SERVICE LEVEL AGREEMENT BASED ARCHITECTURES AND MECHANISMS IN PRIORITY-AWARE SHARED MESH OPTICAL NETWORKS

by

Alireza Nafarieh

Submitted in partial fulfilment of the requirements
for the degree of Doctor of Philosophy

at

Dalhousie University
Halifax, Nova Scotia
December 2011

DALHOUSIE UNIVERSITY

DEPARTMENT OF ENGINEERING MATHEMATICS AND INTERNETWORKING

The undersigned hereby certify that they have read and recommend to the Faculty of Graduate Studies for acceptance a thesis entitled "SERVICE LEVEL AGREEMENT BASED ARCHITECTURES AND MECHANISMS IN PRIORITY-AWARE SHARED MESH OPTICAL NETWORKS" by Alireza Nafarieh in partial fulfilment of the requirements for the degree of Doctor of Philosophy.

Dated: December, 5th, 2011

External Examiner _____

Supervisor _____

Reader _____

Reader _____

Reader _____

Departmental Representative _____

DALHOUSIE UNIVERSITY

DATE: December, 5th , 2011

AUTHOR: Alireza Nafarieh

TITLE: SERVICE LEVEL AGREEMENT BASED ARCHITECTURES AND MECHANISMS IN PRIORITY-AWARE SHARED MESH OPTICAL NETWORKS

DEPARTMENT OR SCHOOL: DEPARTMENT OF ENGINEERING MATHEMATICS AND INTERNETWORKING

DEGREE: Ph.D. CONVOCATION: MAY YEAR: 2012

_____

Signature of Author

To my family

You have always inspired me

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABSTRACT

Service providers' goals include providing reliable connections with the minimum allocated resources over a shared-mesh path restoration scheme in WDM networks. However, in some cases, the requested parameters in an SLA are beyond the capacity of the network, and the connection is typically blocked. To give the customer a chance to choose another provider, or in the case of having only one provider, to comply with the provider's network capacity, new SLA-based architectures and mechanisms are required to be introduced to provide better service to prioity-aware shared mesh WDM networks. To achieve this goal, the dissertation's contributions focus on three main characteristics of the network design: i) A dynamic SLA negotiation infrastructure to negotiate and propagate crucial SLA parameters, ii) Path attributes which can provide a better picture of network resources and status and are suitable to be propagated by the negotiating system, and iii) Algorithms benefiting from the path attributes to improve the blocking probability and resource utilization of the network.

To fulfill the first goal of the contributions, a dynamic SLA negotiation mechanism for both intra and inter-domain communications using OSPF and BGP protocols is proposed. Link attributes via intra-domain, and new proposed TE path attributes through inter-domain mechanisms are advertised. Several novel path constraints and attributes are proposed which are dynamically updated and propagated through the network over the connections provisioning process period to satisfy the second objective of the contributions in this dissertation. The path availability, holding time, SLA violation risk, and path risk factor are the important characteristics of the proposed path attributes. As the third goal considered for the contributions, novel priority-aware algorithms and SLA-based mechanisms are proposed to improve the network performance for different traffic types of various priority classes. The algorithms and mechanisms proposed in this thesis take advantage of the new path attributes and SLA negotiation infrastructure to better serve high-priority connection requests at the lowest cost. The mechanisms and network architectures proposed in this work are a solution for the high-priority requests that normally cannot be accommodated as they violate the best availability offered by service providers.

LIST OF ABBREVIATIONS USED

ADT	Allowable Down Time
APSA	Adaptive Provisioning SLA-Aware
AS	Autonomous System
ASR	Availability Satisfaction Ratio
AWPC	Average assigned Wavelengths Per Connection
BGP	Border Gateway Protocol
BGP-TE	Border Gateway Protocol- Traffic Engineering
BHC	Buffering High priority Connection
BP	Blocking Probability
BP-B	Blocking Probability Bronze
BP-G	Blocking Probability Gold
BP-S	Blocking Probability Silver
BR	Blocking Rate
CDT	Cumulative Down Time
CNF	Cumulative Number of Failures
COPS	Common Open Policy Service
CRM	Connection Request Matrix
CSPP	Conventional Shared Path Protection
CST	Committed Service Time
DMPA	Dynamic Maximum Path Availability Algorithm
DT	Down Time
EBGP	External Border Gateway Protocol
ECM	Established Connection request Matrix
ER	Edge Router
FF	First-Fit
FMPA	Floating Maximum Path Availability
GMPA	Guaranteed Maximum Path Availability
GMPLS	Generalized Multi-Protocol Label Switching
GSLP	Generic Signaling Layer Protocol
GT	Graph Topology
HASP	History-aware SLA-based Shared Path Protection
HB	High Bound
HPPR	High-Priority Provisioned Request
HT	Holding Time
IBGP	Internal Border Gateway Protocol
IGP	Internal Gateway Protocol
ILP	Integer Linear Programing
IMPA	Initial Maximum Path Availability
ISP	Internet Service Provider
IU	Immediate PSA Update
JWR	Joint Wavelength-Route
LA	Link Attribute
LB	Low Bound

LL	Least-Loaded
LSA	Link State Advertisement
LSP	Label Switched Path
LSR	Label Switching Router
LU	Least-Used
MATLAB	Matrix Laboratory
MP	Min-Product
MPA	Maximum Path Availability
MTBF	Mean Time Between Failure
MTTR	Mean Time To Repair
MU	Most-Used
MΣ	MAX-SUM
NP	No Protection
NSFNet	National Science Foundation Network
OSPF	Open Shortest Path First
OSPF-TE	Open Shortest Path First- Traffic Engineering
PA	Path Attribute
PAA	Priority-Aware Algorithm
PDT	Possible Down Time
PECM	Path risk factorized Established Connection Matrix
PPBC	Pre-Provisioned number of Blocked Connections
Pr	Probability
PRF	Path Risk Factor
PSA	Path State Advertisement
PU	Period-based Update
QoS	Quality of Service
RADT	Residual Allowable Down Time
RHT	Residual Holding Time
RHTM	Residual Holding Time Matrix
RNAP	Resource Negotiation and Pricing
RO	Resource Overbuild
RWA	Routing and Wavelength Assignment
SECM	Shared risk Established Connection Matrix
SLA	Service Level Agreement
SLS	Service Level Specification
SMPA	Static Maximum Path Availability Algorithm
SPA	Statically Pre-provisioned Priority-aware Algorithm
SRLG	Shared Risk Link Group
SrNP	Service Negotiation Protocol
SSPP	Standard Shared Path Protection
STSR	Service Time Satisfaction Ratio
TE	Traffic Engineering
TED	Traffic Engineering Database
TLV	Type Length Value
TMPA	Time-aware Maximum Path Availability
TU	Threshold-based Update

WDM	Wavelength Division Multiplexing
WMPA	Weighted Maximum Path Availability

ACKNOWLEDGEMENTS

It would not have been possible to write this doctoral thesis without the help and support of the kind people around me, to only some of whom it is possible to give particular mention here.

This thesis would not have been possible without the help, support and patience of my principal supervisors, Dr. William Phillips and Dr. Bill Robertson. I would also like to acknowledge their financial, academic and technical support.

The good advice, support and friendship of my other committee member, Dr. Shyamala Sivakumar has been invaluable on both an academic and a personal level, for which I am extremely grateful.

I thank the other committee member Dr. Peter Bodorik for reading the thesis.

I would like to acknowledge the academic and technical support of the Internetworking Engineering program and its staff, particularly the program manager Mrs. Shelley Caines.

I would like to thank my wife Maryam for her personal support and great patience at all times.

CHAPTER 1 INTRODUCTION

Survivable mesh optical wavelength division multiplexing (WDM) networks play a crucial role in serving recent tremendous growth in the Internet traffic demand. In WDM networks, every fiber link has multiple channels (wavelengths) and each channel carries a huge amount of traffic over each wavelength. Any failure on any link or wavelength causes considerable data losses for customers. Since failures in optical networks are inevitable specifically in metro and access layers, protection or restoration schemes are a necessity for optical transport networks. To have an effective protection scheme, the customer and the service provider sides should be able to negotiate with each other.

On the other hand, the increasing demand on quality of service (QoS)-based traffic, which carries large amounts of high-priority traffic class, requires the development of new traffic engineering strategies along with provisioning algorithms and protection schemes. The new strategies typically take service level agreement (SLA)-aware algorithms into account to maintain a satisfactory level of QoS for connection requests with regard to the parameters requested in an SLA.

