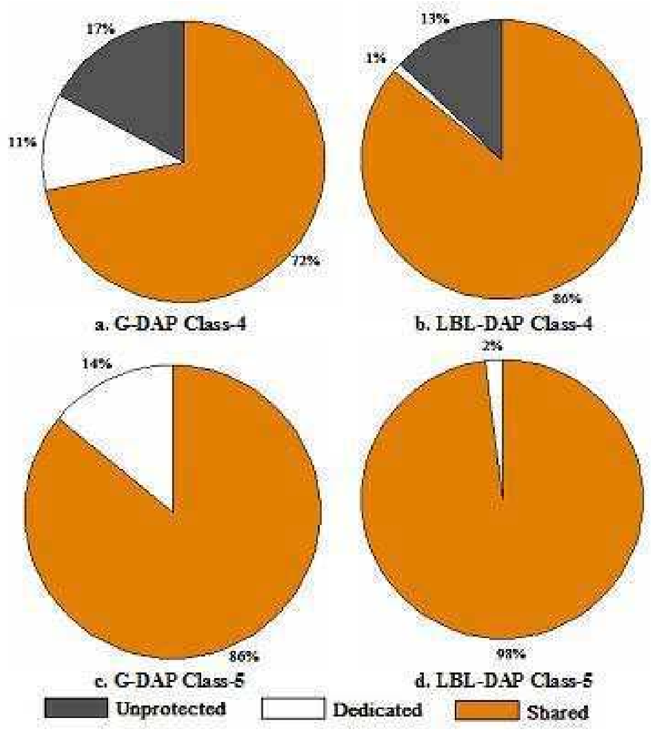


Figure 4.10: Distribution of protection types when provisioning the connections under EON

reliable connection provisioning scheme CAFES although they decrease the blocking probability and limit resource overbuild under the 28-node EON topology.

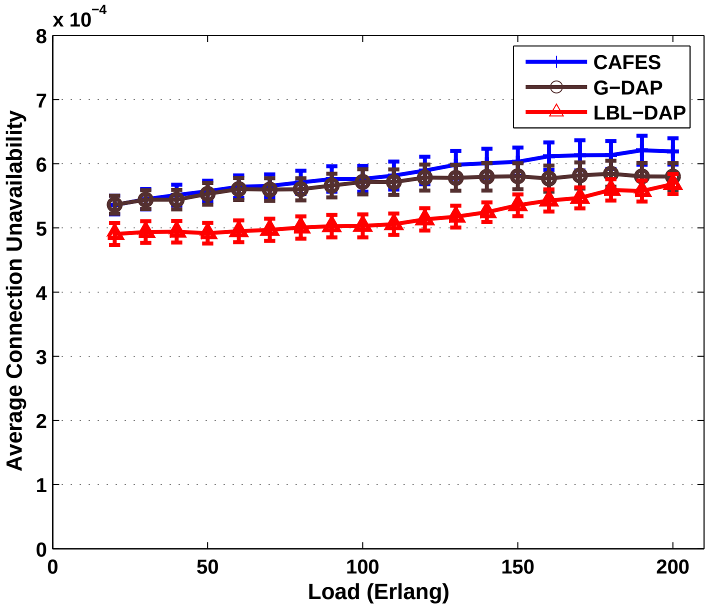


Figure 4.11: Average unavailability per connection with LBL-DAP and G-DAP under EON

As a supplement for the results in Figure 4.7, Figure 4.8, Figure 4.9, and Figure 4.11, we also present the statistically collected data showing the blocking reason of the dropped connections as seen in Figure 4.12. Similar to the results in Figure 4.4, under the heavy load levels, the amount of the blocked connections that are dropped due to their availability requirements are less in G-DAP and LBL-DAP when compared to those in CAFES. Under light and moderate loads, due to efficient resource utilization, low blocking probability, and the major contribution of $class - 5$ connections to the resource overbuild, LBL-DAP drops less amount of connections due to resource unavailability. As a result, the adaptive schemes do not cause a decrease in the unavailability per connection while they introduce improvement in terms of blocking probability and resource overbuild.

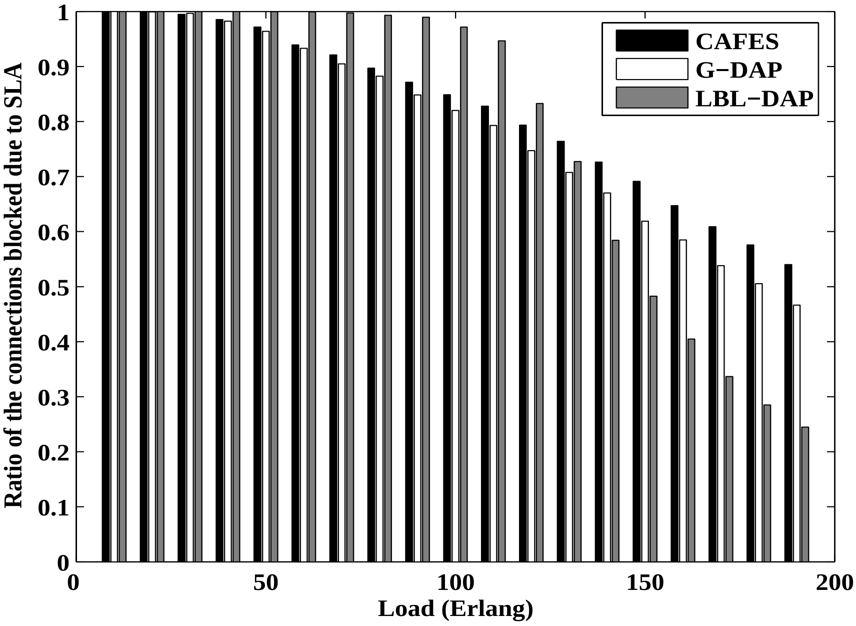


Figure 4.12: Ratio of blocked connections due to SLA requirement with LBL-DAP, G-DAP, and CAFES under EON

As a concluding remark, we have seen that the proposed schemes lead to higher acceptance rates. Moreover, G-DAP leads to a close resource overbuild value while LBL-DAP significantly degrades the resource overbuild of the conventional scheme. Besides these, G-DAP introduces almost the same availability level with the conventional reliable connection provisioning scheme. As the load gets heavier, G-DAP also enhances the connection availability. LBL-DAP introduces better connection availability at each load level. Thus, the proposed adaptive schemes lead to better blocking probabilities, and resource overbuild values without violating the average connection unavailability. Moreover, we also show that, LBL-DAP leads to the best performance when this performance parameters are considered, and under both of the topologies while its performance in terms of blocking probability gets closer to that of G-DAP under EON due to the heterogeneous nodal degree distribution in EON. As a supporting result, we have also shown that the proposed adaptive schemes decrease the amount of the blocked connections that are dropped due to their availability requirement under heavy load levels since they offer better availability per connection.

5. AVAILABILITY AND OVERLAPPING SHARED SEGMENT PROTECTION

As seen in the literature survey in Chapter 2, most of the previous work in this field focuses on the availability constrained connection provisioning under dedicated or shared path protection. In this chapter, we deal with availability and shared segment protection. First, we present an availability analysis method for overlapping segment protection. We verify our theoretical availability calculation with the actual availability of a connection. We show that our proposed availability calculation lies within a very small precision interval. Relying on the verified availability analysis, we present two availability constrained connection provisioning schemes that work under shared segment protection and that are built on top of the *Generalized Segment Protection (GSP)* [34]. The first scheme is called *Availability-Constrained Generalized Segment Protection (AC-GSP)*. The objective of *AC-GSP* is assigning working and protection segments by offering maximum availability for the incoming connections. The second scheme is called *Shareability Driven Availability-Constrained Generalized Segment Protection (SDAC-GSP)* [95]. *SDAC-GSP* is a modified version of *AC-GSP*. It attempts to decide feasible sharing degrees for the *intersecting links* of the backup segments. For a connection, *intersecting links* of a backup segment are the links that intersect with the working path of the connection. We show that *SDAC-GSP* introduces higher acceptance rate and increased availability per connection due to the attempt of forcing to protect every working link with more than one segment. However, protection of a working link with more than one protection segment is not a must. Thus, since the more segments the better availability and the less blocking probability for a connection, this approach increases resource consumption in a feasible range.

5.1 Preliminary Information For Shared Segment Protection

Segment protection is a compromise between link protection and path protection. The working path of a connection is partitioned into segments and each segment is protected by a backup segment [9, 33]. The partitioned segments can be either overlapping [33,34,41] or non-overlapping [96]. In this work, we consider overlapping segment protection as shown in Figure 2.4, and we ue the term *shared segment protection* to point *overlapping shared segment protection*. In the related figure, three overlapping backup segments are illustrated to protect the working path between source and destination. The protection capacity is twice for the links at the overlapping sections of the backup segments. In the illustrated scenario, $link-4$ (between $node-2$ and $node-3$) and $link-6$ (between $node-5$ and $node-6$) are protected by two segments per each.

Another advantage of shared segment protection is its robustness to multi-failure. Let us consider the protection scenario in Figure 2.4. Assume that the link between $node-2$ and $node-3$ fails, followed by the failure of any link or links in the protection segment that starts from $node-2$ and ends at $node-6$. Moreover, assume another concurrent failure on the working path between $node-1$ and $node-2$. In this multi-failure scenario, the protection segment originating at *source* and ending at node $node-3$ is activated. Thus, the traffic from *source* to $destination$ is switched on this protection segment starting at *source*. The traffic is switched onto the working path, and forwarded to the $destination$ at $node-3$.

A number of algorithms are previously proposed for segment protection [33,34,40,97]. We investigate some of this algorithms briefly in Chapter 2. Several shared segments protection schemes are based on GSP [98, 99]. Therefore, as a basis to our proposed availability constrained provisioning schemes, we use the Generalized Segment Protection (GSP) algorithm in [34] to select the protection domains constructed by the segments. We give a brief explanation on the working principle of the algorithm. At the beginning, K working paths are selected based on a pre-determined criteria (shortest path, minimum unavailability, shortest hop count, etc.). Upon selecting the *K-paths*, for each working path, the links along the working path are reversed. The cost of every link that has at least one spare channel is degraded by a negligible coefficient ε. Each link that originates out of the working path but ends on the working path is modified so that its end point is moved to the previous node on the working path. At the end, a path with minimum cost is selected from source to destination. Following the path selection, the modified links are restored, and the connection is provisioned with the corresponding overlapping backup segments [34, 98]. The working path/backup segments group with the minimum cost is selected out of K different solutions. The algorithm is given in Appendix-D.

5.2 Availability Analysis under Shared Segment Protection

To best of our knowledge, no availability analysis formulation for shared segment protection exists in the literature. Therefore, here, we define our analytical estimation method for connection availability under overlapping shared segment protection. A connection is available if one of the following conditions holds: 1) all the links on its working path are available, 2) If there is a link failure in the working path, the corresponding segment protection of the failed link is available. Here, it is worth noting that *segment protection of a link* stands for the set of the protection segments that protects the corresponding link on the working path. Thus, in its fundamental form, this statement can be formulated as in Equation 5.1 where A$_c$ is the availability of the connection, W_c is the set of links in the working path of the connection, A_i is the availability of the i^{th} link in the working path, and A_{S_i} is the availability of the segment protection of the i^{th} link of the working path. Due to overlapping of the protection segment, a working link can be protected by more than one backup segments. Therefore the availability of the segment protection of $link\ i$ (A_{S_i}) is the sum of the availabilities of its protecting segments excluding the probabilities including more than once. This can be formulated as shown in Equation 5.2 where Seg_i is the set of the segments protecting the $link\ i$.

$$A_c = \prod_{i \in W_c} (A_i + A_{S_i} - A_i \cdot A_{S_i}) \qquad \textbf{(5.1)}$$

A segment is available if all the links along this segment are available. However, $connection\ c$ may share the backup resources with other connections on a segment. When a link on the working path of $connection\ c$ fails, in case of a failure along the

$$A_{S_i} = \sum_{s \in Seg_i} (A_s) - \sum_{p \in Seg_j} \sum_{s \in Seg_i, i \neq j} (A_s \cdot A_p) \\ + \sum_{r \in Seg_k} \sum_{p \in Seg_j, j \neq r} \sum_{s \in Seg_i, i \neq j} (A_s \cdot A_p \cdot A_r) - \ldots \cong 1 - \prod_{s \in Seg_i} (1 - A_s) \qquad \textbf{(5.2)}$$

working path of any of the connections in the sharing group of *connection c* at the same time, *connection c* may not get the resources along the corresponding backup segment. Therefore, the availability of a protection segment for the i^{th} working link of the connection-*c* has to be expressed with additional constraints. A protection segment is available to a link on the working path of *connection c* if one of the following two conditions holds: 1) The working paths of all connections that are in the sharing group of the connection-*c* on this segment are available, 2) If there is at least one failure in those working paths, connection-*c* can still have the backup segment channels with a probability of δ. These can be generalized and formulated as seen in Equation 5.3 where SG_s represents the set of connections that share at least one backup channel with *connection c* on *segment s*. It is assumed that a failure in the working path of the connections in the sharing group SG_s affects the availability of the *segment s* if the failed link is protected by the corresponding segment. Therefore we include $|Seg_z|$ in the denominator to normalize the unavailability of the working path of $connection - z$ with the number of its protection segments where $connection - z$ is in the sharing group of $connection - c$ whose availability is being calculated.

$$A_s = (\prod_{k \in s} A_k) \cdot [\prod_{z \in SG_s} [1 - \frac{(1 - \prod_{j \in W_z} A_j)}{|Seg_z|}] \\ + [1 - \prod_{z \in SG_s} [1 - \frac{(1 - \prod_{j \in W_z} A_j)}{|Seg_z|}]] \cdot \delta] \qquad \textbf{(5.3)}$$

When we substitute the formulations in Equation (5.2) and Equation (5.3) into Equation (5.1), we obtain the generalized open formula in Equation 5.4 for availability calculation of the *connection c*.

According to the availability analysis, it can be said that a connection is available if all of its protection domains are available. Each protection domain is formed by the working links and their corresponding backup segments. Hence, the more protection by more backup segments, the more availability offered to a connection. In

$$
\begin{aligned}
A_c = \prod_{i\in W_c} [A_i \\
+1 - \prod_{s\in Seg_c} \{1 - [(\prod_{k\in s} A_k)\cdot [\prod_{z\in SG_s} (1 - \frac{(1-\prod_{j\in W_z} A_j)}{|Seg_z|}) \\
+[1 - \prod_{z\in SG_s} (1 - \frac{(1-\prod_{j\in W_z} A_j)}{|Seg_z|}]) \cdot \delta]]\} \\
-A_i \cdot +1 - \prod_{s\in Seg_c} \{1 - [(\prod_{k\in s} A_k)\cdot [\prod_{z\in SG_s} (1 - \frac{(1-\prod_{j\in W_z} A_j)}{|Seg_z|}) \\
+[1 - \prod_{z\in SG_s} (1 - \frac{(1-\prod_{j\in W_z} A_j)}{|Seg_z|}]) \cdot \delta]]\}
\end{aligned}
\qquad \textbf{(5.4)}
$$

performance evaluation section, we show the validation of this analysis by numerical results.