Routing within the optical network relies on both knowledge of network topology and resource availability. This information may be gathered and used by a centralized system, or by a distributed link state routing protocol. In either case, the first step towards network-wide link state determination is the discovery, by each router, of the status of local links to all neighbors. To disseminate traffic engineering (TE) information to all the nodes of a network, the information should be propagated inside and outside the autonomous system (AS), along the path from source to destination.

An SLA parameters negotiation infrastructure, novel algorithms, together with new path attributes, and improved path/link cost functions can help customers to modify, refine and further process connection requests over shared mesh network topologies. They can then better comply with service providers' network capacity. By taking advantage of an entire architecture, service providers will better serve customers at lower cost.

1.1 MOTIVATIONS AND OBJECTIVES

The communication between customers and service providers takes place using SLA parameters, and connections are established when SLA parameters are satisfied. Service providers' goals include maintaining reliable connections with the minimum allocated resources over a shared-mesh path restoration scheme in WDM networks. However, in some cases, the requested parameters in an SLA are beyond the capacity of the network, and the connection is typically rejected or blocked. To give the customer a chance to choose another provider, or in the case of having only one provider, to comply with the provider's network capacity as much as possible, a dynamic architecture for SLA parameters negotiation between service providers and customers, and automatic dissemination mechanisms over this dynamic infrastructure are required. In other words, to enable the customers of shared mesh WDM optical networks to negotiate some aspects of SLA contracts with service providers in an automatic and dynamic manner is the motivation for developing dynamic architectures and mechanisms. The goal is to develop the algorithms and related aspects over the existing internet infrastructure and protocols rather than developing independent protocols from scratch.

However, having a negotiation infrastructure alone may not help service providers to achieve the goals mentioned above. To achieve these goals, in addition to a dynamic negotiation infrastructure, some tools and mechanisms are required to take advantage of the negotiation infrastructure. Among the tools presented in this dissertation are algorithms which can benefit from the negotiation infrastructure to serve a specific class of traffic. The other tools are the new link and path attributes used by the proposed algorithms. New link/path attributes give customers and service providers a better picture of the network status. The need for such tools that enable customers and service providers to better accommodate high-priority requests is the motivation for presenting some effective priority-aware and SLA-based algorithms together with traffic engineering path attributes and constraints.

Based on the facts discussed in [1] and [2], the main basic building blocks of a QoS-based routing mechanism are: i) QoS metrics selection, ii) Advertisement of link state information, iii) Path selection, and iv) Path maintenance and recovery. The following three architectural network components are similarly proposed and followed in this thesis so that if they work together, they can improve the service to certain classes of traffic. These components are developed, modified, enhanced, and evaluated in Chapters 3 to 7. The three components are shown in Figure 1.1.

1) A negotiation infrastructure: dynamic negotiation mechanisms being capable of negotiating SLA parameters and other desirable path attributes or constraints
2) Negotiating parameters: SLA parameters or other desirable path attributes or constraints proposed in this thesis
3) Provisioning algorithms: algorithms being capable of benefiting from two other components to serve certain classes of traffic

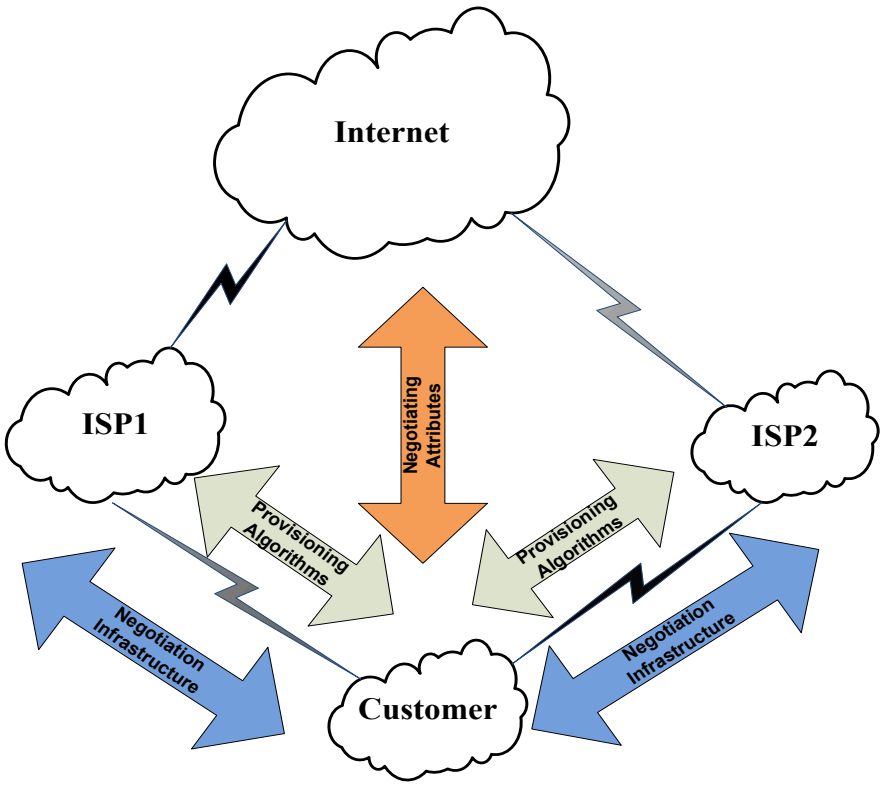


Figure 1.1 Main components of the SLA-based architecture

1.2 RESEARCH CONTRIBUTIONS

The five contributions forming this dissertation are breifly pointed out in the following sections. The main objectives of the contributions are to look for SLA-based architectures and mechanisms to provide better service to prioity-aware shared mesh WDM networks. To achieve this goal, the contributions focus on three main characteristics of the network design: 1) An SLA-based architecture as an infrastructure to negotiate SLA parameters, 2) Path and link attributes which can provide a better picture of network resources and status and are suitable for propagation by the negotiating system, and 3) Algorithms benefiting from the path/link attributes to improve the blocking probability and resource utilization of the network.

1.2.1 Dynamic SLA negotiation infrastructure over shared mesh optical networks

To establish a dynamic intra- and inter-domain SLA negotiation mechanism for shared mesh optical networks, some TE extensions over open shortest path first (OSPF) and border gateway protocol (BGP) protocols are introduced in Chapter 3. The OSPF-TE extensions are responsible for carrying the link attributes proposed in this thesis via intra-domain negotiation mechanisms, and the BGP-TE extensions are responsible for carrying newly proposed path attributes via inter-domain negotiation mechanisms. Since the proposed link and path attributes may cause heavy control overheads in a dynamic environment, an alternative means of communication is proposed to reduce the overheads and resolve scalability issues.

Two simulation environments are tested: one to evaluate the control overheads reduction process, and the other to evaluate the performance improvement of the network status. The simulation results will show how the negotiation protocols together with the proposed TE attributes can improve the performance of different protection schemes or algorithms.

1.2.2 Statically pre-provisioned priority-aware mechanisms over shared mesh optical networks

A path constraint is proposed in Chapter 4 to provide an improved picture of network resources for the customers of shared mesh WDM networks. The path constraint represents the maximum initial status of the network in terms of the path availability under no load and when no traffic is applied to the network. Assuming a dynamic SLA negotiation mechanism, the path metric can be disseminated all over the network. Benefiting from the proposed path constraint, a pre-provisioned priority-aware mechanism is introduced to provide service to the high-priority connection requests which are beyond the initial capacity of the network. The algorithm together with the proposed attribute modify potentially blocked requests (the requests which might be blocked by existing algorithms) to comply with the initial condition of the network. Simulation environments evaluate and verify network performance when the algorithm is used.

1.2.3 Dynamically provisioned priority-aware algorithms over shared mesh optical networks

As a complementary study to the contribution presented in Chapter 4, another path constraint which is a general case of the path metric proposed in Chapter 4 is introduced in Chapter 5. The new path metric is dynamically updated after the occurrence of any changes to connections, including release of old connections or establishment of new connections. To update the new path attribute dynamically, an algorithm calculates the highest path availability offered by the service providers for any chosen source and destination pairs and updates the matrix of the path attribute for all possible pair of nodes. Since there is a dynamic SLA negotiation infrastructure proposed in Chapter 3, the path constraint introduced in Chapter 5 is propagated all over the network. The new path attribute helps the two algorithms proposed in Chapter 5 to modify and process their requests before they send the requests out to the service providers, and consequently they improve the network performance for static and dynamic traffic. Two simulation environments injecting static and dynamic traffic are tested.