5.3 Availability-aware Connection Provisioning For Shared Segment Protection

In this section, we present the two availability constrained connection provisioning schemes that we introduced [95] under overlapping shared segment protection. Both of the schemes are derived from Generalized Segment Protection (GSP) algorithm [34].

5.3.1 Availability-Constrained Generalized Segment Protection (AC-GSP)

Relying on the availability analysis model in the previous section, we modify and adapt the Generalized Segment Protection algorithm to availability constrained connection provisioning. We call this adapted scheme, *Availability Constrained General Segment Protection (AC-GSP)*. AC-GSP starts with searching for three alternative working paths ($W^{(1)}$-$W^{(3)}$). The search criteria for the working parts are as follows:

- W^1: Most Reliable Path: The path that leads to the minimum cost when each link is set to the cost of the unavailability value of a wavelength channel on it. When connections arrive with previously specified availability requirements, and W^1 leads to a value greater than the availability requirement of the connection, there is no need to search for a backup lightpath for the connection. Thus, the connection can be unprotected.
- W^2: The path that leads to the minimum cost when each link is set to the cost of the unavailability value of a wavelength channel on it (one's complement of the

availability), and the link with the minimum cost in W^1 is removed.
- W^3: The path that leads to the shortest hop count.

The corresponding backup path search for the working paths is straightforward. Link cost assignment for the backup path search is shown in Equation 5.5 where $\lambda_f(e)$ and $\lambda_s(e)$ are the free and spare capacity on link-e respectively, $\bar{e}$ is the link between the same nodes but in the reverse direction of the link-e. C_e^{old} is the link cost used for searching the corresponding working path which is the unavailability of $linke$ for the first two working paths, and one for the last candidate working path. We set ε to 10^{-5} in AC-GSP and its counterpart which is presented in the next subsection.

$$C_e^{new} = \left\{ \begin{array}{cc} \infty & e \in W_c \vee \lambda_s(e) + \lambda_f(e) = 0 \\ -C_e^{old} & \bar{e} \in W_c \\ \varepsilon \cdot C_e^{old} & \lambda_s(e) > 0 \\ C_e^{old} & else \end{array} \right\} \tag{5.5}$$

Upon assigning the link costs for the backup path search, the modification of the links, searching for the minimum cost path between source-destination, and the restoration of the modified links are done as in GSP. Once AC-GSP has the backup paths for the alternative working paths of the connection, it assigns wavelengths for the backup paths. Wavelength assignment is done by sorting the wavelengths on each link according to the number of connections sharing those channels as backup resources in ascending order. Then hop-by-hop, AC-GSP searches an available wavelength starting from the first wavelength in the sorted list. If assigning the selected wavelength does not cause any availability violation for any of the currently provisioned connections,the wavelength is assigned, and AC-GSP proceeds with wavelength assignment for the next hop. If the wavelength assignment is rejected due to availability violation for any other connection, the algorithm proceeds with the the next spare wavelength in the list. If all the spare wavelengths reject the assignment, a free wavelength is tried to be assigned. If there is neither a shareable spare wavelength nor a free wavelength for the connection on the corresponding link, connection provisioning for the corresponding working path is blocked due to lack of resource.

Upon obtaining the candidate working paths and their corresponding backup segments, the working path/backup segment pair that leads to the highest availability is selected. If neither of the pairs provide a solution set, the connection is blocked due to resource limitation. On the other hand, if the connection arrives with a specific availability requirement in its service level agreement (SLA), and if the selected working/backup group does not meet the availability requirement, the connection is blocked due to availability non-satisfaction.

5.3.2 Shareability Driven Availability-Constrained Generalized Segment Protection (SDAC-GSP)

We modify AC-GSP to provide shareability awareness for sake of introducing higher availability and less blocking probability for the incoming connections. We call the modified scheme *shareability driven availability constrained connection provisioning (SDAC-GSP)*. SDAC-GSP inherits all the main properties of AC-GSP, like being based on GSP and working with differentiated availability requirements. As we see in Equation 5.4, the more protection segments the more availability introduced to a connection. A segment intersects the working path of a connection at two points which are the beginning and the end point of the segment. Therefore the more intersecting points the more protection segments, and the more availability. Hence, for each availability class, SDAC-GSP attempts to estimate a feasible sharing degree on the *intersecting links*. Feasible sharing degree estimation was used in the adaptive availability-aware connection provisioning schemes in Chapter 3 and Chapter 4 for SBPP. Similar the concept for those schemes, we define a tradeoff function by using the periodically collected data from the network. As seen in Equation 5.6, the unavailability per connection for the corresponding class and the resource overbuild are the input parameters of the tradeoff function. Obviously, the value of the tradeoff function is updated periodically, and aimed to be minimized. The idea behind the sharing degree modification approach is inherited from the availability modification in [46] as in the other works [83, 91, 93]. In Equation 5.6, $T_n^{(k)}$, stands for the tradeoff value for the connections of *class k* calculated for the (n^{th}) period while $R_{(n-1)}$, and $A_{(n-1)}^{(k)}$ stand for the ratio between resource overbuild and the average availability value at the end of the last period ($(n-1)^{th}$) respectively.

$$T_n^{(k)} = R_{(n-1)} \cdot (1 - A_{n-1}^{(k)}) \qquad \textbf{(5.6)}$$

Increase in the number of protection segments leads to increase in the number of WDM channels. This behavior decreases the average connection unavailability $(1-A)$. As expected, the opposite way of change in backup resource consumption also causes the connection unavailability to increase. This inverse relation is investigated periodically where a period consists of N connection arrivals. At the end of the each period, the heuristic runs to update the feasible sharing degrees on the *intersecting links* for each availability class.

The pseudocode of the algorithm to update the sharing degree is shown in Appendix-C. According to the sharing degree update heuristic, the tradeoff value for an availability class is compared to its previously calculated value. If current value is less than the previous one, the update heuristic repeats the last action taken for the sharing degree of the corresponding availability class. If the last action was to increment, sharing degree is incremented, otherwise it is decremented. However, if currently calculated tradeoff value for the corresponding availability class is greater than its previous tradeoff value, the opposite of the last action is taken for the sharing degree of the related class. Similar to our previous works using this tradeoff update, sharing degree for *class k* (S_k) is limited by an upper bound, $UPLIMIT$, and a lower bound, $DOWNLIMIT$.

SDAC-GSP uses the same strategy with AC-GSP for routing and wavelength assignment. However, it differs from AC-GSP in assigning costs when searching for the backup segments. Equation 5.7 shows the link cost assignment of SDAC-GSP for the backup segment search where C_e^{old} is set to the cost of the link used in working path selection. According to the equation, the connection is preferred to select as much as backup segments it can, however, it is also forced to select the *intersecting links* that form the segments considering the shareability for the corresponding availability class. It is expected that, forcing the connection to have more backup segments forces every single link of the working path to be protected by double segments. As a result, a resource consumption overhead is also introduced by SDAC-GSP for sake of enhanced availability and acceptance rate as we discuss in the performance evaluation section.

$$C_e^{new} = \left\{ \begin{array}{cc} \infty & e \in W_c \vee \lambda_s(e) + \lambda_f(e) = 0 \\ -C_e^{old} & \bar{e} \in W_c \\ \varepsilon \cdot (-SH_k) \cdot C_e^{old} & \lambda_s(e) > 0 \wedge \lambda_s(e) < SH_k \wedge e \cap W_c \neq \phi \\ \varepsilon \cdot C_e^{old} & \lambda_s(e) > 0 \\ C_e^{old} & else \end{array} \right\} \qquad \textbf{(5.7)}$$

Since AC-GSP and SDAC-GSP use the same routing and wavelength assignment strategy, they have the same running time complexity due to sorting the wavelength channels on each link. During the backup segment search, link cost assignment takes $O(W \cdot L)$ time since each wavelength on each link is checked once. In the wavelength assignment step, the channels are first grouped as working, spare and free channels, and then the spare channels are sorted. Thus, the time for searching and assigning a spare channel takes $O(W)$ time in the worst case on each link.

5.4 Performance Evaluation

This section presents the validation of the availability analysis for shared segment protection, and evaluates the performance of the proposed connection provisioning schemes, namely AC-GSP and SDAC-GSP under different network constraints. We run our simulations by using Visual C++, and use the simulation environment defined in Appendix-C. We use the topology in Figure C.4. We use the formula in Equation 1.1 to calculate the link availabilities. Each point in the graphs represent the average of five simulation runs and we also present 90%confidence intervals in the figures. In the connection provisioning schemes AC-GSP, and SDAC-GSP, the negligible coefficient ε is set to 10^{-5} in backup segment search. We assume that all the nodes have wavelength conversion capability.

5.4.1 Availability Analysis Validation

To validate our proposed availability analysis method, we assume that the network is capable of provisioning a working path and its corresponding backup segments to every incoming connection arriving without a pre-specified availability requirement, i.e the network has infinite amount of resources.

In availability analysis validation step, connection provisioning scheme is selected to be AC-GSP. It is worth noting that due to running the simulations to compare the actual and calculated availability values of the connections, the connections are not blocked due to availability requirements. Therefore, we modify AC-GSP appropriately to handle this situation. MTTR values on the links are distributed negative exponentially with mean of 12 hours. In the simulations, failures arrive following a Poisson distribution. At each run, we introduce 2000 failures into the network. The validation of the availability analysis is two-fold: 1) We apply different error rate values ($1/MTTF$) as 200 FIT, 400 FIT, 600 FIT, 800 FIT, and 1000 FIT to a fixed number of provisioned connections where FIT corresponds to the failures in 10^9 hours. 2) We set the 1/MTTF value to 400 FIT and run the same simulation scenarios for different number of connection demands.

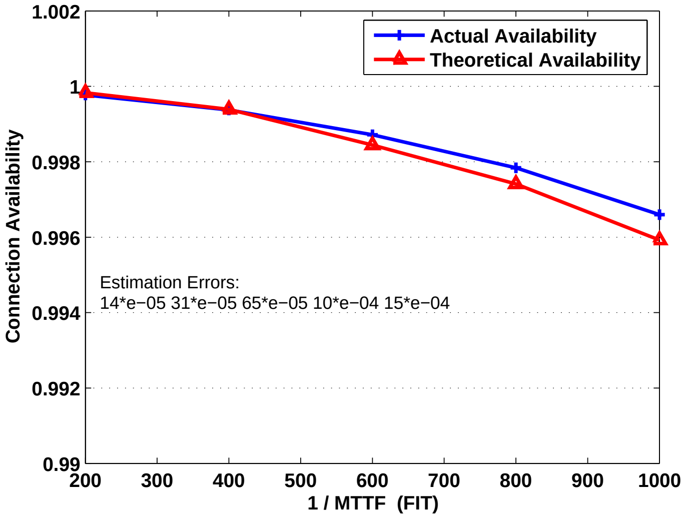


Figure 5.1: Actual and theoretical availability per connection with different failure rates

We compare the theoretical availability and the actual availability per connection in Figure 5.1. The results are collected from 150 connections that are uniformly provisioned previously. Although the failure rate increases estimation error ratio, the maximum value for estimation error ratio is still at the level of 0.15% as seen in the figure above.

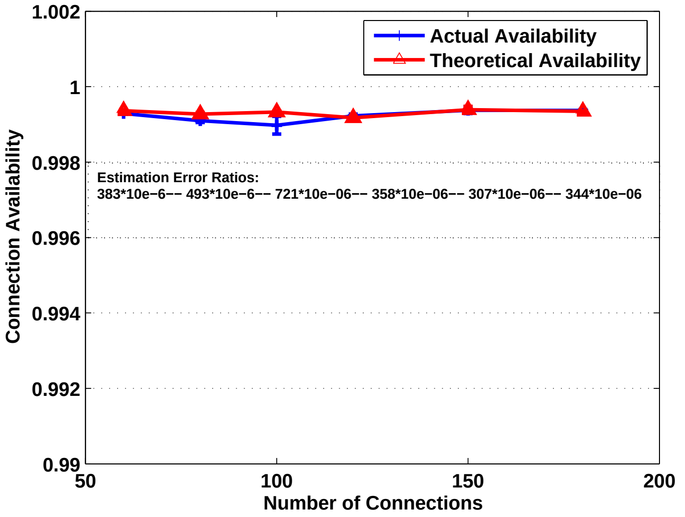


Figure 5.2: Actual and theoretical availability per connection with different connection demands

In the second step, the 1/MTTF value is set to 400 FIT and the availability analysis method is tested with the simulation scenarios for different number of connection demands. The results are shown in in Figure 5.2. According to the results, the availability estimation error ratio is at the level of 10^{-6}. As a result, the availability analysis approach also holds under different traffic loads.

Based on the validation of the analysis, it can be concluded that the theoretical and the actual availability comparisons in the figures verify that the proposed availability analysis for overlapping shared segment protection can be used as a basis for availability calculation of the connection provisioning policies proposed to work with shared segment protection. Hence, the performance comparison section evaluates the performance of AC-GSP and SDAC-GSP by using this availability analysis for the incoming connections with pre-specified SLA requirements.

5.4.2 Performance Comparison

This part of the simulations evaluate and compare the performance of AC-GSP and SDAC-GSP under resource-plentiful and resource-scarce environments. In the resource plentiful environment the number of wavelengths per fiber is set to 32 while in the resource-scarce environment it is set to 16. Thus, we compare both of the techniques in terms of blocking probability, connection availability, resource consumption, and resource dependency. Connections arrive with previously specified availability requirements. Three availability levels are assumed as 0.98, 0.99, and 0.999. Based on AC-GSP and SDAC-GSP, a connection can be provisioned unprotected, shared backup path protected or shared segment protected. If the most reliable path ($W^{(1)}$) satisfies the availability requirement of an incoming connection by itself, SDAC-GSP and AC-GSP ends and provision the connection unprotected.