1.2.4 Adaptive SLA-aware provisioning mechanism for long duration shared mesh protected connections

A time-aware path attribute is presented in Chapter 6 by which the maximum path availability of the network, for any specific source and destination pair, is scheduled, and is valid for a certain period of time. Path availability and connection holding-time, two crucial SLA connection parameters, are used to dynamically build and update the new time-aware path attribute. Taking this new path attribute into account, an adaptive provisioning SLA-aware mechanism is introduced to buffer and further process the potentially blocked high-priority connection requests in a timed manner. Simulation environments are developed to show the improved performance of the proposed architecture, with respect to previously existing algorithms, when serving a large number of high-priority connection requests with fairly long durations.

1.2.5 History-aware SLA-based mechanism over shared mesh WDM networks

An algorithm is introduced in Chapter 7 which takes advantage of attributes of the previously established connections, and builds a history-aware database of those path attributes to process upcoming requests. By implementing this mechanism, service providers will be able to exploit the unused allowable down time of the existing connections to serve additional requests. Two characteristics of connection requests, holding time and failure arrival rate, help the algorithm to route the requests in such a way that any SLA violation is either avoided or minimized. To achieve this goal, path risk factors of previously established paths are calculated and are flagged based on their risk tolerance to SLA violation. The path attribute introduced in Chapter 7 is disseminated throughout the network and is considered as a constraint in path calculation of upcoming connection requests.

In addition, a novel path cost function is introduced by which the routing algorithm calculates optimal primary-backup pairs. The optimal path cost function proposed in Chapter 7 considers the number of wavelengths, the failure arrival rate of the

connections, and the path risk factor (introduced in Chapter 7) as three criteria for choosing the lowest cost paths.

Different test bed environments are simulated and used to evaluate networks with high link failure arrival rate, representing high risk networks, and networks with low link failure arrival rate, representing low risk networks. In addition to performance improvement, simulation results show how the proposed mechanism provides higher revenue for service providers compared to standard and existing SLA-aware algorithms over high risk networks.

1.3 ORGANIZATION OF THE DISSERTATION

Chapter 2 reviews the literature regarding the five major topics namely: i) SLA negotiation protocols and mechanisms, ii) Priority-aware algorithms over protected optical networks, iii) SLA-based algorithms over protected optical networks, iv) Mathematical models for path availability analysis, v) Routing and wavelength assignment approaches. Different protection and restoration schemes including shared mesh schemes are also discussed.

Chapter 3 presents a dynamic SLA negotiation mechanism considering intra/inter-domain communications over shared mesh optical networks. New traffic engineering extensions to OSPF-TE and BGP-TE are introduced. This chapter shows how SLA negotiation protocols together with the proposed TE extensions improve the performance of priority-aware algorithms. A solution is introduced to resolve scalability issues and to reduce control overheads caused by communications of the TE extensions. The network performance and control overheads are evaluated by testing the mechanism in a simulation environment.

Chapter 4 presents a pre-provisioned priority-aware algorithm to accommodate higher priority requests. It discusses a new algorithm to improve resource utilization and availability performance of shared mesh optical networks. The proposed algorithm pre-provisions the requests and processes and modifies them before it applies the routing and

wavelength assignment to any of them. Then a path constraint considering the initial status of the network in terms of the path availabilities is presented. The simulation environments are presented to evaluate the blocking rate, the availability satisfaction rate, and the number of pre-provisioned high-priority connection requests that are established.

Chapter 5 introduces two priority-aware algorithms, for static and dynamic traffic, for different levels of priority. In addition to the algorithms proposed in Chapter 5, a novel TE path attribute is introduced. This new path constraint helps the proposed algorithms to improve the performance of high-priority requests using dynamic negotiation of SLA parameters between a customer and service providers.

Chapter 6 proposes a mechanism with three main objectives: proposing a new time-aware TE path attribute, introducing a novel adaptive provisioning SLA-aware algorithm which considers the proposed path attribute as a criterion in its calculation, and applying a high volume of high-priority dynamic traffic with long duration to the introduced mechanism. The mechanism accommodates some of those high-priority connection requests with long durations which would probably have been blocked in other SLA-aware algorithms or protection schemes.

Chapter 7 has two parts. In the first part, a routing algorithm is discussed through which a new cost function for the path calculation is presented. The path selection policy is based on the possible and allowable down time of the paths. In the second part, a mechanism is presented to either avoid or minimize the SLA violation. The main goal of the proposed mechanism is to bring higher revenue to Internet service providers (ISP). The simulation results of both parts are compared favorably to conventional algorithms and existing related mechanisms in terms of the revenue that a service provider can earn.

Chapter 8 concludes the dissertation and gives some potential research directions regarding future work. The mechanisms proposed in this dissertation have been evaluated by simulation in MATLAB. Although the MATLAB codes are not included in the thesis, the codes related to the algorithms, simulation environments, and traffic patterns can be provided by the author upon request.

CHAPTER 2 A REVIEW OF QOS-BASED MECHANISMS OVER SHARED MESH PROTECTED INFRASTRUCTURES

2.1 INTRODUCTION

Today's core telecommunication networks are based on optical networking infrastructures. Optical networks have been generalized to support metropolitan access links [1]. Nowadays, some telecommunication companies offer optical networks to homes, such as Bell/Alliant in Canada. The tremendous demand of QoS-based services by customers requires service providers to consider more service management than network management. To achieve this goal, service providers should be capable of coping with management architecture problems including dynamic SLA negotiation, probability of SLA violation, and translating SLA to network provisioning [3]. A path attribute is a characteristic of a path, which can affect the path computation, routing, and optimization process. For instance, bandwidth available on the links, link protection capabilities, and the type of network resources associated with the links are taken into consideration during the path selection or optimization process [4]. Service availability and resilience, routing constraints, class of service, level of priority, and path attributes are considered to be service level specifications (SLSs) in this thesis.

Definition: SLA and SLS

A service level agreement (SLA) is a formal contract between a service provider and a subscriber that contains technical and non-technical terms and conditions [5]. *The detailed technical specifications are called service level specifications (SLSs). An SLS is a set of parameters and their values that together define the service offered to a traffic stream in a network* [6]. *A thorough discussion of the SLA and SLS in optical networks has been presented in* [7].

2.2 SLA NEGOTIATION INFRASTRUCTURE

Since OSPF and BGP are widely used by service providers as intra-domain and inter-domain routing protocols, respectively, the majority of the work referenced here modifies or adds extensions to these protocols to enhance their ability for serving in traffic engineered environments. The authors in [8] describe extensions to the OSPF protocol version 2 to support intra-area TE, using opaque link state advertisements (LSAs) [9]. Different types of opaque LSAs and their associated format have been discussed in [8]. The standard track presented in [8] talks about LSA payload details in which one of the top-level Type/Length/Value (TLV) triplets is the link TLV which describes a single link, and is constructed of a set of sub-TLVs. The link TLV presented in [8] contains sub-TLVs including reservable, used, and unreserved bandwidth, and a traffic engineering metric. The traffic engineering metric sub-TLV in the link TLV of the LSA payload specifies link metrics for traffic engineering purposes. Although this sub-TLV is usually used for propagating the standard OSPF link metrics, it can also be used for other traffic engineering purposes [8]. In [10], extensions to the OSPF routing protocol in support of carrying link state information for Generalized Multiprotocol Label Switching (GMPLS) have been presented. The sub-TLVs for the link TLV in support of GMPLS have been enhanced in [10]. The link protection type and shared risk link group (SRLG) sub-TLVs presented in [10] are the new sub-TLVs added to the link TLV presented in [8]. The link protection type identifies that the protection scheme is shared. The concept of a shared risk link group is also used in Chapter 7 when a new path attribute is defined. The extensions introduced in [8] and [10] are considered as the base of the new extensions to OSPF-TE proposed in this thesis. Although standards [8] and [10] have proposed traffic engineering metric extensions, they discuss neither path constraints nor efficient ways of propagation of such constraints inside and/or outside an autonomous system. In Chapter 3, new sub-TLVs to OSPF-TE extensions are proposed to support intra-domain TE path/link attribute dissemination, and to propagate the link availability inside an autonomous system. In Chapter 3, a dynamic path availability negotiation scheme is developed and it is shown how the conventional shared-mesh path protection (CSPP) scheme benefits from that development, and the network performance when compared to

the no protection (NP) and standard shared-mesh path protection (SSPP) schemes, is improved. The no-protection mechanism does not consider backup paths to protect primary paths. The mathematical analysis of the path availability for the NP scheme is discussed later in Section 2.5.2. The SSPP mechanism is an approach to reduce recovery resource requirements. The SSPP protects lightpaths by sharing network resources when the working lightpaths that they protect are physically (i.e., link, node, SRLG, etc.) disjoint. The SSPP mechanism has been described in [11] and [12] in which link availabilities are not considered as a constraint for the path calculations. As discussed in detail in [11], the SSPP scheme is a shared mesh restoration scheme that is a particular case of pre-planned LSP re-routing to reduce the restoration resource requirements. It does so by allowing multiple restoration LSPs initiated from distinct ingress nodes to share common resources including links and nodes. The CSPP mechanism is considered as a generalized case of the SSPP scheme in this thesis in which link availabilities are involved in the path calculation process. One of the most important issues for network end users is reliability [1]. The link/path availability is one of the QoS parameters of the reliability class among other QoS parameter classes [1]. The mathematical analysis of the path availability for the CSPP scheme, and the way link availabilities affect the path calculation of the CSPP are discussed later in Section 2.5.6. Although the SSPP scheme is a shared mesh protection scheme, it does not take any traffic engineering parameters for primary/backup path calculations into account. The advantage of those path protection schemes which consider link availability (including the CSPP scheme) as one of the most fundamental and simplest traffic engineering metrics is investigated in Chapter 3 by introducing a dynamic SLA negotiation mechanism.