In the simulations, we set $1/MTTF$ to 400 FIT and $MTTR$ to 12 hours. Connections arrive following a Poisson distribution. The average connection holding time is negative exponentially distributed and is normalized to 1s. Since the connections arrive with pre-specified availability requirements, connection blocking can be due to either resource limitation or availability requirement as in the schemes work under SBPP. Blocking due to resource limitation stands for the case where AC-GSP or SDAC-GSP returns three empty sets in the routing phase of the RWA process. Then, blocking due to availability requirement corresponds to the case where AC-GSP or SDAC-GSP successfully configures the RWA for a connection but the configured RWA leads to less availability compared to the availability requirement of the related connection. We run our simulations for 30000 connection arrivals after a warming up period. In SDAC-GSP, we set the DOWNLIMIT and UPLIMIT values to two and eight respectively which are determined empirically in previous studies [83, 91, 93]. In SDAC-GSP, the running period for the tradeoff update heuristic is selected as 1000 connection arrivals as in [93].

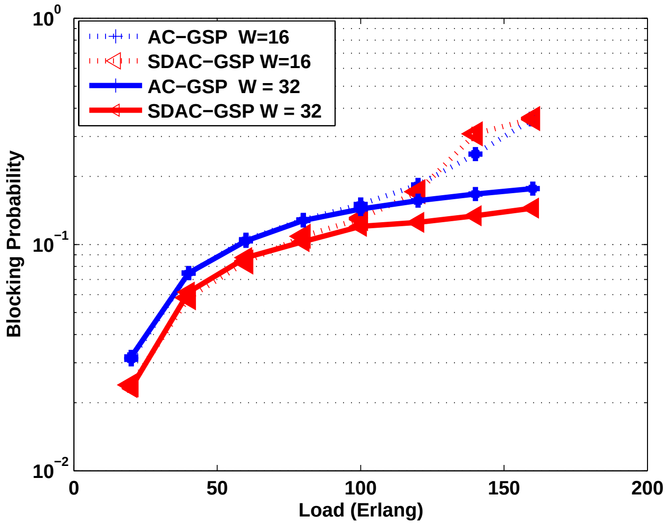


Figure 5.3: Blocking probability vs load with AC-GSP and SDAC-GSP

The first evaluation and comparison metric is blocking probability of AC-GSP and SDAC-GSP under resource-plentiful and resource-scarce environments in Figure 5.3. The results collected under resource-plentiful environment are represented by the straight lines where the results corresponding to the resource-scarce environment are represented by the dashed lines. In the resource-scarce environment, connections are expected to be blocked due to both availability requirement and resource limitation. For this reason, as load gets heavier, the connections are more likely to be blocked due to resource constraints and the blocking probabilities in the resource-scarce environment is greater than those in the resource-plentiful environment. For the same reason, SDAC-GSP seems to outperform AC-GSP in resource-plentiful environment. However, in the resource-scarce environment, as the load gets heavier, e.g after the network load of 100 Erlangs, blocking probability increases. SDAC-GSP forces connections to use more protection segments considering feasible sharing degrees on the WDM channels on links for each class, it leads to higher resource consumption where the network can hardly handle the incoming requests as the load gets heavier. Under resource-plentiful environment, SDAC-GSP leads to lower blocking probability at each load level as seen from the straight lines in the figure. Since SDAC-GSP aims to protect the links of the connection with as much as protection segments, and also considers the feasible sharing degrees on the backup channels, it targets high availability for the connections. As a result, SDAC-GSP can satisfy the availability requirement of more connections compared to AC-GSP. It is worth noting to say that, in the resource-plentiful environment, connections are not blocked due to resource limitation but to availability requirements. Thus, SDAC-GSP is runs efficiently under sufficient number of wavelengths per fiber at each load level or under restricted number of wavelengths at light and moderate load levels. We also evaluate the effect of the ε parameter to the heuristics, and present the results in the Appendix section in Fig.F.1.

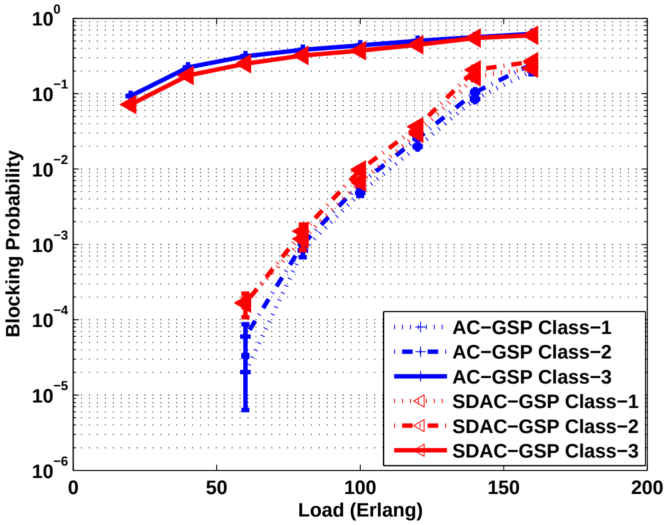


Figure 5.4: Blocking Probability for different classes under AC-GSP and SDAC-GSP in resource-scarce environment

Figure 5.4 shows the blocking probabilities for each availability class in resource-scarce environment. As expected, the major contribution to the blocking probability comes from the blocked connections of *class* 3. This can be seen in the figure for both of the schemes, AC-GSP and SDAC-GSP. For the load levels less than 120 Erlangs, SDAC-GSP blocks less number of connections compared to AC-GSP. SDAC-GSP aims to introduce better availability for the incoming connections, therefore, it forces the connections to select more number of segments considering feasible sharing degrees on the *intersecting links* of the segments. Thus, SDAC-GSP gives priority to *class* – 3 connections in terms of availability, and allows introducing degraded availability to *class* 2 and *class* 1 connections. Since the major contribution of the overall blocking probability comes from the dropping of the highest availability class connections, this figure is a supplement for the results illustrating the overall blocking probability in Figure 5.3.

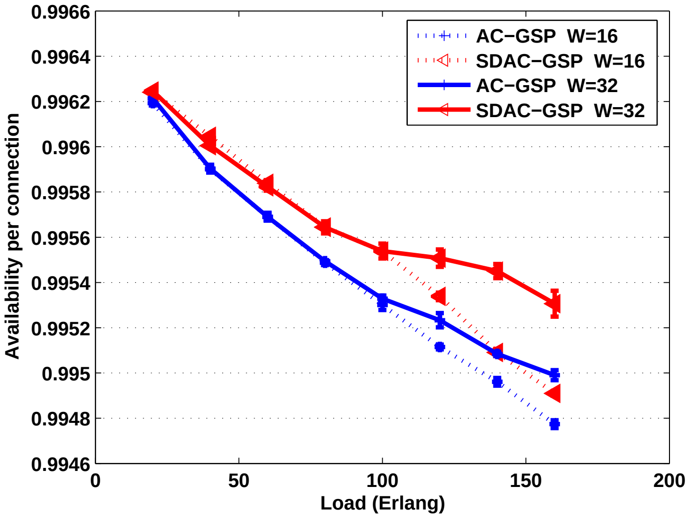


Figure 5.5: Average connection availability vs load for AC-GSP and SDAC-GSP

We evaluate and compare the performance of AC-GSP and SDAC-GSP under the two different environments in terms of availability per connection in Figure 5.5. In the resource-plentiful environment, connection blocking is due to availability requirements of the incoming connections so SDAC-GSP is supposed to introduce higher availability to the connections as a result of leading to high acceptance rate seen in Figure 5.3. SDAC-GSP aims to increase the availability connection by forcing them to select more protection segments by considering the feasible sharing degree on the intersecting links, it leads to better connection availability even in resource-scarce environment when compared to AC-GSP. Another observation and a required justification on the result is that, both of the provisioning schemes offer the same connection availability until the load level of 100 Erlangs. Beyond 100 Erlangs, due to the resource constraints, both of the techniques provide less availability for the provisioned connections than those they offer in resource-plentiful environment. Moreover, the performance difference with respect to the connection availability starts to occur after this load level.

Table 5.1: Average availability per connection for different values when W=32

Scheme	Load	Class-1	Class-2	Class-3
AC-GSP	20	0.9919	0.9973	0.9997
	60	0.9917	0.9970	0.9996
	100	0.9915	0.9967	0.9995
	140	0.9914	0.9965	0.9995
SDAC-GSP	20	0.9919	0.9974	0.9997
	60	0.9917	0.9971	0.9996
	100	0.9916	0.9969	0.9995
	140	0.9916	0.9968	0.9995

Table 5.2: Average availability per connection for different values when W=16

Scheme	Load	Class-1	Class-2	Class-3
AC-GSP	20	0.9918	0.9974	0.9997
	60	0.9917	0.9970	0.9996
	100	0.9915	0.9967	0.9995
	140	0.9913	0.9964	0.9995
SDAC-GSP	20	0.9919	0.9974	0.9997
	60	0.9917	0.9971	0.9995
	100	0.9916	0.9969	0.9995
	140	0.9912	0.9966	0.9995

We summarize the connection availability per-class basis in Table 5.1 under different load levels for AC-GSP and SDAC-GSP in resource-plentiful environment. Obviously, the availability values of the connections are close to each other. Furthermore, both of the schemes lead to the same availability levels for $class$ 3 connections. However, being coherent with the results presented in Figure 5.5, under heavier loads SDAC-GSP provides better availability for $class-2$ and $class-1$ connections which causes the overall availability per provisioned connection to be better for SDAC-GSP in Fig 5.5. The results taken in resource-scarce environment are given in Table 5.2 and are also similar to the ones taken in resource-plentiful environment. The difference between the availability values of $class$ 1 and $class$ 2 connections under the lightest and the heaviest loads also complies with the connection availability comparison between AC-GSP and SDAC-GSP.

Since the connections can be blocked either due to availability requirement or due to resource limitation in resource-scarce environment, in Figure 5.6, blocking reason of the blocked connections is shown under varying load. According to the figure, SDAC-GSP tends to block the connections are blocked due to resource limitation

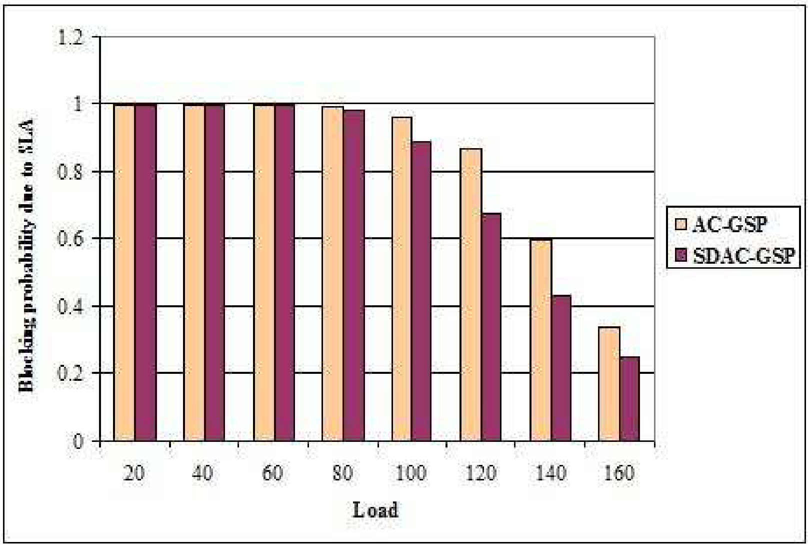


Figure 5.6: Connection blocking reason under AC-GSP and SDAC-GSP in resource-scarce environment

rather than availability requirement as the load gets heavier. SDAC-GSP offers higher connection availability as the load gets heavier. Offering high connection availability is done by protecting the working path with increased number of overlapping segments by taking into consideration the shareability constraint. This introduces increased wavelength consumption where insufficient resources problem occur for future connections. As a result, SDAC-GSP starts blocking the connections due to resource constraints more than AC-GSP does.

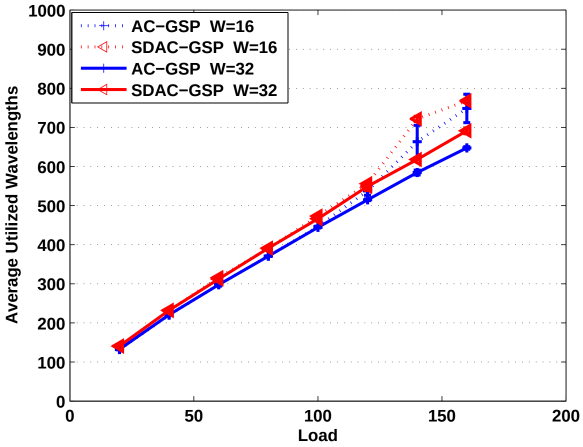


Figure 5.7: Wavelength utilization of AC-GSP and SDAC-GSP

To explain the results related to blocking probability, connection availability, and connection blocking reason, we compare the proposed schemes in terms of wavelength utilization and resource overbuild in Figure 5.7 and Figure 5.8under resource-plentiful