Since traffic engineering information should be able to travel throughout the entire network, an efficient and uncomplicated mechanism is required to propagate TE path attributes between different autonomous systems. A BGP-TE attribute which enables BGP to carry TE-information, has been presented in [13]. In [13], connection bandwidth at different priority levels and switching capability information were introduced as the attributes added to BGP for traffic engineering. Although the BGP-TE protocol introduced in [13] is meant to act as an inter-autonomous TE parameters propagation

protocol, it does not discuss how TE path attributes can be disseminated over several autonomous systems while making no changes on the path calculation process.

The scalability issues should be considered as another implication of the new BGP path attributes dissemination. Although the use of the traffic engineering attribute does not increase the number of routes, it may increase the number of BGP Update messages required to distribute the routes. In Chapter 3, new sub-TLVs to BGP-TE extensions are proposed in order to support inter-domain TE path attribute propagation while the path attributes have no impact on the BGP path calculation procedure. In addition, a solution for scalability implications of such propagations is introduced. How the scalability issue is addressed will be discussed later in this section. The new inter-domain sub-TLVs proposed in Chapter 3 will propagate new desirable TE path attributes. Some of these new TE path attributes will be used in Chapters 4 to 7.

The idea of disseminating path-related (not domain-related) QoS-metric per destination within an extended TE-attribute has been presented in [14], and the efficiency of BGP-TE extensions under the GMPLS framework has been evaluated. The proposed path-related TE-attribute in [14] is representative of the overall path from a certain node to the destination. In order to provide multiple paths per destination and to map the hop-by-hop BGP into the source-routing requirements of GMPLS, the authors in [14] have proposed a behavioral modification of the protocol which consists of using the BGP only as a dissemination protocol, not as a path selection one. Since the proposed mechanism in [14] propagates TE-related information without affecting the BGP path selection process, it has been considered as an appropriate model for the mechanism presented in this research. However, the link availability dissemination through a dynamic mechanism has not been considered in [14]. The sub-TLVs proposed in Chapter 3 facilitate a dynamic mechanism for link/path availability dissemination. Link availability is one of the most important QoS parameters representing the network reliability [1].

As mentioned above, another challenging issue in propagating, routing, signaling, or managing information over the entire network is control overheads that the flooded information applies to the network. An improved OSPF-TE protocol has been proposed

in [15] so that rather than disseminating link state information through LSAs, a newly designed path sub-TLV called path state advertisements (PSAs) propagates path attributes. Unlike the traditional OSPF-TE, the proposed protocol in [15] does not advertise the absolute value of available link resources. Instead, it only disseminates resources' increments or decrements to cope with control overheads issues. As mentioned earlier, the link and path availabilities are important TE metrics requested by customers through the SLA to guarantee the reliability of the network [1]. Although [15] has proposed a path-related extension to OSPF, it does not propagate link or path availability. In addition, inter-AS communications has not been considered in [15]. In Chapter 3, the PSA concept is expanded to be used to overcome the scalability issues concerning control overheads while it considers link and path availabilities as TE constraints over inter-AS communications.

Several other protocols have already been proposed for SLA parameters negotiation, such as Resource Negotiation and Pricing (RNAP) protocol [16], Service Negotiation Protocol (SrNP) [17], Common Open Policy Service- Service Level Specification (COPS-SLS) [18], and QoS Generic Signaling Layer Protocol (QoS-GSLP) [19], to name a few. The RNAP protocol enables service negotiation between user applications and the access network. The protocol permits negotiation and communication of QoS specifications, user traffic profiles, admission of service requests, and pricing and charging information for requested services [16]. The Service Negotiation Protocol (SrNP) [17] supports dynamic SLS negotiation using network-level QoS parameters. A unique feature of SrNP is that the protocol is not specific to any particular SLS format or to the context of an SLS. It is general enough to be applied for negotiating any parameters provided the parameter is in the form of attribute–value pairs. The semantics and format of the parameter under negotiation are transparent to the protocol. The objective of the negotiation process is to agree on the value of the attributes included in the parameter under negotiation, rather than the attributes themselves [20]. COPS-SLS protocol follows a client-server model which provides all operations needed for service level negotiation such as requesting, accepting, rejecting, proposing, or degrading a service level [18]. A characteristic feature of COPS is that it distinguishes the interactions between a

subscriber and the negotiating node into two phases: configuration and negotiation. In the configuration phase, the service provider informs the subscriber how to request a level of service [20]. However, those protocols have mainly been designed either for wireless networks or for pricing purposes [20]. They do not use the commonly used traffic engineering IP routing protocols, such as OSPF, BGP, and they are independent and complicated protocols. In addition to the complexity, there are message overhead considerations for the protocols such as RNAP which requires periodic signaling to refresh the negotiated service [20]. As studied in detail in [20], none of the above mentioned negotiating protocols have been widely deployed on real networks since the issues involved in inter-working of these negotiation protocols with other standardized protocols have not been resolved yet. In addition, a dynamic service negotiation should be able to interact with other network components including QoS routing, wavelength assignment, and network provisioning. Therefore, the above discussed protocols have not been considered as the primary means of propagation in this thesis although they can be considered as alternative options.

2.3 PRIORITY-AWARE MECHANISMS

The first steps of establishing a mutual and bidirectional SLA-based negotiating communication between customers and service providers are taken in Chapter 3 by introducing a dynamic SLA parameters negotiation infrastructure. The communication mechanism introduced in Chapter 3 negotiates the SLA parameters and the desirable path constraints proposed in the following chapters. Considering an infrastructure for disseminating the SLA parameters introduced in Chapter 3, new path attributes propagated over this infrastructure can be suitable criteria for the path calculation and routing processes of certain class of traffic. In other words, the SLA negotiation bed, desirable path attributes, and proper routing and wavelength assignment algorithms are the three main characteristics of priority-aware mechanisms by which high-priority connection requests are provisioned.

Shared-mesh protection schemes have been extensively studied recently and algorithms have been proposed to improve the performance of either path computation algorithms or sharing processes. The SSPP scheme presented in [11] and [12] does not consider any SLA parameters, such as links' availability, and requests priority level as a part of the process of the path computation. A priority-aware shared mesh protection algorithm has been presented in [21] by which the backup paths are found based on the priority of the connection requests. Connection requests in [21] are submitted dynamically and the algorithm has no prior knowledge of incoming requests. The priority-aware algorithms in [21] and [22] have presented new insight into the definition of the path availability with respect to the traffic priority level. The algorithm in [21] has been applied to static traffic and the algorithm in [22] has considered dynamic traffic. The network performance improvements for both algorithms have been proven through both mathematical integer linear programing (ILP) model and heuristic algorithms.

In Chapter 4, the behavior of the algorithm proposed in [21] for a static traffic pattern is investigated. Although the mechanisms presented in [21] and [22] consider SLA parameters as criteria in routing the requests they receive, they have no capability of negotiating and revising these parameters to improve the network performance. Considering the existence of a dynamic SLA negotiation infrastructure presented in Chapter 3, the mechanism proposed in Chapter 4 negotiates the network parameters to more effectively assign the network resources, and better serve high-priority requests. The algorithm and the TE path constraint presented in Chapter 4 facilitate a bidirectional negotiation mechanism between customers and service providers when a static traffic pattern is applied to the network. In other words, the mechanism introduced in Chapter 4 not only takes the SLA parameters into account as an effective factor in the routing process, but it is also capable of negotiating the new introduced path attribute, the initial maximum path availability, between customers and service providers. The new path attribute proposed in Chapter 4 is disseminated over the network using the dynamic SLA negotiation mechanism introduced in Chapter 3, and gives an opportunity to network nodes to be better aware of maximum resource availability on the network.