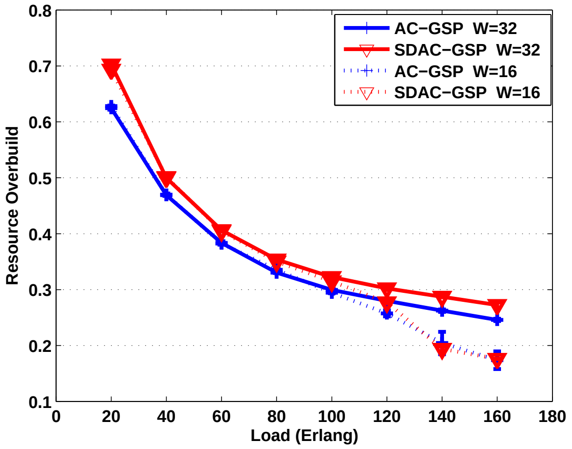
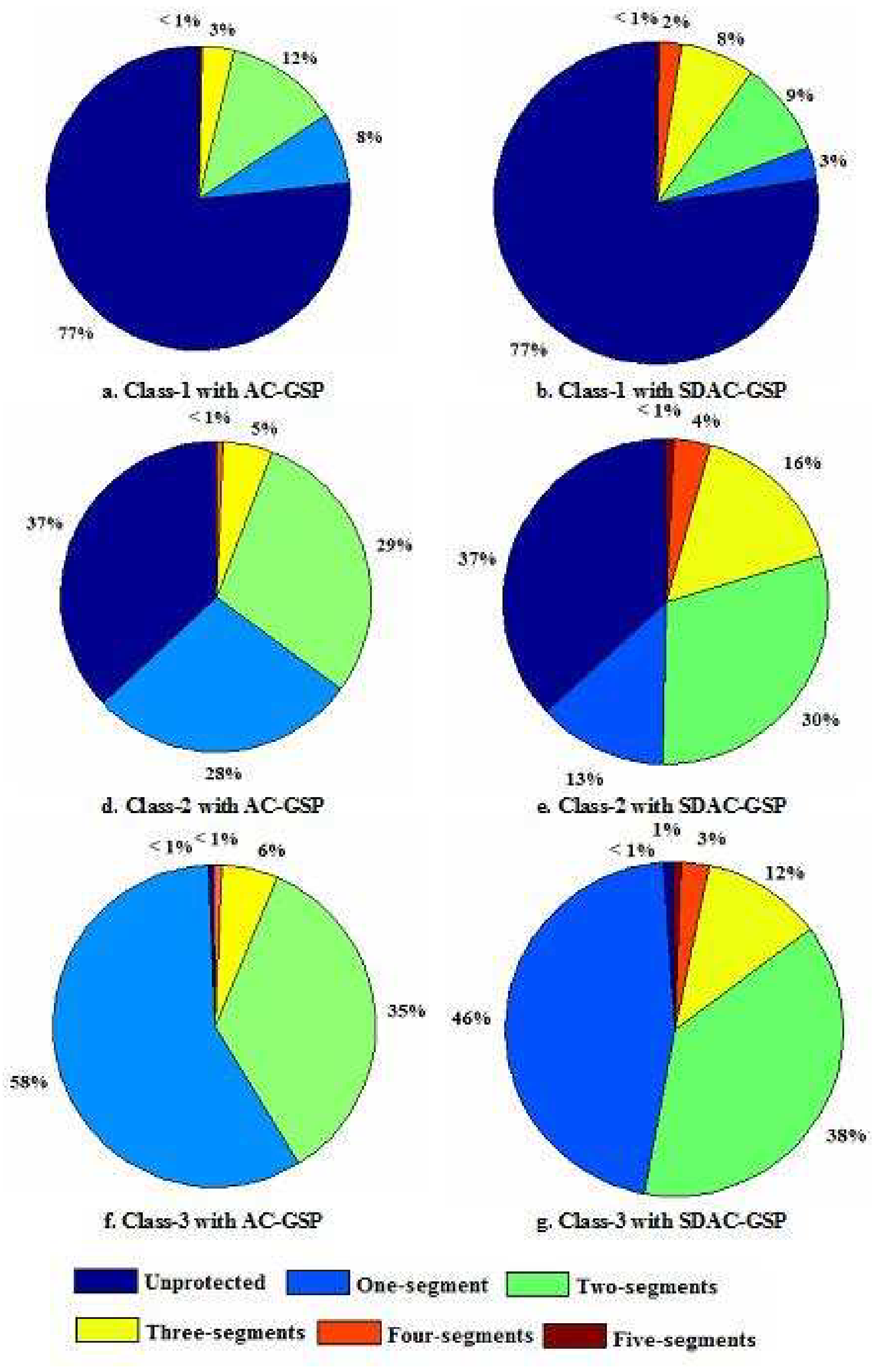


Figure 5.8: Average resource overbuild under AC-GSP and SDAC-GSP

and resource-scarce environment, respectively. As seen in the figures, SDAC-GSP leads to an increased number of utilized wavelength in the network, especially in the resource-plentiful environment. SDAC-GSP also leads to an enhanced resource utilization under resource-plentiful environment. However, in resource-scarce environment, as the network load gets heavier, both of the schemes get closer to each other in terms of resource overbuild due to the limited amount of resources under heavy loads.

Figure 5.9 illustrates the protection strategies of the provisioned connections in resource-plentiful environment. At first sight, the basic difference is on the number of protection segments. SDAC-GSP provisions a little portion of the connections with five segments. However, the maximum number of segments with AC-GSP is four for each availability class. As we have shown in the previous results, SDAC-GSP modifies the costs of the intersecting links by considering the sharing degree, and offers better availability to the connections. Therefore, figure also complies with the previously obtained results. As seen in Figure 5.9.a and Figure 5.9.b, majority of the conenctions from $class-1$ are unprotected. For $class-2$ connections, the portion for unprotected connections, the ones protected with one segment, the ones and protected with two segments have close ratios to each other. It is expected that a minor amount of $class-3$ connections are unprotected due to having the highest availability requirement. The figure complies with this presumption, and it is also seen that the majority of the connections are provisioned with one or two protection segments. It is worth noting that the amount of the connections provisioned with three protection



a. Class-1 with AC-GSP

b. Class-1 with SDAC-GSP

d. Class-2 with AC-GSP

e. Class-2 with SDAC-GSP

f. Class-3 with AC-GSP

g. Class-3 with SDAC-GSP

Figure 5.9: Protection strategies of connections in resource-plentiful environment under AC-GSP and SDAC-GSP

segments is significantly greater than the amount of those unprotected when both of the schemes run. Table 5.3 shows the results taken in resource-scarce environment to investigate the portions of the protection strategies under both schemes. The results are similar to those obtained under W=32. Based on this, it can be concluded that the protection type of a connections is not directly related to the resource restriction of the environment. In Table 5.3, U stands for the ratio of unprotected connections of the related class, and $n-S$ stands for the ratio of the connections that are protected by n backup segments in the corresponding availability class.

Table 5.3: Provisioning of connections according to their protection when W=16

Scheme	Availability Class	U	1-S	2-S	3-S	4-S	5-S
AC-GSP	Class-1	0.769	0.077	0.116	0.033	0.006	-
	Class-2	0.369	0.280	0.288	0.055	0.008	-
	Class-3	0.012	0.643	0.304	0.037	0.005	-
SDAC-GSP	Class-1	0.766	0.049	0.100	0.066	0.017	0.003
	Class-2	0.376	0.196	0.289	0.113	0.023	0.004
	Class-3	0.010	0.523	0.359	0.089	0.018	0.002

Based on the analysis and simulation results, it can be said that, SDAC-GSP is convenient to be deployed where connections are more probable to be blocked due to availability requirements, and AC-GSP is convenient to be deployed where connections are blocked also due to resource limitation while AC-GSP can be preferred in a resource restricted environment and under heavy traffic to provision more number of connection requests. Thus, AC-GSP is preferred to be used in resource-scarce environment while SDAC-GSP can be preferred for resource-plentiful environment for sake of enhanced availability for the connections.

6. CONCLUSION AND FUTURE DIRECTIONS

Routing and wavelength assignment in optical networks have been studied a lot in the literature. As survivable optical network design started to be considered, availability-aware connection provisioning have been a key issue for the robust design and planning of optical WDM networks. Basically, availability of a connection stands for the probability of a connection to be in the operating state at an arbitrary time. Due to the single, multi-failures, long switching durations to the backup paths, there might be connection service outages which lead to unavailability.

There are several previous works focusing on availability aware optical network design and connection provisioning. Majority of the schemes deal with availability-aware provisioning under DPP and SBPP. Since it is hard to come up with a single precise availability calculation method for a shared protection system, there are various availability analysis methods analyzing the availability of the connections that are protected by shared resources. Some of the availability analysis approaches are based on linear models while there are also Markovian models. Availability aware connection provisioning schemes attempt to guarantee high availability and / or SLA satisfaction by controlling resource consumption.

This thesis study has focused on availability aware connection provisioning for different protection schemes. As the first step, we have proposed a two-step connection provisioning scheme for availability design of optical networks. The proposed scheme is built on top of a previously proposed scheme which works under static traffic matrix and over-provisioned network. In the first step, it attempts to arrange the feasible sharing degree on the channels dynamically. Determination of the feasible sharing degree is done periodically by a tradeoff update function. The tradeoff update function uses the contradiction between connection unavailability and resource overbuild. The connections are routed over a multi-layered graph with respect to minimum unavailability target where each arc corresponds to a wavelength channel, and where the arc costs are assigned by taking the calculated feasible sharing degree into consideration. The second step of this scheme is the same as the second step of the scheme which forms a base for it. Starting from the least utilized fiber, each fiber is released together with the connections passing through it, and an alternate RWA configuration for the released connections is searched by not violating the former unavailability value. However, in the corresponding step, routing is done on a single-layered graph by considering the feasible sharing degree at the end of the first step. The second step assigns the wavelengths by starting from the least utilized wavelength on the selected optical link. Here, the sharing degree can be violated if a less utilized wavelength cannot be shared by the corresponding connection. The dynamic sharing scheme is evaluated and compared with the previously proposed scheme which forms a base for it. According to the simulation results under different topologies and traffic matrices, the dynamic sharing scheme seems to offer less unavailability to the connections. It causes an increase in the wavelength utilization. However, it still leads to a significantly less resource consumption than a DPP-based availability aware connection provisioning scheme does.

The design scheme in the first step has been modified to work under dynamic traffic environment as a matter of network planning under SBPP. The proposed scheme is named as *Global Shareability Surveillance (GSS)*. GSS monitors the network status periodically, and by running the tradeoff heuristic, it determines the feasible sharing degree on the channels of the fibers. An enhanced version of GSS is also proposed, namely *Link-By-Link Shareability Surveillance (LSS)* which collects information from the network, and constructs an ILP model based on those collected information. The output of the solution of the ILP model provides the feasible sharing degrees for the wavelength channels of each link. Performance of GSS and LSS is evaluated and compared to that of a conventional reliable connection provisioning scheme CAFES. The results show that the GSS and LSS lead to decrease in the connection unavailability in comparison to CAFES. Moreover, the decrease in unavailability under LSS is more significant when compared to that under GSS. The proposed schemes introduce an increase in resource overbuild due to many reasons discussed in the text, however, the increase is kept less than one unit of magnitude which is reasonable.

As the next step, differentiated availability has been considered where the connections arrive with pre-specified availability requirements in their SLAs. Markovian unavailability analysis is used which considers dual failure issue. Two connection provisioning schemes have been proposed which are the adapted versions of GSS and LSS to differentiated and resource restricted environment. The first one is named as Global Differentiated Availability-aware Connection Provisioning (G-DAP) which aims to estimate a feasible sharing degree for the wavelength channels on the links for each availability class. The second scheme is the adapted version of LSS, and it attempts to estimate a feasible sharing degree for each class on the channels of each link separately. This scheme is called Link-By-Link Availability Aware Differentiated Connection Provisioning (LBL-DAP). LBL-DAP constructs an ILP model and runs it periodically based on the collected data from the network to estimate the feasible sharing degrees on each link for each availability class. We have evaluated the performance of the proposed schemes G-DAP and LBL-DAP, and compared the performance to that of CAFES. The proposed schemes decrease the overall blocking probability and the blocking probability for the highest availability classes. G-DAP and LBL-DAP do not introduce higher resource overbuild and unavailability than those of CAFES. The reason for the better performance of the proposed schemes is that the intelligent route and wavelength selection based on the feedback collected from the network, considering the feasible sharing degrees. Obviously, LBL-DAP introduces the best performance due to considering each link and availability class separately in the ILP model.

The last part of the thesis focuses on shared segment protection. To the best of our knowledge, there is not a work for availability analysis in shared segment protection. Thus, we have proposed an availability calculation method for shared segment protection. According to the proposed availability analysis, a connection is said to be available if the protection domain of each link along its working path is available. the protection domain is defined as the link itself and its corresponding backup segments. Here, the contribution of the backup segments to the availability is affected by the size of the sharing group on the backup channels of the protection segment. The model is verified by simulation and used in the availability calculation of the incoming connections for the connection provisioning schemes that we have proposed for availability aware shared segment protection. We have modified and adapted a conventional segment selection scheme (Generalized Segment Protection-GSP) to support availability aware routing and wavelength assignment. The proposed scheme is called Availability Constrained Generalized Segment Protection (AC-GSP). We have derived another provisioning scheme which is a hybrid of G-DAP and AC-GSP. The proposed scheme is based on AC-GSP, however, it attempts to estimate a feasible sharing degree for each availability class on the links which are candidates to originate or end the protection segments by running the tradeoff heuristic periodically. It assigns appropriate costs to the corresponding links considering the estimated feasible sharing degree. The performance of the proposed schemes is evaluated and compared under resource plentiful and resource scarce environments in terms of connection availability, blocking probability, and resource consumption. It has been shown that SDAC-GSP is appropriate to be used in resource plentiful environment or in resource scarce environment under low and moderate load levels. On the other hand, AC-GSP performs better in resource scarce environment under heavy load levels.

This work is open to be extended for future studies. WDM-based availability aware concept can be extended to availability design of GMPLS and multi granular optical networks where optimal design of multi granular optical networks exist in the literature [100, 101] as a reference guide for this extension. Layer-1 virtual private networks (VPN) are also becoming attractive for the service providers and the enterprizes, and there are several works for the survivable design of Layer-1 VPNs [102, 103]. Availability design of Layer-1 VPNs seems to be an open issue for future extensions of availability design of optical WDM networks. As it is mentioned in the introduction, optical packet and burst switching seem to be the most attractive future services of optical networks. To the best of our knowledge, availability and optical packet/burst switching are not considered as a design constraint which seems to be an open issue for the researchers in this field.

REFERENCES

[1] **Mukherjee, B.**, 2006. *Optical WDM Networks*, Springer.

[2] **Ramaswami, R. and Sivarajan, K.**, 2002. *Optical Networks: A Practical Perspective*, Morgan Kaufmann Publishers, Inc., San Francisco, 2nd Ed.

[3] **Yao, S.**, **Yoo, S.J.B. and Dixit, S.**, 2001. All-optical packet switching: Challenges and opportunities, *IEEE Communications Magazine*, **39**, 142–148.

[4] **Chen, Y.**, **Qiao, C. and Yu, X.**, 2004. Optical burst switching: a new area in optical networking research, *IEEE Network*, June, **18(3)**, 16–23.

[5] **Ou, C.S. and Mukherjee, B.**, 2005. *Survivable Optical WDM Networks*, Springer.

[6] **Ramamurthy, S.**, **Shasrabuddhe, L.**, **and Mukherjee, B.**, 2003. Survivable WDM Mesh Networks, *IEEE Journal on Lightwave Technology*, **21**, 870–883.

[7] **Chauban, S.**, **Anand, V. and Qiao, C.**, 2001. *Sub-Path Protection: A new framework for Optical Layer Survivability and Its Quantitative Evaluation*, Buffalo NY, Tech Rep.

[8] **Stamatelakis, D. and Grover, W.D.**, 2000. Theoretical underpinnings for the efficiency of restorable networks using preconfigured cycles (p-cycles), *IEEE Journal on Lightwave Technology*, August, **48 no 8**.

[9] **Shooman, M.L.**, 2002. *Reliability of Computer Systems and Networks: Fault Tolerance, Analysis, and Design*, Wiley InterScience.

[10] **Stamatelakis, D. and Grover, W.**, 2000. Bridging the ring-mesh dichotomy with p-cycles, Design of Reliable Communication Networks (DRCN), Workshop on, IEEE, pp. 92–104.