In addition, Chapter 4 investigates the effect of applying the traffic to high risk rather than low risk networks. As shown in the performance evaluation in Chapter 4, although the algorithms presented in [21], [22] may have good performance over low risk networks, their performance degrades when they are applied to high risk networks (see below for the definition). The mechanisms proposed in this thesis are mainly evaluated over high risk networks in order to simulate a network layer, such as metropolitan or access layers, rather than the core layer.

Definition: Dynamic/Static traffic

In dynamic pattern, lightpaths are requested dynamically with randomly generated availability requests so that the algorithm has no knowledge about the coming request. Dynamic traffic has been used interchangeably with online traffic in some references [22]. *However, in the stati traffic, connection requests are permanent and known a priori. Static traffic has been used interchangeably with offline traffic in some references* [21].

Definition: High/Low risk networks:

Here the term "high risk network" is applied to the networks whose links have high failure arrival rate on average. In contrast, the term "low risk network" is applied to networks whose links have low failure arrival rate on average. In other words, high-risk networks are those with randomly chosen low link availabilities, and low risk networks are those with randomly chosen fairly high link availabilities.

Although the algorithms presented in [21] and [22] are priority-aware algorithms and they improve the blocking rate and availability satisfaction rate of shared mesh optical networks compared to the SSPP algorithm, they have no knowledge of what happens in the network dynamically in terms of availability of the requested paths based on the current status of the network resources. Besides, they do not consider any dynamic negotiation of path constraints between customers and service providers before establishing requested connections. Even for the mechanism introduced in Chapter 4 which benefits from the dynamic SLA negotiation infrastructure presented in Chapter 3 and accommodates the high-priority connection requests better than the lower priority connection requests, the nature of the SLA negotiation is static as the pre-provisioned

requests are calculated based on the initial link availability of the network. That is, although the mechanism proposed in Chapter 4 is based on an SLA negotiation, it does not benefit from a dynamic mechanism to inform the customer about the ongoing changes in the availability of the requested paths. In fact, Chapter 4 proves the necessity and capabilities of a static negotiation mechanism. To extend the concept of SLA negotiation to the bidirectional dynamic type of communication, Chapter 5 introduces the new algorithms and TE path attributes. The mechanism presented in Chapter 5 takes advantage of a dynamic mechanism for propagating requested paths' availabilities to update dynamically the new path constraint, to propagate the proposed path constraint over the entire network, and to better serve high-priority connection requests. In other words, the advantages of the priority-aware mechanism concept are proved in Chapter 4 using a static path attribute and a mechanism, and then the concept is generalized in Chapter 5 by introducing a dynamic path attribute and a mechanism to support different types of traffic in various levels of priorities.

2.4 SLA-BASED MECHANISMS

As mentioned earlier, the standard shared mesh algorithm [11], [12] takes advantage of constraint-based shortest path algorithms for the path calculation process. The algorithm does not consider SLA parameters as the constraints in its path calculations. It is only considered in some performance evaluations as the original shared mesh path protection scheme.

In [23], the authors have discussed an SLA-aware shared mesh protection algorithm in which the partial link-disjoint protection technique was presented and the link-availability and hop count were considered as the main constraints. The algorithm discussed in [23] has considered SLA parameters as important factors to guarantee customers' requests reliability. The cost function definitions for both primary and backup paths' calculations in [23] and [24] have enabled the algorithm to introduce a novel case of protection, partial link-disjoint protection, to increase the availability satisfaction rate, and to reduce the restoration time of shared mesh WDM networks. The authors in [23] and [24] have

presented a lightpath provisioning mechanism by which primary paths are first calculated. Backup paths are calculated if the primary paths cannot satisfy the SLA requirements of connection requests. Since the path calculation process presented in [23] and [24] is an efficient way of utilizing network resources, it is adopted as the main path calculation scheme in Chapters 6 and 7. The other concept presented in [23] is the partial link-disjoint concept which is taken into account when primary and backup paths are calculated. The link cost functions presented in [23] modify the cost of the links based on the availability of the links while the cost functions consider the disjoint degree of primary and backup paths. The disjoint degree affects the value of links' cost in a way that a higher disjoint degree of two paths translates to a lower link cost. The path availability analysis of the partial disjoint paths is presented later in Section 2.5.4. Although the simulation results presented in [23] show that the mechanism has had an acceptable network performance, it has considered neither the connection priority nor the connection holding time as SLA requirements. In other words, [23] has not discussed how the changes on the number of the high-priority connections and their durations affect the network performance. Moreover, the algorithm presented in [23] has not been designed in a way to benefit from a dynamic SLA communication mechanism and modify the customers' requirements dynamically based on the available resources offered by service providers. Chapter 6 introduces an SLA-aware mechanism which not only takes advantage of the dynamic negotiation infrastructure presented in Chapter 3 to negotiate traffic characteristics, but it also presents a remedy for those high-priority connection requests which are blocked by the mechanisms proposed in [23] and [24]. How the mechanism presented in Chapter 6 addresses the above shortcomings is discussed in the following two paragraphs.

In optical network metropolitan/access layers, there are many applications generating QoS-based traffic such as voice or video traffic which are mainly high-priority traffic and require special treatment in terms of routing and resource allocation. Examples of such application are voice over IP, video conferencing, and some online gaming applications which set some specific QoS parameters. However, the majority of the existing SLA-aware algorithms have been evaluated employing a small portion of the traffic as high

priority, and short connection holding times. That is, mechanisms which consider variations on the number of high-priority requests and their durations as factors of SLA negotiation are still required. The connection duration or connection holding time is another crucial SLA parameter. Many studies have considered connections duration as one of the important factors in SLA-based routing mechanisms [25] [26] [27] [28] [29]. Chapters 6 and 7 employ the connection duration as a negotiating factor in the routing and path calculation processes.

The mechanisms and algorithms proposed in Chapter 4 and Chapter 5 are priority-aware mechanisms that take advantage of new path metrics proposed in these two chapters to serve a higher percentage of high-priority requests. In Chapter 4, a static priority-aware pre-provisioning algorithm is proposed based on the SLA parameters negotiation for shared-mesh WDM networks. In Chapter 5, two priority-aware algorithms are introduced for survivable shared mesh WDM networks. Since the pre-provisioning algorithm presented in Chapter 4 benefits from static SLA parameters negotiation, dynamic concept for dissemination of path availability information is extended in Chapter 5. In addition, Chapters 4 and 5 focus on the priority-aware mechanisms which are designed for connections with a small percentage of high-priority requests and short durations. That is, the high-priority traffic with long connection holding times are not applied to and evaluated through such mechanisms. Chapter 6 extends the work presented in Chapters 4 and 5 by proposing new path attributes and mechanisms to study the effect of variations on the number of high-priority requests and their durations on network performance. Considering the new type of traffic introduced in Chapter 6, in addition to the priority level of the traffic, the duration of the connection requests plays an important role on how the connection requests should be served. Therefore, a path constraint based on a combination of connection availability and connection holding-time is introduced in Chapter 6 for SLA-aware routing mechanisms other than a path metric relying only on connection availability.

Exploiting the knowledge of the holding time of connection requests has been the core idea presented in [25] and [26] to minimize resource overbuild in the form of backup capacity and hence achieving better resource-usage efficiency. The algorithm proposed in

[25] has improved sharing of backup resources by applying the holding time directly on the path computation process. In [26], a new holding time based algorithm has been proposed by which all existing connections that have not been affected by failures during their lifetime are allocated a new SLA availability target which is a function of holding-time. Unlike the algorithms presented in [25] and [26], the mechanism proposed in Chapter 6 does not affect the routing and wavelength assignment process directly, but takes advantage of holding time as *a priori* knowledge to determine when the best time is to serve requests and provision the already buffered high-priority requests.

SLA-based algorithms working based on the connection holding-time have also been discussed in [27], [28], and [29]. As authors in [27] have proposed, if the SLA requirement of a connection is violated, one more wavelength on each backup link of the availability-downgraded connection is newly assigned. The new cost function proposed in [27] has considered the capacity of the backup paths so that the availability requirements are satisfied. In [28] and [29], SLA-based algorithms have been proposed to accommodate customer-specific requirements. These algorithms assume that some connections may need extra protection at certain periods of time. The mechanisms in [28] and [29] have proposed that a connection can be protected with different SLA requirements at different times over the entire holding time of the connection. The mechanism presented in Chapter 6 assumes that the SLA requirement of the connection is not changing over the holding-time of the connection.