[11] **Tornatore, M.**, **Maier, G. and Pattavina, A.**, 2006. Availability Design of Optical Transport Networks, *IEEE Journal on Selected Areas in Communications*, December, **24**, 1520–1532.

[12] **Clouqueur, M. and Grover, W.**, 2002. Availability analysis of span restorable mesh networks, *IEEE Journal on Selected Areas in Communications*, May, **20 no 4**, 810–822.

[13] **Clemente, R.**, **Bartoli, M.**, **Bossi, M.**, **D'Orazio, G. and Cosmo, G.**, 2005. Risk Management in Availability SLA, International Workshop on Design of Reliable Communication Networks (DRCN), IEEE, October.

[14] **Ehrhardt, A.**, 2007. Next Generation Optical Networks and New Services: an Operatorś Point of View, International Conference on Transparent Optical Networks (ICTON), IEEE, June, volume 1, pp. 323–326.

[15] **International Telecommunications Union, G.709**, [Online], *<http://www.itu.int/rec/T-REC-G.709/e>, 2008, August*.

[16] **Arci, D.**, **Pattavina, A. and Petecchi, D.**, 2003. Availability Models for Protection Techniques in WDM Networks, Design of Reliable Communication Networks (DRCN), Workshop on, IEEE, October, pp. 158–166.

[17] **Mukherjee, D.S.**, **Assi, C. and Agarwal, A.**, 2006. An Alternative Approach for Enhanced Availability Analysis and Design Methods in p-cycle-Based Networks, *IEEE Journal on Selected Areas in Communications*, December, **24**, 23–34.

[18] **Ho, P.H.**, **Mouftah, H.T. and Haque, A.**, 2007. Availability-Constrained shared backup path protection (SBPP) for GMPLS-Based spare capacity reconfiguration, IEEE International Conference on Communications (ICC), IEEE, June, pp. 2186–2191.

[19] **Babbit, J. and Best, R.**, 2006. Maintaining availability in an optical backbone network, Optical Fiber Communication Conference (OFC) and National Fiber Optics Engineers Conference.

[20] **Lackovic, M. and Mikac, B.**, 2003. Analytical vs. simulation approach to availability calculation of circuit switched optical transmission network, International Conference on Telecommunications (ConTEL), June, pp. 743–750.

[21] **Zhang, J.**, **Zhu, K.**, **Zang, H. and Mukherjee, B.**, 2003. A new provisioning framework to provide availability-guaranteed service in WDM mesh networks, International Conference on Communications, IEEE, volume 2, pp. 1484–1488.

[22] **Cavdar, C.**, **Song, L.**, **Tornatore, M. and Mukherjee, B.**, 2007. Holding-Time-Aware and Availability-Guaranteed Connection Provisioning in Optical WDM Mesh Networks, International Symposium on High Capacity Optical Networks and Enabling Technologies, IEEE, November.

[23] **Al-Sukhni, E. and Mouftah, H.T.**, 2008. A Novel Distributed Availability-Aware Provisioning Framework for Differentiated Protection Services in Optical Mesh Networks, Canadian Conference on Electrical and Computer Engineering (CCECE), IEEE, May, pp. 1553–1558.

[24] **Al-Sukhni, E. and Mouftah, H.T.**, 2008. A Novel Distributed Destination Routing Based Availability-Aware Provisioning Framework for Differentiated Protection Services in Optical Mesh Networks, IEEE Symposium on computers and Communications (ISCC), July.

[25] **Song, L. and Mukherjee, B.**, 2007. Impacts of Multiple Backups and Multi-Link Sharing among Primary and Backups for Dynamic Service Provisioning in Survivable Mesh Networks, Optical Fiber Communication and the National Fiber Optic Engineers Conference, (OFC/NFOEC), IEEE, March, pp. 1–3.

[26] **Rai, S.**, **Deshpande, O.**, **Ou, C.**, **Martel, C.U. and Mukherjee, B.**, 2007. Reliable multipath provisioning for high-capacity backbone mesh networks, *IEEE/ACM Transactions on Networking*, August, **15 issue 4**, 803–8012.

[27] **Clouqueur, M. and Grover, W.**, 2005. Availability analysis and enhanced availability design in p-cycle-based networks, *Springer Science Photonic Network Communications*, July, **10:1**, 55–71.

[28] **Ge, C.**, **Lian, Z.**, **Sun, X. and Zhang, M.**, 2006. Design for WDM rings based on differentiated path availability, *Springer Science Photonic Network Communications*, June, **13 no 1**, 13–18.

[29] **Piletstys, R. and Siurkus, A.**, 2006. Information transmission availability in WDM networks, International Conference on Information Technology Interfaces, IEEE, June, pp. 639–644.

[30] **Koster, A.M.C.A.**, 2006. Cost-Efficient Transparent Optical Networks with High Connection Availabilities, International Conference on Transparent Optical Networks (ICTON), IEEE, June, volume 3, pp. 101–104.

[31] **Wosinska, L. and Held, M.**, 2004. Optimization of optical networks: price and value of reliability, International Conference on Transparent Optical Networks (ICTON), IEEE, July.

[32] **Jaeger, M.**, 2007. Service Availability in Optical Network Design, Optical Fiber communication/National Fiber Optic Engineers Conference,(OFC/NFOEC), IEEE, March, pp. 1–3.

[33] **Xu, D.**, **Xiong, Y. and Qiao, C.**, 2003. Novel algorithms for shared segment protection, *IEEE Journal on Selected Areas in Communications*, October, **21 no 8**.

[34] **Ou, C.**, **Rai, S. and Mukherjee, B.**, 2005. Extension of Segment Protection for Bandwidth Efficiency and Differentiated Quality of Protection in Optical/MPLS Networks, *Optical Switching and Networking*, January, **1**, 19–33.

[35] **Zhemin, D. and Hamdi, M.**, 2003. *Optical Network Resource Management and Allocation. The Handbook of Optical Communication Networks*, Ch 9, Eds, Ilyas M., Mouftah H., CRC Press, New York.

[36] **Chen, L.P.**, **Shi, C.X.**, **Shinta, M.**, **Kamata, H.**, **Nakamura, S.**, **Chen, J. and Cvijetic, M.**, 2000. A novel bi-directional wavelength path switched ring (BWPSR): principle and experiment, Optical Fiber Communication Conference (OFC), IEEE, March, volume 1, pp. 243–245.

[37] **Doucette, J.**, 2006. Joint working and spare capacity design of node-inclusive span-restorable optical networks, Optical Fiber Communication Conference (OFC), IEEE, March, volume 1, p. 10pp.

[38] **Uzunpostalci, O.F.**, 2006, **P-Cycles: Survivability in Optical WDM Networks, M.Sc Thesis**, istanbul Technical University.

[39] **Saradhi, C.V. and Murthy, C.S.R.**, 2003. Segmented protection paths in WDM networks, Worshop on High Performance Switching and Routing (HPSR), IEEE, June, volume 1, pp. 311–316.

[40] **Gummadi, K.P.**, **Pradeep, M.J. and Murthy, C.S.R.**, 2003. An efficient primary-ed backup scheme for dependable real-time communication in multihop networks, *IEEE/ACM Transactions on Networking*, February, **11**, 81–94.

[41] **Ho, P.H.**, **Tapolcai, J. and Cinkler, T.**, 2004. Segment Shared Protection in Mesh Communication Networks With Bandwidth Guaranteed Tunnels, *IEEE/ACM Transactions on Networking*, December, **12 no 6**, 1105–1118.

[42] **Grover, W.**, **Doucette, J.**, **Clouqueur, M.**, **Leung, D. and Stamatelakis, D.**, 2002. New Options and Insights for Survivable Transport Networks, *IEEE communications Magazine*, January, **40 no 1**, 34–41.

[43] **Grover, W.D. and Kodian, A.**, 2005. Failure independent path protecting p-cycles: efficient and simple fully preconenected optical-path protection, *IEEE Journal of Lightwave Technology*, October, **Volume 23 issue 10**, 3241–3259.

[44] **Wang, H. and Mouftah, H.T.**, 2005. P-cycles in multi-failure network survivability, International Conference on Transport Optical Networks (ICTON), IEEE, July, pp. 381–384.

[45] **Mukherjee, D.S.**, **Assi, C. and Agarwal, A.**, 2006. Alternate strategies for dual failure restoration using p-cycles, International Conference on Communications (ICC), IEEE, June, volume 6, pp. 2477–2482.

[46] **Lin, R.**, **Wang, S.**, **Li, L. and Guo, L.**, 2005. A New Network Availability Algorithm for WDM Optical Networks, International Conference on Computer and Information Technology (CIT), IEEE, September, pp. 480–484.

[47] **Snow, A.P. and Weckman, G.R.**, 2007. What Are the Chances an Availability SLA will be Violated, International Conference on Networking, IEEE, April, pp. 35–35.

[48] **Seeman, G.**, 2008. Designing Networks with the Optimal Availability, Optical Fiber communication/National Fiber Optic Engineers Conference,(OFC/NFOEC 2008), IEEE, February.

[49] **Pandi, Z.**, **Tacca, M.**, **Fumagalli, A. and Wosinska, L.**, 2006. Dynamic Provisioning of Availability-Constrained Optical Circuits in the Presence of Optical Node Failures, *IEEE Journal of Lightwave Technology*, September, **24 no 9**, 3268–3279.

[50] **Grover, W.D.**, 1999. High avaialbility path design in ring-based optical networks, *IEEE/ACM Transactions on Networking*, August, **7 no 4**, 558–574.

[51] **Schupke, D.A.**, 2000. Reliability models of WDM self-healing rings, International Workshop on Design of Reliable Communication Networks (DRCN), April.

[52] **Benlarbi, S.**, 2006. Estimating SLAs Availability/Reliability in Multi-services IP Networks, *Springer Lecture Notes in Computer Science*, December, **4328/2006**, 30–42.

[53] **Clouqueur, M. and Grover, W.**, 2000. Computational and design studies on the unavailability of mesh-restorable networks, International Workshop on Design of Reliable Communication Networks (DRCN), April, pp. 181–186.

[54] **Tacca, M.**, **Fumagalli, A.**, **Paradisi, A.**, **Unghvary, F.**, **Gadhiraju, K.**, **Lakshmanan, S.**, **Rossi, S.M.**, **de Campos Sachs, A. and Shah, D.S.**, 2003. Differentiated reliability in optical networks: Theoretical and practical results, *IEEE Journal of Lightwave Technology*, November, **21 no 11**, 2576–2586.

[55] **Song, L.**, **Zhang, J. and Mukherjee, B.**, 2007. Dynamic Provisioning with availabiltiy guarantee for differentiated services in survivable mesh networks, *IEEE journal on Selected Areas in Communications*, April, **25**, 35–43.

[56] **Huang, Y.**, **Wen, W.**, **Zhang, J.**, **Heritage, J.P. and Mukherjee, B.**, 2004. A new link state availability model for reliable protection in optical WDM networks, International Conference on Communications (ICC), IEEE, June, volume 3, pp. 1649–1653.

[57] **Mello, D.A.**, **Schupke, D.**, **Scheffel, M. and Waldman, H.**, 2005. Availability Maps for connections in optical networks, International Workshop on Design of Reliable Communication Networks (DRCN), IEEE, October, p. 8pp.

[58] **Velasco, L.**, **Spadaro, S.**, **Comellas, J. and Junyent, G.**, 2006. Failure aware diverse routing: A novel algorithm to improve availability in ASON/GMPLS networks, International Conference on Transport Optical Networks (ICTON), IEEE, June, volume 3, pp. 195–198.

[59] **Dobbelaere, P.D.**, **Falta, K. and Gloeckner, S.**, 2003. Advances in integrated 2D MEMS-based solutions for optical networks applications, *IEEE Communications Magazine*, May, **Volume 41 issue 5**, 16–23.

[60] **Verbrugge, S.**, **Demester, D.C.P.**, **Huelsermann, R. and Jaeger, M.**, 2005. General Availability Model for Multilayer Transport Networks, Design of Reliable Communication Networks (DRCN), Workshop on, IEEE, pp. 85–92.

[61] **Machuca, C.M.**, **Moe, O. and Jaeger, M.**, 2008. Impact of protection schemes and network components availability on operational expenditures, *OSA Journal of Optical Networking*, February, **7 no 2**, 142–150.

[62] **Ou, C.**, **Zhang, J.**, **Zhang, H.**, **Sahasrabuddhe, L.H. and Mukherjee, B.**, 2004. New and improved approaches for shared-path protection in wdm mesh networks, *IEEE Journal of Lightwave Technology*, May, **Volume 22**, 1223–1232.

[63] **Zhou, L.**, **Marcel, H. and Woskinska, L.**, 2004. Analysis and optimization of connection availabilities in optical networks with different protection strategies, SPIE Photonics Eur., September, volume 5465, pp. 157–167.

[64] **Wosinska, L.**, 2006. Connection Availability in WDM Mesh Networks with Multiple Failures, International Conference on Transport Optical Networks (ICTON), IEEE, June, volume 3, pp. 126–129.

[65] **Zhou, L.**, **Held, M. and Sennhauser, U.**, 2007. connection availability analysis of shared backup path-protected mesh networks, *IEEE Journal of Lightwave Technology*, May, **25 no 5**, 1111–1119.

[66] **Held, M. and Zhou, L.**, 2006. Redundancy, Restorability and Path Availability in Optical Mesh Networks, International Conference on Transparent Optical Networks (ICTON), IEEE, June, volume 3, pp. 18–22.

[67] **Mello, D.A.A.**, **Schupke, D. and H.Waldman**, 2005. A Matrix-Based Analytical Approach to Connection Unavailability Estimation in Shared Backup Path Protection, *IEEE Communication Letters*, September, **Volume 9 no 9**, 844–846.

[68] **Mello, D.A.A.**, **Pelegrini, J.U.**, **Ribeiro, R.P.**, **Schupke, D.A. and Waldman, H.**, 2005. Dynamic provisioning of shared-backup path protected connections with guaranteed availability requirements, International Conference on Broadband Networks (BROADNETS), IEEE, October, volume 2, pp. 1320–1327.

[69] **Tornatore, M.**, **Maier, G. and Pattavina, A.**, 2006. Capacity versus availability trade-offs for availability-based routing, *OSA Journal of Optical Networking*, November, **5**, 858–869.

[70] **Bhandari, B.**, 1998. *Survivable Networks: Algorithms for Diverse Routing*, Kluwer Academic Publishers.

[71] **Mykkeltveit, A. and Helvik, B.E.**, 2008. Comparison of Schemes for Provision of Differentiated Availability-Guaranteed Services Using Dedicated Protection, International Conference on Networking (ICN 2008), IEEE.