Authors in [30] have developed a dynamic provisioning in SLA-based mesh networks. As mentioned in [30], the revenue earned by an ISP is a function of holding time. In the scheme proposed in [30], resource preemption has been introduced to balance the bandwidth allocation and enhance the performance of provisioning. To avoid or minimize the SLA violation, the authors of [30] have developed a priority factor which can enable an ISP to satisfy more SLAs, improve the network's bandwidth utilization, and increase the service provider's net revenue. According to the authors, [30] has been the first study to jointly consider SLA, dynamic resource preemption, and economic issues in telecom mesh networks, a topic that should receive more attention for future network commerce. Similarly, in Chapter 7, a new path attribute is introduced by which the SLA violation is

controlled and monitored. The path metric introduced in Chapter 7 is a statistical attribute of the paths obtained from already established paths.

Definition: SLA violation risk

The risk of SLA violation has been defined in [31] *as follows, in which ADT is the allowable down time and DT is the actual down time of a connection.*

SLA violation risk $= P_r(ADT < DT)$

The authors in [32] have proposed an event-triggered re-provisioning scheme to meet SLA satisfaction requirements. Chapter 7 takes advantage of the concept of the residual graph presented in [32] including residual holding time, residual allowed down time, residual bandwidth, and in general residual status of the network to minimize the number of SLA violations over the entire connection duration period. Similar to [30], a dynamic resource preemption mechanism has been used in [32] to efficiently allocate network resources and better guarantee the success of re-provisioning. However, in Chapter 7, a history-aware mechanism is introduced which uses the novel path attribute proposed in that chapter to improve the network performance compared to existing SLA-aware algorithms. In addition to the proposed path attribute, a new optimal cost function for the routing algorithm is presented in Chapter 7.

The approach in [33] will allow lightpaths to pre-empt each other during an outage. Therefore when a failed lightpath approaches its SLA limit, it can pre-empt a lightpath which has not experienced a significant outage to use its bandwidth, and avoid violating its own SLA. Although the goal in Chapter 7 is to avoid SLA violation, the focus is not on pre-empting the lightpaths during an outage period, but is on benefiting from the residual status of the network to satisfy the SLA requirements of additional connections.

2.5 MATHEMATICAL MODELS FOR AVAILABILITY ANALYSIS

The network components are represented as $G\ (V,E,W,A_{ij})$, where V is the set of nodes, E the set of links, W the set of free wavelength per each link, and A_{ij} the link availability for

a pair of nodes *(i,j).* A connection request is considered in the form *(s,d,A_{sdr},p),* where *s* is the source, *d* is the destination, A_{sdr} is the availability requested for the lightpath between *s* and *d* , and *p* shows the class of traffic which could be either Gold or Silver. The definition of the availability of a connection for different protection schemes has been discussed in [24] and [34] in detail. The following sections investigate the mathematical models for different network resources, protection schemes, and mechanisms.

Definition: Gold/Silver/Bronze priority levels

Several priority levels for connection requests are considered in this thesis based on the requested availability of the requests. High-priority requests are known as Gold with requested availability of 0.9999, low-priority requests as Silver with requested availability of 0.999, and requests with no priority significance as Bronze with no availability consideration [7] [21] [22] [30].

2.5.1 Link availability

A network link's availability can be estimated based on its failure characteristics. Upon the failure of a link, the link is repaired and restored to be "as good as new". Consequently, the availability of a link *j* can be calculated using Equation 2.1. In this equation, MTBF represents mean time before failure, MTTR represents mean time to repair, *j* represents a link, and A_j is the link availability.

$$A_j = \frac{MTBF}{MTBF + MTTR} \qquad 2.1$$

Based on the definition of mean time between failures and mean time to repair, MTBF cab be written as MTBF=1/λ_f , and MTTR can be considered as failure holding time. Then another similar definition presented in [23], the availability of a fiber link *j* can be calculated based on the fiber link's failure rate (denoted as λ_f) and the average time to fix a failure, i.e., failure holding time (denoted as H_f) through Equation 2.2.

$$A_j = 1 - H_f \times \lambda_f \quad [23] \tag{2.2}$$

2.5.2 Path availability for the NP scheme

When a connection is not protected, it is available only when all the network components along its primary path P are available. That is, the path P is available as long as all fiber links along its route are available. The path availability, A_p then can be calculated through Equation 2.3 in which A_js are the availability of the links forming the path P, j denotes the set of components used by path P [23].

$$A_p = \prod_{j \in P} A_j \tag{2.3}$$

2.5.3 Primary/backup path availability

Availability of the primary and backup paths is calculated through Equations 2.4 and 2.5 where A_{pCn} and A_{bCn} are the availability of the primary and backup paths, respectively, for the n^{th} connection request C_n.

$$A_{pC_n} = \prod_{(i,j) \in C_{n(primary-path)}} a_{(i,j)} \tag{2.4}$$

$$A_{bC_n} = \prod_{(i,j) \in C_{n(\ backup-path)}} a_{(i,j)} \tag{2.5}$$

2.5.4 Joint Path Availability

In a conventional shared mesh optical network, each connection corresponds to a pair of link-disjoint paths, i.e., one primary path P and one link-disjoint backup path B. Spare resources can be shared by different backup paths on condition that their corresponding primary paths do not traverse common links. Only if primary path P and backup path B

both fail at the same time, will the connection be unavailable. Therefore, the partial link-disjoint availability of path P and path B can be computed as shown in Equation 2.6. In this equation, A_P and A_B represent the availability of primary path and backup path, respectively. The parameter θ denotes the probability that the connection can use the spare capacity reserved in backup path B to recover from failures of primary paths P, which is determined by the probability that primary paths of other connections sharing backup resources with the connection fail before the failure of the connection [23].

$$A_{PB} = 1 - (1 - A_P)(1 - \theta A_B) \quad [23] \tag{2.6}$$

As discussed in [23] in detail, in the case of multiple link failures, more than one primary path may fail at the same time in the network. If other connections which share backup resources with a connection fail before the failure of the connection, they will use the spare resource to restore. In this case there will be no backup resource for the connection to recover if its primary path fails. If more connections share spare resources with the connection, there will be more possibility for failed connections to occupy the sharing backup resources. This results in having a smaller value for θ, which means less probability for the connection to use backup path B to recover its primary path failure. However, in the case of single link failures, only one connection may fail at any time. Therefore, θ can be set to 1 [23].

Authors in [21], [22], and [23] have discussed the definition of the joint path availability of a pair of primary and backup paths in detail. Assuming that a single failure is considered for the primary paths whose backup paths share the same resources, the availability formulas discussed in [21], [22], and [23], are summarized as Equations 2.7 and 2.8.

$$A_{G(s,d)} = \prod_{i,j \in P} A_{PG(i,j)} + \prod_{i,j \in B} A_{BG(i,j)} \left(1 - \prod_{i,j \in P} A_{PG(i,j)} \right) \tag{2.7}$$

$$A_{S(s,d)} = \prod_{i,j \in P} A_{PS(i,j)} + \prod_{i,j \in B} A_{BS(i,j)} \left(1 - \prod_{i,j \in P} A_{PS(i,j)} \right) \quad 2.8$$

where $A_{G(s,d)}$ and $A_{S(s,d)}$ are availability of a pair of primary and backup paths from *s* to *d* for Gold and Silver class of traffic, respectively, $A_{PG(i,j)}$ and $A_{PS(i,j)}$ are the link availabilities forming the primary paths for Gold and Silver class of traffic, respectively, $A_{BG(i,j)}$ and $A_{BS(i,j)}$ are the link availabilities forming the backup paths for Gold and Silver class of traffic, respectively, and P and B are the set of the links forming primary and backup paths, respectively.

2.5.5 Path availability for dedicated path protection scheme

When primary path P fails, its traffic is switched to backup path B as long as B is available; otherwise, the connection becomes unavailable until the failed component is replaced or restored, or becomes available. That is, the connection is up only when P is up or B is up when P fails. A_{PB} can thus be computed by Equation 2.6 for θ =1 presented as the joint path availability in Equation 2.9, where A_P and A_B are the availability of primary P and backup B paths, respectively.

$$A_{PB} = A_P + A_B \times (1 - A_P) \quad 2.9$$

2.5.6 Path availability for the shared path protection scheme

Assuming S_p is the set of all primary paths (except P) whose backup paths are sharing some resources with B, connection C is available if i) P is available; or ii) P is unavailable, B is available, and the failure on P happens before failure to other primary paths in S_p. Therefore, A_{PB} can be computed through Equation 2.9 in which the parameter θ is substituted by Equation 2.10 presented in [35] where *n* is the size of S_p; and P_i is the probability that exactly *i* primary paths in S_p are unavailable. The final formula for the path availability of the CSPP scheme is as Equation 2.11.

$$\theta = \sum_{i=0}^{n} \frac{P_i}{i+1} \quad [35] \tag{2.10}$$

$$A_{PB} = A_P + A_B \times (1 - A_P) \times \sum_{i=0}^{n} \frac{P_i}{i+1} \quad [35] \tag{2.11}$$

P_i can be easily calculated by enumerating all the possible i unavailabilities among the n sharing primary paths. The correctness of the Equation 2.11 has been verified in [35] through an ILP approach.

2.5.7 Path availability for priority-aware shared path protection schemes

The availability of a connection depends in this scheme on the class of service of the connection. So, if C_G is a Gold connection carried by one primary path P_G and protected by one backup path B_G, which is link disjoint with P_G, then, even if S_{PG} contains primary paths of both Silver and Gold connections, the availability of C_G is influenced only by the Gold ones. S_{PG} is the set of all primary Gold connections (except P_G) whose backup paths are sharing some resources with B_G. In other words, C_G is available if 1) P_G is available; or 2) P_G is unavailable, B_G is available, and the failure on P_G happens before failure to other gold primary paths in S_{PG}. Therefore, C_G can be computed using Equation 2.12 presented in [22].

$$A_{PB_G} = A_{P_G} + A_{B_G} \times \left(1 - A_{P_G}\right) \times \sum_{i=0}^{n_G} \frac{P_{G_i}}{i+1} \quad [22] \tag{2.12}$$

where n_G is the number of Gold primary paths in S_{PG} and P_{Gi} is the probability that exactly i Gold primary paths in S_{PG} are unavailable. On the other hand, if C_S is a silver connection whose primary path P_S is link disjoint with the backup path B_S, then, the availability of C_S is influenced by both Gold and Silver connections primary paths present in S_{PS}. In other words, C_S is available if 1) P_S is available; or 2) P_S is unavailable, B_S is available, no gold primary path in S_{PS} fails, and the failure on P_S happens before

failure to other silver primary paths in S_{PS}. Therefore, A_{PBS} can be computed using Equation 2.13 presented in [22].

$$A_{PB_S} = A_{P_S} + A_{B_S} \times \left(1 - A_{P_S}\right) \times \sum_{i=0}^{n_S} \frac{P_{S_i}}{i+1} \times P_{G_0} \quad [22] \tag{2.13}$$

where n_S is the number of Silver primary paths in S_{PS} ; P_{G0} is the probability that no Gold primary path in S_{PS} is unavailable and P_{Si} is the probability that exactly i Silver primary paths in S_{PS} are unavailable.

2.6 ROUTING STRATEGIES

Network architectures such as GMPLS have steadily increased the interest in QoS-based routing in the networks. The goal of QoS routing is to find a network path which satisfies the given constraints, and simultaneously optimizes resource utilization. The path selection process uses the available link state information to compute the best path to accommodate QoS requirements of lightpaths.

As discussed in [1] and [2], the main objectives of QoS-based routing can be summarized as i) Dynamic path calculation process, ii) Network resource optimization, and iii) Performance improvement. However, as per the results published in [1], [36], and [37], the problem of determining a QoS route that satisfies two or more path constraints is known to be NP-complete. Hence, much of the focus over the last few years has been on the development of heuristics and approximation algorithms for multi-constrained QoS paths [38].

The authors in [39] and [40] have categorized the routing strategies over optical networks to the following major approaches:

i) Fixed routing: the fixed routing is the most straightforward approach to routing a connection. It always chooses the same fixed route for a given source-destination pair. The fixed shortest-path routing is an example of the fixed routing scheme [39].

ii) Fixed-alternate routing: unlike the fixed routing, the fixed-alternate calculates multiple routes. In fixed-alternate routing, each node in the network is required to maintain a routing table. When a connection request arrives, the source attempts to establish the connection on each of the routes from the routing table in sequence, until a route with a valid wavelength assignment is found [39].

iii) Adaptive routing: the adaptive routing chooses the route from a source to a destination dynamically. The path calculation process depends on the network state. The network state is determined by the set of all connections that are currently in progress. The adaptive routing is well-suited for use in WDM optical networks. Employing the adaptive routing approach, a connection is blocked only when there is no route from the source to the destination in the network. An advantage of adaptive routing is that it results in lower connection blocking than fixed and fixed-alternate routing. However, it requires extensive support from the control and management protocols to continuously update the routing tables at the nodes [39].

Path calculation algorithms mainly used in this dissertation are Dijkstra and k-shortest path. The algorithms and their applications in optical transport networks have been discussed in [41]. Adaptive routing is also selected as the routing approach used for the routing mechanisms proposed in this thesis. The reasons for choosing this approach are given in the next section when the combination of the wavelength assignment approaches and routing strategies is evaluated. Although adaptive routing is the basis of the routing algorithms proposed in this thesis, priority-aware and SLA-based mechanisms are proposed in Chapters 4 to 7 to satisfy the QoS-based routing requirements in traffic engineered environments.

2.7 WAVELENGTH ASSIGNMENT APPROACHES

As per the study done in [39], wavelength assignment approaches can be categorized into the following main approaches:

i) Random Wavelength Assignment (R): Using this scheme, among the available wavelengths, one is chosen randomly (usually with uniform probability) [39].

ii) First-Fit (FF): In this scheme, all wavelengths are numbered. When searching for available wavelengths, a lower numbered wavelength is considered before a higher-numbered wavelength. The first available wavelength is then selected. Compared to Random wavelength assignment, the computation cost of this scheme is lower [39].

iii) Least-Used (LU): LU selects the wavelength that is the least used in the network. The performance of LU is worse than Random, while also introducing additional communication overhead. The scheme also requires additional storage and computation cost; thus, LU is not preferred in practice [39].

iv) Most-Used (MU): MU is the opposite of LU in that it attempts to select the most-used wavelength in the network. It outperforms LU significantly. The communication overhead, storage, and computation cost are all similar to those in LU [39].

v) Min-Product (MP): MP is used in multi-fiber networks. In a single-fiber network, MP acts as FF [39].

vi) Least-Loaded (LL): The LL heuristic, like MP, is also designed for multi-fiber networks. That is, it reduces to FF in single-fiber networks [39].

vii) MAX-SUM (MΣ): MΣ was proposed for multi-fiber networks but it can also be applied to the single-fiber case. MΣ considers all possible paths in the network and attempts to maximize the remaining path capacities after lightpaths establishment [39].

As the simulation results in [39] for the blocking probability of various wavelength assignment approaches has shown, although the FF method has not represented the best

performance among the other wavelength assignment schemes, it has been a marginally better choice compared to other approaches, in sense of simplicity. In addition, the blocking probability evaluation of combination of various wavelength assignment approaches with different routing strategies in [39] has shown that the FF technique together with adaptive routing strategy have made an appropriate combination of routing and wavelength assignment by better blocking rate performance. That is the main reason for choosing FF and adaptive routing as routing and wavelength assignment approaches in this thesis. However, in some mechanisms proposed in this thesis, more effective routing and wavelength assignment approaches are introduced.

Although the FF technique might be a suitable choice for wavelength assignment of the primary/backup paths for no protection and dedicated protection schemes, other wavelength assignment techniques should be investigated in the shared protecting paths in which a single WDM channel can be shared with other paths. To satisfy this condition, a new wavelength assignment scheme for priority-aware mechanisms is proposed in Chapter 5. Chapter 5 describes how wavelengths are assigned to connection C's backup links in a different way. The wavelength assignment algorithm presented in Chapter 5 is based on the FF technique which takes the sharability of the backup paths into account.

2.8 SUMMARY

This chapter has described a literature overview of the main building blocks of SLA-based architectures over priority-aware shared mesh optical networks. The fundamental module of the discussed architecture has been introduced as the SLA negotiation infrastructure. The standardized protocols and existing algorithms for path attributes and SLA parameters negotiation have been studied in this chapter and shortcomings of each have been identified. An SLA negotiation mechanism which has benefited from the existing routing protocols was presented as the solution to those shortcomings.