[72] **Tornatore, M.**, **Canhui, O.**, **Zhang, J.**, **Pattavina, A. and Mukherjee, B.**, October 2005. Photo: an efficient shared-path-protection strategy based on connection holding- time awareness, *IEEE Journal of Lightwave Technology*, **23**, 3138–3146.

[73] **Tornatore, M.**, **Lucerna, D.**, **Song, L.**, **Mukherjee, B. and Pattavina, A.**, 2008. SLA Redefinition for Shared-Path-Protected Connections with Known Duration, Optical Fiber communication/National Fiber Optic Engineers Conference (OFC/NFOEC 2008), IEEE, February, pp. 1–3.

[74] **Wei, X.**, **Guo, L.**, **Wang, X.**, **Song, Q. and Li, L.**, 2008. Availability guarantee in survivable WDM mesh networks: A time perspective, *Elsevier Information Sciences*, June, **178 issue 11**.

[75] **Zhang, J.**, **Zhu, K.**, **Zhang, H.**, **Matloff, N.S. and Mukherjee, B.**, 2007. Availability-Aware Provisioning Strategies for Differentiated Protection Services in Wavelength-Convertible WDM Mesh Networks, *IEEE/ACM Transactions on Networking*, October, **15**, 1177–1190.

[76] **Zhang, J.**, **Zhu, K. and Mukherjee, B.**, 2003. Service Provisioning to provide per-connection-based availability guarantee in optical WDM networks, Optical Fiber Communication Conference (OFC), pp. 622–624.

[77] **Zhang, J.**, **Zhu, K. and Mukherjee, B.**, 2004. A comprehensive study on backup repositioning to remedy the effect of multiple-link failures in WDM Mesh Networks, International conference on Communications (ICC), IEEE, June, pp. 1654–1658.

[78] **Huang, Y.**, **Heritage, J.P. and Mukherjee, B.**, 2004. Availability-guaranteed service provisioning with shared path protection in optical WDM networks, Optical Fiber Communicaiton Conference (OFC), IEEE.

[79] **Huang, Y.G.**, **Wen, W.**, **Heritage, J.P. and Mukherjee, B.**, 2004. A New Protection Model to Provide Availability-Guaranteed Service for Reliable Optical WDM Networks, *Springer Lecture Notes in Computer Science*, January, **2918/2004**, 372–382.

[80] **Mykkeltveit, A. and Helvik, B.E.**, 2008. On provision of availability guarantees using shared protection, International Conference on Optical Network Design and Modeling (ONDM), IEEE, March, pp. 1–6.

[81] **Ma, H.**, **Fayek, D. and Ho, P.H.**, 2007. Availability-Aware Multiple Working-Paths Capacity Provisioning in GMPLS Networks, *Springer Lecture Notes in Computer Science*, November, **4786/2007**, 85–94.

[82] **Zhang, J.**, 2005. Architecture and Algorithms for Fault Management in Optical WDM Networks, Ph.D. thesis, University of California, Davis, *ISBN:0-542-08607-7*.

[83] **Kantarci, B.**, **Mouftah, H.T. and Oktug, S.**, 2008. Arranging Shareability Dynamically for the Availability-Constrained Design of Optical Transport Networks, IEEE Symposium on Computers and Communications (ISCC), IEEE, July.

[84] **Willems, G.**, **Arijs, P.**, **Parys, W.V. and Demeester, P.**, 2003. Capacity vs. availability trade-offs in mesh-restorable WDM networks, International Workshop on Design of Reliable Communication Networks (DRCN), pp. 158–166.

[85] **Doucette, J.**, **Clouqueur, M. and Grover, W.D.**, 2003. On the availability and capacity requirements of shared backup path-protected mesh networks, *SPIE Optical Networks Magazine*, November, **4 no 6**, 29–44.

[86] **Song, L.**, 2007. Design and analysis of survivable telecom mesh networks, Ph.D. thesis, University of California, Davis, *AAT 3303206 Available: <http://proquest.umi.com>,2008, August*.

[87] **Tornatore, M.**, **Maier, G.**, **Pattavina, A.**, **Villa, M.**, **Righetti, A.**, **Clemente, R. and Martinelli, M.**, 2003. Availability optimization of static path-protected WDM networks, Optical Fiber communications Conference(OFC), IEEE, March, pp. 621–622.

[88] **Miyso, Y. and Saito, H.**, 1998. Optimal design and evaluation of survivable wdm transport networks, *IEEE Journal on Selected Areas in Communications*, September, **16**, 1190–1198.

[89] **Segovia, J.**, **Calle, A. and Vila, P.**, 2008. Availability Analysis of GMPLS Connections based on Physical Network Topology, International Conference on Optical Network Design and Modeling (ONDM), IEEE, March, pp. 1–6.

[90] **Maesschalck, S.**, **Colle, D.**, **Lievens, I.**, **Pickavet, M.**, **Demeester, P.**, **Mauz, C.**, **Jaeger, M.**, **Inkret, R.**, **Mikac, B. and Derkacz, J.**, 2003. Pan-european optical transport networks: An availability-based comparison, *Springer-Photonic Network Communications*, May, **5**, 203–225.

[91] **Kantarci, B.**, **Mouftah, H.T. and Oktug, S.**, 2008. Connection Provisioning with Feasible Shareability Determination for Availability-Aware Design of Optical Networks, International Conference on Transparent Optical Networks (ICTON), IEEE, June, volume 3, pp. 63–66.

[92] **ILOG Optimization Suite**, [Online], *<http://www.ilog.com>, 2008, September*.

[93] **Kantarci, B.**, **Mouftah, H.T. and Oktug, S.**, 2008. Differentiated Availability-Aware Connection Provisioning in Optical Transport Networks, Global Communications Conference (GLOBECOM), IEEE, December.

[94] **Kantarci, B.**, **Mouftah, H.T. and Oktug, S.**, 2009. Adaptive Schemes for Differentiated Availability-Aware Connection Provisioning in Optical Transport Networks, *IEEE Journal on Lightwave Technology*, accepted to be published in, *<http://www.ieee.org/ieeexplore>*.

[95] **Kantarci, B.**, **Mouftah, H.T. and Oktug, S.**, 2008. Availability Analysis and Connection Provisioning in Overlapping Shared Segment Protection for Optical Networks, International Symposium on Computer and Information Systems (ISCIS), IEEE, November.

[96] **Ou, C.**, **Zang, H.**, **Singhal, N. and Mukherjee, B.**, 2004. Subpath protection for scalability and fast recovery in optical WDM mesh networks, *IEEE J. on Sel. Areas in Communications*, November, **22 no 9**, 1859–1875.

[97] **Ouyang, Y.**, **Zeng, Q. and Wei, W.**, 2006. Segment protection algorithm based on an auxiliary graph for wavelength-division multiplexing optical networks, *Journal of Optical Networking*, **5**, 15–25.

[98] **Tornatore, M.**, **Carcagni, M.**, **Mukherjee, B.**, **Ou, C. and Pattavina, A.**, 2006. Efficient shared-segment protection exploiting the knowledge of connection holding time, Global Telecommunications Conference, IEEE, pp. 1–5.

[99] **Tornatore, M.**, **Carcagní, M.**, **Ou, C.S.**, **Mukherjee, B. and Pattavina, A.**, 2008. Intelligent shared-segment protection, *Elsevier Computer Networks*, July, **52 issue 10**, 1965–1974.

[100] **Naas, N. and Mouftah, H.T.**, 2006. Optimum Planning of GMPLs Transport Networks, International Conference on Transparent Optical Networks (ICTON), IEEE, June, volume 3, pp. 70–73.

[101] **Cao, X.**, **Anand, V. and Qiao, C.**, 2007. Waveband switching for dynamic traffic demands in multigranular optical networks, *IEEE/ACM Transactions on Networking*, August, **15 Issue 4**, 957–968.

[102] **Yayimli, A.G.**, 2009. Selective survivability with disjoint nodes and disjoint lightpaths for layer 1 VPN, *Elsevier Optical Switching and Networking*, January, **6 no 1**, 3–9.

[103] **Cavdar, C.**, **Yayimli, A.G. and Mukherjee, B.**, 2008. Multi-Layer Resilient Design for Layer-1 VPNs, Optical Fiber communication/National Fiber Optic Engineers Conference,(OFC/NFOEC 2008), IEEE, February, pp. 1–3.

[104] **Ramamurthy, R.**, **Labourdette, J.F.**, **Akyamach, A. and Chaudhury, S.**, 2003. Limiting sharing on protection channels in mesh optical networks, Optical Fiber Communication Conference (OFC), IEEE, pp. 204–205.

APPENDICES

APPENDIX A: Bhandari's Algorithm
APPENDIX B: ACPRO Pseudocode and explanation
APPENDIX C: Simulation Environment
APPENDIX D: The basis scheme for AC-GSP and SDAC-GSP: Generalized Segment Protection (GSP) Algorithm
APPENDIX E: Performance of the adaptive schemes , G-DAP and LBL-DAP under uniformly distributed SLA-classes
APPENDIX F: Blocking probability for AC-GSP and SDAC-GSP for a different epsilon value

APPENDIX A: Bhandari's Algorithm

In MCAD-DPP Bhandari's one-step diverse path search algorithm [70] is used together with the two-step Dijkstra's algorithm [11]. In our work (Chapter 3), two-step Dynamic Sharing, we have also used MCAD-DPP as a reference to evaluate the connection unavailability and the wavelength utilization of our proposed scheme. Therefore, in this section we give a brief definition of the Bhandari's one-step shortest path search algorithm which is not commonly deployed as Dijkstra's shortest path algorithm. The pseudocode for the algorithm can be seen in Algorithm 1.

Algorithm 1 Bhandari's algorithm

```
{INPUT}
{N: Set of nodes in the network}
{E: Set of unidirectional links}
{C: Cycle of minimum cost consisting of links}
$P1 \leftarrow Shortest path from S to D$
for $i$=1 to $|N|$ do
    for $j$=1 to $|N|$ do

        if $e_{ij} \in P1$ then
            $e_{ij} \leftarrow \infty$
            $e_{ji} \leftarrow -e_{ji}$
        end if
    end for
end for
$P2 \leftarrow Shortest path from S to D$
for $i$=1 to $|N|$ do
    for $j$=1 to $|N|$ do
        if $e_{ij} \in P1$ AND $e_{ji} \in P2$ then
            $P1 \leftarrow P1 - \{e_{ij}\}$
            $P2 \leftarrow P2 - \{e_{ji}\}$
        end if
    end for
end for
$C \leftarrow \{P1\} \cup \{P2\}$
```

The algorithm above starts the cycle search by calculating the shortest path, $P1$, between the source and the destination node. Upon finding the shortest path, it sets the costs of the links on the found path to infinity, and negates the costs of the links which are in the opposite directions to those links. As the second step, by using the modified topology, it computes another path, $P2$ consisting of set of links. Once $P1$

and *P*2 are obtained, the links on which *P*1 and *P*2 intersect in reverse directions are removed from the two sets. Finally the remaining parts of the two sets are merged and the links in the union set form a cycle that passes through the source and destination.

APPENDIX B: ACPRO Pseudocode and explanation

In Chapter 3, the second step of our our proposed scheme (Dynamic Sharing-2) is built on top of the second step of the MCAD/ACPRO approach which was proposed in [11]. In Chapter 3, we define our proposed scheme in details, however, it is worth to include the pseudocode of the second step of its counterpart in this section.

Algorithm 2 ACPRO (X(f),M)

```
{Input}
{$\Omega_{MCAD}[X(f)]$: MCAD Result Set}
{$M$: Tolerance margin}
{Output}
{$ACPRO[X(f)]$: ACPRO Result Set}
$K \leftarrow 0$
while $K < W - 1$ do
    {Remove Empty Fibers}
    $K \leftarrow K + 1$
    while any K-fibers exist do
        {Store $\Omega_{MCAD}[X(f)]$}
        $U_1 \leftarrow U\{\Omega_{MCAD}[X(f)]\}$
        {Deallocate X(f)}
        {Disable f temporarily}
        if alternate configuration ($\Omega^*$) exists then
            $U_2 \leftarrow U\{\Omega[X(f)]\}$
            if $U_2 > M \cdot U_1$ then
                {Restore $\Omega[X(f)]$}
            else
                $\Omega[X(f)] \leftarrow \Omega^*[X(f)]$
            end if
        else
            {Restore $\Omega[X(f)]$}
        end if
    end while
end while
```

In the *ACPRO* pseudocode, K stands for a counter and a $K - fiber$ stands for a fiber that has K allocated WDM channels. Currently processed fiber is represented by f. W is the number of WDM channels per fibers. $X(f)$ represents the set of connections either their working or protection path passes through. $\Omega[X(f)]$ stands for the particular RFWA solutions for the connections in $X(f)$. The unavailability values for the RFWA solutions of the connections in $X(f)$ is represented by $U\{\Omega[X(f)]\}$. ACPRO attempts to search for an alternate RFWA solution for the connections passing on each fiber by keeping the connection unavailability in a feasible range.

APPENDIX C: Simulation environment

Simulation Structure

We have developed our simulation environment by using Visual C++ using the discrete event simulation methodology. The main objects of the simulation environment are *event*, *topology*, *link*, *fiber*, *channel*, and *connection*.

An event can be `connection_arrival()`, `connection_release()`, `link_failure()`, `link_repair()`. Each event has a timestamp and a corresponding event code. Events are kept in a queue, eventQueue sorted by their timestamps.

When the simulation starts, a connection arrival event is generated at time zero, and pushed into the eventQueue. As the connection is generated and pushed into the queue, immediately its release time is calculated and an appropriate event for that is generated and pushed into the queue. Then the simulation starts running in its main loop. The pseudocode for the main loop in the simulation is shown in Algorithm 3. Each event object in the eventQueue occurs with its timestamp. Since the simulations run in discrete time, the global clock of the simulation, *CurrentTime* is updated each time an event is popped from the queue.

Algorithm 3 Main Loop

```
while $arrivals < totalConnections$ AND $eventQueue$ NOT EMPTY do
    $nextEvent \leftarrow eventQueue.getNextEvent()$
    $CurrentTime \leftarrow nextEvent.time$
    if $nextEvent.eventType = arrival$ then
        $releaseCon \leftarrow newEvent()$
        $nextArrive \leftarrow newEvent()$
        $eventQueue.push(releaseCon)$
        $eventQueue.push(nextArrive)$
    end if
    if $nextEvent.eventType = failure$ then
        $repairLink \leftarrow newEvent()$
        $nextFailure \leftarrow newEvent()$
        $eventQueue.push(repairLink)$
        $eventQueue.push(nextFailure)$
    end if
    $runprocessEvent()$
end while
```

The *topology* includes two main matrices, namely the distance matrix (*DM*), and the link cost matrix (*CM*) containing the distance between the nodes and the link costs which corresponds to the unavailability value of a single WDM channel in our simulations respectively. The main objects of the simulation environment are the *link*, *fiber*, *channel*, and *connection* objects. In Figure C.1, the main properties and the functions of these classes, and the relation between them can be seen.

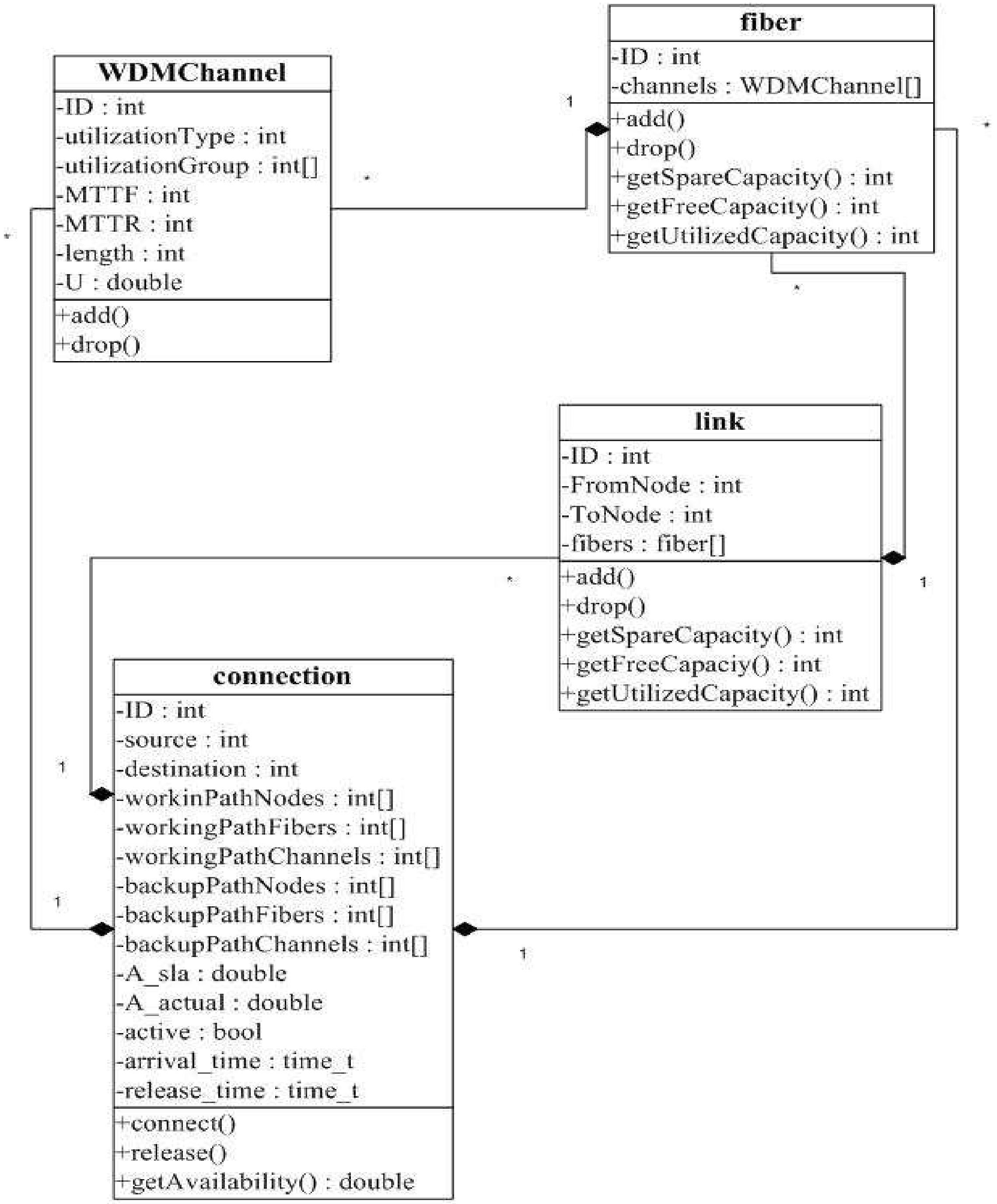


Figure C.1: Optical link, fiber, channel, and connection structures with main properties and functions

An object from the *link* class consists of several objects from the *fiber* class. Similarly a *fiber* consists of several channels. The property of the class *channel* named as *uType* stands for the utilization type of the corresponding channel, i.e unutilized, working channel, or backup channel. Thus, $utilizingGroup$ is a vector of the ID(s) of the connection(s)that utilize(s) the corresponding channel. $MTTF$, $MTTR$, $length$, U stand for the mean time to fail, mean time to repair, length and the unavailability of the corresponding channel respectively. The main functions of a WDM channel are defined as adding or dropping a function. A link and a fiber have extra functions to get their spare, free, and total utilized capacities. A connection has its working and backup path information in the related vectors. For the simulations run under shared segment protection, properties related to each backup segment are added to the connection class.

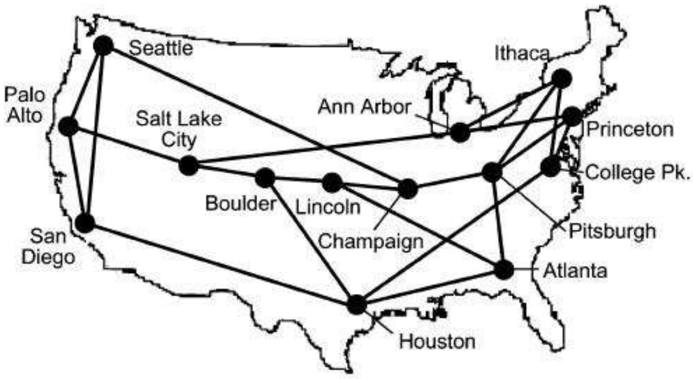


Figure C.2: NSFNET topology used in the simulations (Tornatore, 2006)

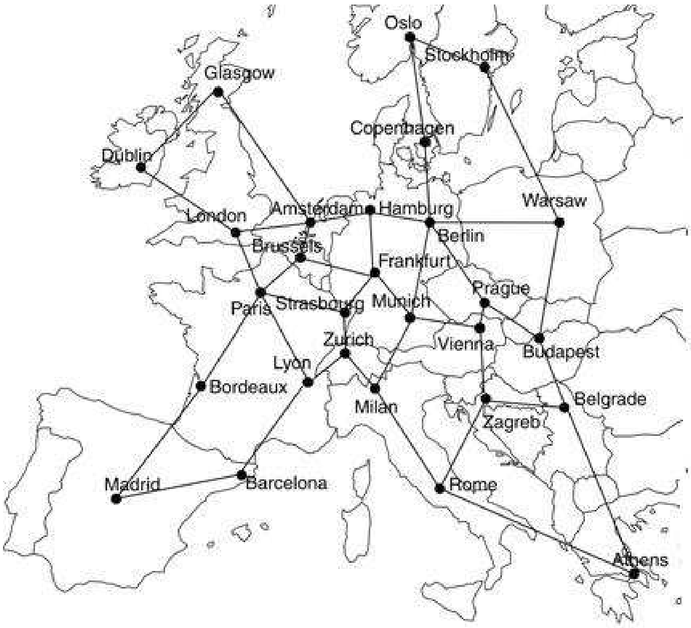


Figure C.3: 28-node European Optical Network topology used in the simulations (Maesschalck, 2003)

In the simulations for DPP and SBPP we use the 14-node NSFNET and the 28-node European Optical Network topologies that are shown in Figure C.2 and Figure C.3 respectively. The length of the links are assigned as the distances between cities in kilometers. In the simulations run under shared segment protection, we require a larger and more heterogeneous topology to be able to provision each connection with more than one segment so we use the topology in Figure C.4.

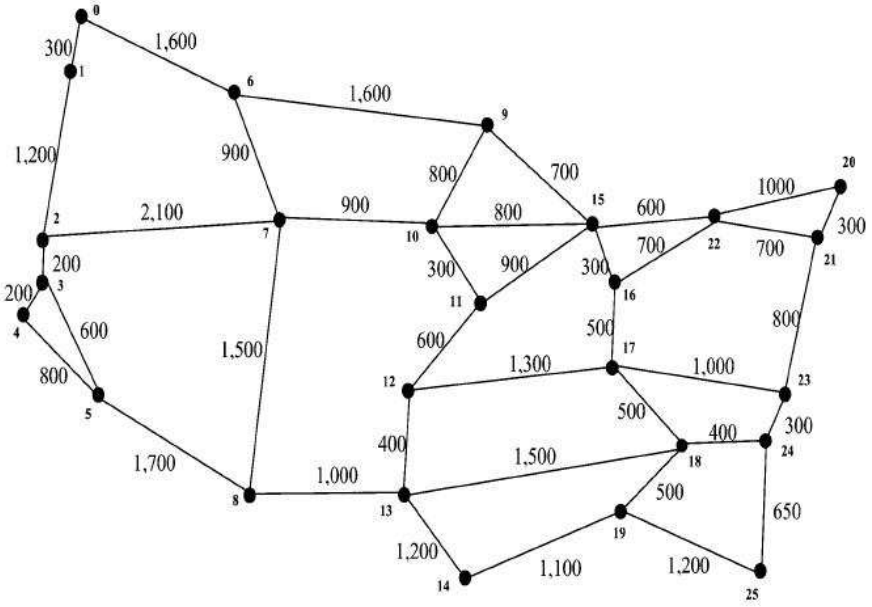


Figure C.4: US nationwide topology used when testing the performance of the segment protection-based schemes (Zhang, 2007)

Feasible Sharing Degree Update

In Dynamic Sharing-Step-1, GSS, G-DAP and SDAC-GSP our proposed schemes attempt to define feasible sharing degrees on the channels. Dynamic Sharing-Step-1 and GSS are the connection provisioning schemes for availability aware network planning. Thus, the connections are attempted to be provisioned with high availability and low resource consumption, i.e non-differentiated SLAs. The pseudocode for $updateTradeoff()$ function is given below. The algorithm runs in Dynamic Sharing-Step-1 and GSS. The tradeoff update approach is adopted from the network availability arrangement in [46]. Here, we aim to arrange the shareability on the channels. In [104], the authors propose to limit the sharing degree around six. According to [104], a well selected sharing limit eliminates the capacity penalties. Therefore, relying on the sharing degree of six as a reference; to allow the system oscillate freely between different sharing degrees, we do not specify a strict sharing limit but set an upper bound ($UPPERBOUND$) of eight which is close to but even more than the proposed value in the related reference, for the global feasible sharing degree in order to avoid the corresponding value ($S(n)$) grow unnecessarily.

G-DAP and SDAC-GSP run the function, $updateTradeoff\_Diff(k)$ for different availability classes. In this case, the modified parameter is the feasible sharing degree for $class\ k$ which is S_k. Therefore, the tradeoff value is also kept per-class basis, namely $T_k(n)$. Tradeoff for the n^{th} period of $class\ k$ is calculated as shown in Equation C.1 where $U_k(n-1)$ and $RO(n-1)$ stand for the average unavailability per connection of $class\ k$ and the resource overbuild respectively, at the end of the $(n-1)^{th}$ period.

$$T_k(n) = RO(n-1) \cdot U_k(n-1) \qquad \textbf{(C.1)}$$

Algorithm 4 updateTradeoff ()

```
{Input}
{$RO(n)$: Resource overbuild at the end of the $n^{th}$ period}
{$U(n)$: Avg. unavailability per connection at the end of the $n^{th}$ period}
{$T$: Last value of the tradeoff function}
{Output}
{$T\prime$: New calculated value of the tradeoff function}
{$S(n+1)$: New calculated value for the feasible sharing degree}
$T\prime \leftarrow RO(n) \cdot U(n)$
if $T\prime < T$ then
    if $LAST\_ACTION = INCREMENT$ then
        if $S(n) < UPPERBOUND$ then
            $S(n+1) \leftarrow S(n) + 1$
        end if
        $LAST\_ACTION \leftarrow INCREMENT$
    else
        if $S(n) > LOWERBOUND$ then
            $S(n+1) \leftarrow S(n) - 1$
        end if
        $LAST\_ACTION \leftarrow DECREMENT$
    end if
end if
if $T\prime \geq T$ then
    if $LAST\_ACTION = DECREMENT$ then
        if $S(n) < UPPERBOUND$ then
            $S(n+1) \leftarrow S(n) + 1$
        end if
        $LAST\_ACTION \leftarrow INCREMENT$
    else
        if $S(n) > LOWERBOUND$ then
            $S(n+1) \leftarrow S(n) - 1$
        end if
        $LAST\_ACTION \leftarrow DECREMENT$
    end if
end if
```

APPENDIX D: The basis scheme for AC-GSP and SDAC-GSP: Generalized Segment Protection (GSP) Algorithm

Our proposed availability constrained connection provisioning schemes AC-GSP and SDAC-GSP that work under shared segment protection are built on top of a conventional segment selection algorithm, namely Generalized Segment Protection (GSP) [34]. In this section, we provide the detailed pseudocode of the GSP algorithm that we also use in our proposed schemes. The pseudocode is given in Algorithm 4.

Algorithm 5 GSP(node S, node D)

```
{Input}
{$N$: Set of nodes}
{$L$: Set of links}
{$S, D$: Source and destination pair}
{$W[]$: vector of working paths}
{$S[]$: vector of solution sets}
{Output}
{$S_{min}$: Solution with the minimum cost}
for $k = 1$ to $| N |$ do
    for $l_{ij} \in W[k]$ do
        $Cost(l_{ij}) \leftarrow \infty$
        $Cost(l_{ji}) \leftarrow 0$
        if $\lambda_s(l_{ij}) > 0$ then
            $Cost(l_{ij}) \leftarrow -Cost(l_{ij})$
        end if
        if $l_{ij} \cap W[k] \neq$ AND $j \neq D$ then
            $l_{ij} \leftarrow l_{i,j-1}$
        end if
        $P \leftarrow Dijsktra(S, D, Cost[])$
        {Restore the modified links}
        $S[k] \leftarrow current\ solution$
    end for
end for
$S_{min} \leftarrow min(S[])$
```

At the beginning, K working paths are selected based on a predetermined criteria (shortest path, minimum unavailability, shortest hop count, etc.). Upon selecting the K-paths, for each working path, the links along the working path are reversed. The cost of every link that has at least one spare channel is degraded by a negligible coefficient ε. Each link that originates out of the working path but ends on the working path is modified so that its end point is moved to the previous node on the working path.

Finally a path from source to destination is selected. Upon obtaining the path, the modified links are restored, and the connection is provisioned with the corresponding backup segments

APPENDIX E: Performance of the adaptive schemes, G-DAP and LBL-DAP under uniformly distributed SLA-classes

We have evaluated the performance of the differentiated availability aware schemes by distributing the incoming connections uniformly among the SLA classes. In this chapter we include the results that correspond to blocking probability, resource overbuild and average connection unavailability under under NSFNET and 28-node EON topology as seen from Figure E.1 to Figure E.7. The illustrated results mostly coincide with the results where the connections are heterogeneously distributed among the classes in Chapter 4.

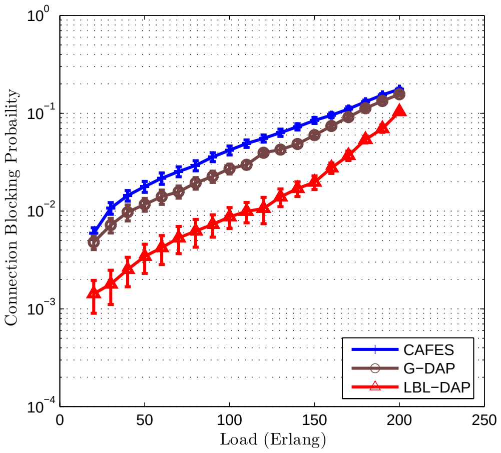


Figure E.1: Blocking probability when SLA-class distribution is uniform under NSFNET

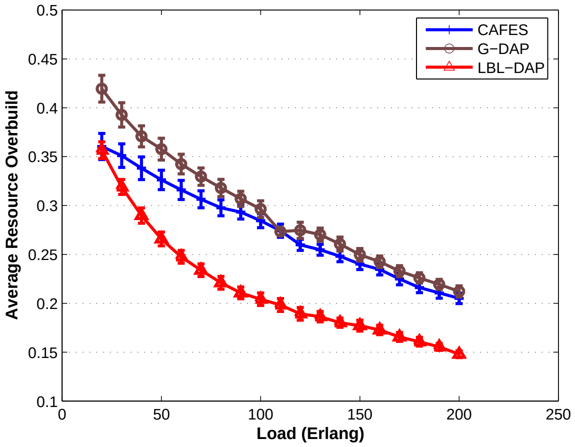


Figure E.2: Resource overbuild when SLA-class distribution is uniform under NSFNET

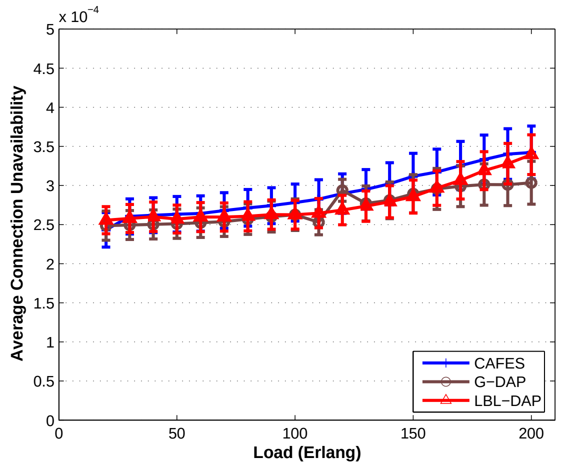


Figure E.3: Average connection unavailability when SLA-class distribution is uniform under NSFNET

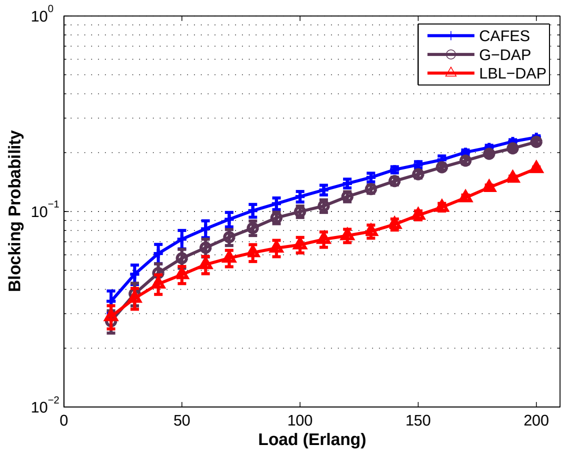


Figure E.4: Blocking probability when SLA-class distribution is uniform under 28-node EON

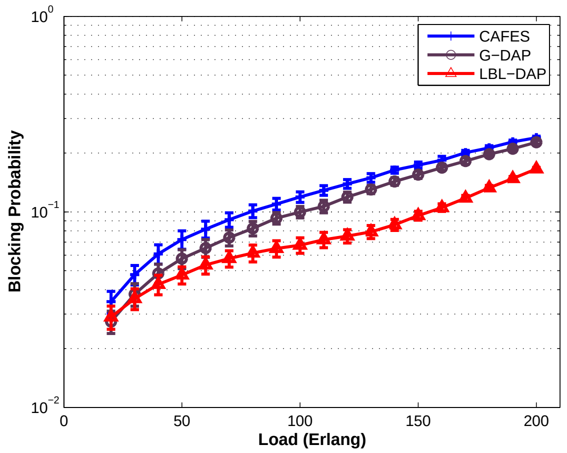


Figure E.5: Blocking probability when SLA-class distribution is uniform under 28-node EON

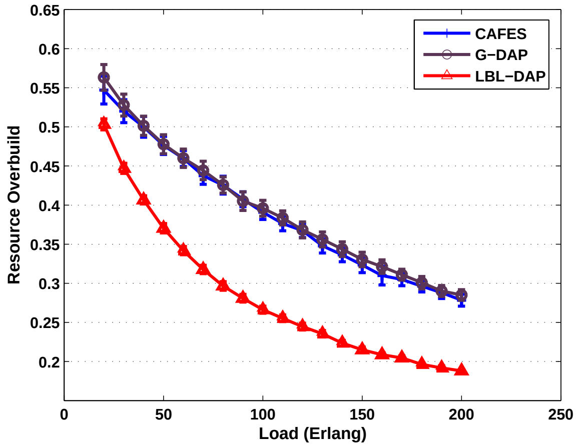


Figure E.6: Resource overbuild when SLA-class distribution is uniform under 28-node EON

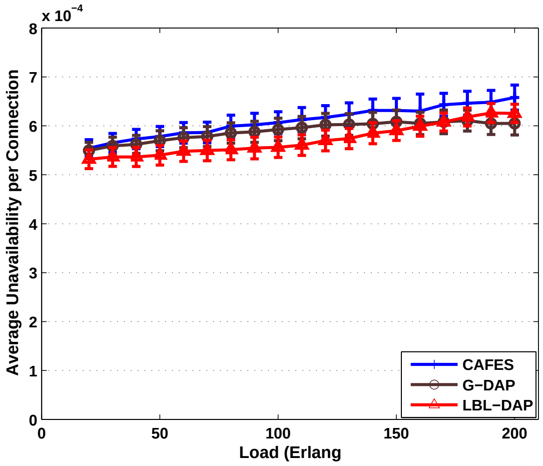


Figure E.7: Average connection unavailability when SLA-class distribution is uniform under 28-node EON

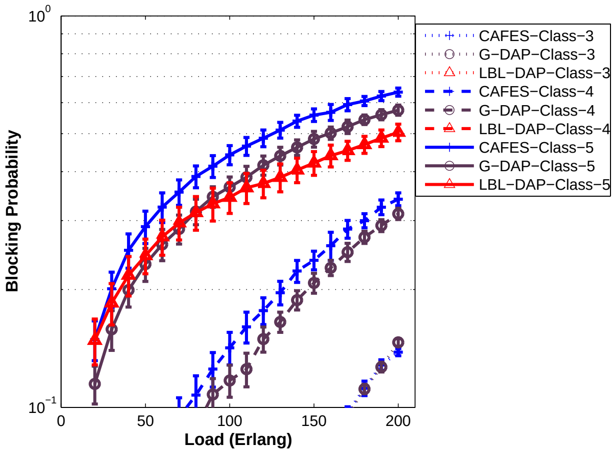


Figure E.8: Blocking probability per SLA class class when SLA-class distribution is uniform under 28-node EON

APPENDIX F: Blocking probability for AC-GSP and SDAC-GSP for a different epsilon value

As seen in Figure F.1, the behavior of availability constrained connection provisioning techniques do not show a significant change when ε is taken as 0.001. Hence, we can say that the performance of the connection provisioning techniques is independent of the ε parameter which is used in the cost assignment function for the backup path search.

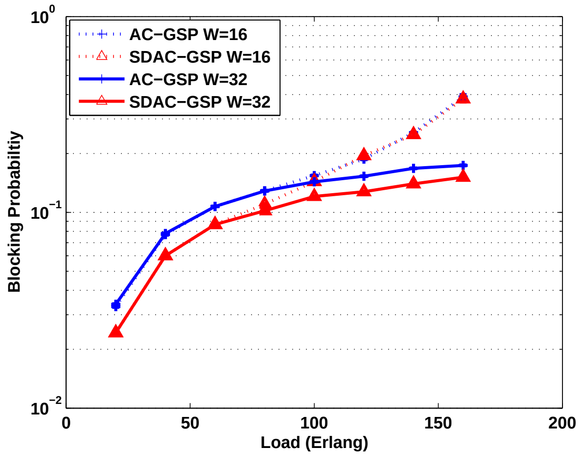


Figure F.1: Blocking probability for AC-GSP and SDAC-GSP when epsilon parameter is 0.001

It is an expected result since the ε parameter is only used to decrease the cost of the links that are shareable for the connections. Thus, a factor which is less than one and close enough to zero works to let the links be preferred by an incoming connection.

CURRICULUM VITAE

Candidate's full name: Burak Kantarcı

Place and date of birth: İstanbul, August 30th, 1981

Permanent Address: Istanbul Teknik Üniversitesi, Bilgisayar Mühendisliği Bölümü, 34469, Maslak / İstanbul, Turkey

Universities and Colleges attended: Istanbul Technical University, M.Sc and B.Sc degrees in 2005 and 2002, respectively. Vefa Lisesi, 1998.

Publications:

Journal Papers

• **Kantarci B.**, Mouftah H. T., 2009: Oktug S Adaptive Schemes for Differentiated Availability-Aware Connection Provisioning in Optical Transport Networks, *accepted to be published by IEEE / OSA Journal of Lightwave Technology*

• Khair M. G., **Kantarci B.**, Zheng J., Mouftah H. T, 2009: Optimization for Fault Localization in All-Optical Networks, *accepted to be published by IEEE / OSA Journal of Lightwave Technology*

• **Kantarci B.**, Oktug S., 2008: Loss Rate Based Burst Assembly to Resolve Contention in OBS Networks, *IET Communications (IEE Proceedings Communications)*, vol 2, Issue 1, pp. 137-143, Jan 2008

• **Kantarci B.**, Oktug S., Atmaca T., 2007: Performance of OBS Techniques under Self-Similar Traffic Based on Various Burst Assembly Techniques, *Computer Communications (Esevier)* vol 30, Issue 2, pp.315-325, January 2007

Papers Published in Springer LNCS Series

• **Kantarci B.**, Sandıkkaya M. T., Gençata A., Oktuğ S., 2007: Prudent Creditization Polling (PCP): A novel adaptive polling service for an EPON, *11th Conference on Optical Network Design and Modeling, (ONDM), Springer Lecture Notes in Computer Science,* Vol. 4534/2007, pp.388 - 397, May 2007

• **Kantarci B.**, Oktug S., 2006: Path Loss Driven Burst Assembly in OBS Networks", *21st International Symposium on Computer and Information Sciences (ISCIS), Springer Lecture Notes in Computer Science,* Vol. 4263/2006, pp.483 - 492, Nov 2006.

International Conference Papers

• **Kantarci B.**, Mouftah H. T., Oktug S., 2008: Differentiated Availability-Aware Connection Provisioning in Optical Transport Networks, *in Proc. IEEE Global Communications Conference (GLOBECOM),* New Orleans, LA, USA, December, 2008.

• **Kantarci B.**, Mouftah H. T., Oktug S., 2008: Availability Analysis and Connection Provisioning in Overlapping Shared Segment Protection for Optical Networks, *in Proc. International Symposium on Computer and Information Sciences (ISCIS),* Turkey, October, 2008.

• Khair M. G., **Kantarci B.**, Mouftah H. T., 2008: Connection Provisioning Constrained to Fault Localization in All-optical Networks, *in Proc. International Symposium on Computer and Information Sciences (ISCIS),* Turkey, October, 2008.

• Khair M. G., **Kantarci B.**, Zheng J., Mouftah H. T., 2008: Performance Optimization for Fault Localization in All-Optical Networks, *in Proc. 5th International Conference on Broadband Communications, Networks, and Systems (BROADNETS),* London, UK, September, 2008.

• **Kantarci B.**, Mouftah H. T., Oktug S., 2008: Connection Provisioning with Feasible Shareability Determination for Availability-Aware Design of Optical Networks, *in Proc. 10th International Conference on Transparent Optical Networks (ICTON),* Athens, Greece, June, 2008.

• Khair M. G., Kantarci B., Zheng J., Mouftah H. T., 2008: Optimization for minimizing fault localization time in all-optical networks, *in Proc. 10th International Conference on Transparent Optical Networks (ICTON),* Athens, Greece, June, 2008.

• **Kantarci B.**, Mouftah H. T., Oktug S., 2008: Arranging Shareability Dynamically for the Availability-Constrained Design of Optical Transport Networks, *in Proc. IEEE Symposium on Computers and Communications (ISCC),* Marrakech, Morocco, July 6-9, 2008.

• **Kantarci B.**, Oktug S., Altilar D. T., 2008: Prioritized Contention Resolution Scheme for Grid Services over OBS Networks, *in Proc. Sixth Annual Conference on Communication Networks and Services Research (CNSR),* Halifax, Nova Scotia, Canada, May 5-8, 2008.

• **Kantarci B.**, Oktug S., Atmaca T., 2006: Burst Loss Rate: Is it precise enough?, *in Proc. International Symposium on Computer Networks (ISCN),* Istanbul, Turkey, pp.173-178, 16-18 June 2006.

- **Kantarci B.**, Oktug S., 2006: *AdaptiveThresholdBasedBurstAssemblyinOBSNetworks*, in Proc. Canadian Conference on Electrical and Computer Engineering (CCECE), Ottawa, Canada,, pp.485-488, 7-10 May 2006.

- **Kantarci B.**, Oktug S., Atmaca T., 2005: Analyzing the Effects of Burst Assembly in Optical Burst Switching under Self-similar Traffic, *in Proc. Advanced Industrial Conference on Telecommunications(AICT)*, Lisbon, Portugal, pp.109-114, 17-20 July 2005.