The other main module of the discussed architecture was presented as routing and wavelength assignment mechanisms. A thorough study of the priority-aware and SLA-

based mechanisms including the existing mechanisms, their advantages and disadvantages, and the remedy for the shortcomings has been provided. The mathematical models for availability analysis of different routing mechanisms, protection schemes, and network resources have been discussed. Different routing strategies and wavelength assignment approaches have been studied as well. The rational for choosing any strategy or approach has been included in this chapter. Alternative and effective routing and wavelength assignment strategies have also been proposed to address the shortcomings of the existing approaches regarding sharability of backup paths.

CHAPTER 3 DYNAMIC SLA NEGOTIATION INFRASTRUCTURE OVER SHARED MESH OPTICAL NETWORKS

3.1 INTRODUCTION

Routing within optical networks relies on knowledge of network topology and resource availability. This information may be gathered and used by a centralized system, or by a distributed link state routing protocol. In either case, the first step towards network-wide link state determination is the discovery, by each route, of the status of local links to all neighbors. To disseminate TE information among entire nodes of a network, the information should be propagated inside and outside the autonomous system, along the path from source to destination. For intra-domain TE-information dissemination, OSPF-TE opaque LSAs with newly proposed extensions are used in this chapter. For inter-domain TE-metrics propagation, new TE extensions on BGP are proposed in this chapter.

In a multi-homed network topology, link attribute information can be communicated using dynamic SLA negotiation mechanisms. The customer side of the network is exposed to SLA information from all the service providers to which it is connected. The customer has the choice to pick the service provider that is the most suitable for satisfying the requested connection.

This chapter presents a dynamic SLA negotiation mechanism considering intra/inter-domain communications over shared mesh optical networks. The intra-domain negotiation mechanism propagates the link attribute as SLA parameters while an inter-domain mechanism advertises the proposed SLA-based traffic engineering path constraints. The chapter shows how SLA negotiation protocols together with the proposed traffic engineering attributes improve the performance of priority-aware algorithms.

The chapter is organized as follows: Section 3.2 identifies the motivations and objectives behind this chapter's discussion. The proposed TE extensions to the routing protocols are

introduced in Section 3.3. Some scalability issues are discussed and addressed in Section 3.4. Network performance evaluation is presented in Section 3.5. Section 3.6 summarizes the chapter discussions.

3.2 MOTIVATIONS AND OBJECTIVES

In some cases, the requested parameters in an SLA are beyond the capacity of the network, and the connection is easily rejected or blocked. To give the customer a chance to choose another provider, or in case of having only one provider, to comply with the provider's network capacity as much as possible, an automatic, bidirectional, and dynamic mechanism for SLA parameters negotiation between service providers and customers is required. This mechanism helps service providers to control the network resource assignment in WDM networks. This is the motivation for proposing a dynamic mechanism to negotiate specific SLA parameters or any other metrics which may be desirable. Some paradigms of the desirable SLA parameters, such as TE path/link attributes will be introduced in the following chapters.

This part of the thesis is the first step of the mutual and bidirectional negotiating communications process between customers and service providers based on the SLA parameters. This work keeps the options open for employing dynamic mechanisms by which customers and service providers can negotiate vital SLA parameters before actually placing the order and establishing the requests.

3.3 PROPOSED TRAFFIC ENGINEERING EXTENSIONS

An SLA is a common means of communication between customers and service providers through which one of the most important parameters for the customers, connection availability, is requested. The service provider goal is to provide a reliable connection with the minimum allocated resources over a shared-mesh path restoration scheme in WDM networks. It is required to show what type of SLA parameters or path/link metrics can be communicated over the proposed negotiating mechanism and how the new

negotiation mechanism can handle the QoS-based routing and wavelength assignment (RWA) using the new mechanism. To achieve this goal, new path constraints by which network performance is enhanced will be introduced in the following chapters. Here, the general communication mechanism of such attributes will be discussed.

3.3.1 Intra-AS negotiation

To disseminate the SLA parameters inside an area, Type-10 OSPF opaque LSAs are a suitable choice since Type-10 opaque LSAs are not flooded beyond the borders of their associated area. In addition, as defined in [10], to disseminate the SLA parameters inside an AS, Type-11 opaque LSAs are a suitable choice. In OSPF-TE, a top-level link TLV in the payload field describes the characteristics of a single link [8]. The link TLV and its sub-TLVs have a format shown in Table 3.1. The new sub-TLV, proposed here to carry and propagate link-attribute (LA) inside an AS, is defined in Table 3.2. Using this new sub-TLV, an important SLA parameter, link availability, can be flooded all through an AS. Although the new TLV is a part of OSPF regular flooding, a solution for controlling the overheads caused by this TLV is introduced in the following sections.

Table 3.1 Link TLV payload format

Link Type	Link Length
Link Sub-TLV 1	
Link Sub-TLV 2	
…..	
Link Sub-TLV n	

Table 3.2 New link attribute sub-TLV

LA Type	LA Length
LA Value	

3.3.2 Inter-AS negotiation

Since in a general case there is no internal gateway protocol (IGP) peering between two different ASs, to find a way to get LSAs describing an AS's traffic engineering properties into the traffic engineering database (TED), [42] suggests that the edge routers (ERs) advertise the external link states, internally to its AS and generates an LSA describing its own side of a link. Since in BGP, no topological and/or state information is allowed to be disseminated beyond ASs' boundaries, the link attribute information cannot be disseminated from inside one AS to another AS. Based on [42], the link state of the links connecting different ASs is advertised inside the ASs by ERs of the same ASs. A number of new TE-based path constraints will be proposed in Chapters 4, 5, 6 and 7 which will distribute some important and effective attributes of the paths calculated in any internal routers and are propagated from the ERs of an AS to the other AS.

The path attribute of any source to any ERs inside an AS should be propagated among different ASs. Then the ERs in each AS need the related information retrieved from the path-attribute (PA) matrix of the neighboring ASs. Since there is no IGP peering between ERs of different ASs, we need another mechanism (other than OSPF-TE) to send the required information from an ER in one AS to another ER in another AS. Since the communications between ERs of different ASs are done through the BGP protocol, an extension to BGP is required to be defined to support the TE-based SLA-constraint and also to transfer a part of the PA matrix of the remote AS to the neighboring one without changing the path selection process of the IGP and BGP protocols. To do so, OSPF-TE and BGP-TE packets are required to be used with specific extensions for carrying SLA-related constraints. Since BGP supports a hop-by-hop routing paradigm and is a path-

vector protocol, whereas OSPF is a source routing and a link-state protocol, the proposed mechanism combines these two protocols to work together for multi-domain SLA parameters dissemination.

In conventional BGP [43], the advertisements propagated between BGP routers are encapsulated in the Update messages. To consider TE-constraints, a new path attribute is added into BGP as an extension. The proposed TE-metric is advertised together with the path information in both intra-AS and inter-AS manners using internal BGP (IBGP) and external BGP (EBGP), respectively. The proposed format of the extension in this thesis is a TLV format, where the proposed TE attribute is carried by a group of TLV fields, specifying the value of the corresponding TE metric. The proposed path attributes are carried through Path Attribute filed in the Update messages in BGP packets. The Path Attribute filed is a triple format of attribute type, attribute length, and attribute value of variable length [43].

The EBGP is used to exchange information about paths and related TE metrics among different ASs. ERs within an AS will advertise path attribute values for each destination to their neighbors that are the ERs in other ASs. The IBGP runs among routers within the same AS. According to IBGP with a TE extension, when an ER in an AS receives the TE path attribute for a destination from another AS, it will send these externally learned paths to internal nodes. In order to cope with legacy BGP routers, the new TE attributes proposed in this thesis are optional and transitive. That is, the proposed attribute may not be recognized by some legacy BGP routers and this attribute should be passed on even if it is not recognized. Accordingly, the BGP routing table is extended to keep the TE-related information. Since only TE-related information is transferred through BGP and the BGP path selection process is not affected by these TE-related changes, there is no need to define any new state machines.

Several new path attributes will be introduced in detail in the following chapters. Examples of the proposed path attribute propagation in this thesis are the initial maximum path availability presented in Chapter 4, the maximum path availability presented in Chapter 5, the time-aware maximum path availability presented in Chapter

6, and the path risk factor presented in Chapter 7. The new sub-TLV in BGP-TE Update packets for carrying TE path attributes in an ER calculated from any node inside the corresponding AS (including the other ERs) is presented in Table 3.3. Figure 3.1 shows how the mechanism disseminates the TE-related SLA-related packets.

Definition: Path attribute matrix (PA)

The packet routed from one AS to another AS should be routed through one of the edge routers. The routers inside an AS advertise the link attribute of the associated links into the AS. Using this information, the PA matrix is built in all decision making nodes inside an AS including edge routers. Then all the edge routers of an AS have a matrix of the form below for a network with m nodes:

$$PA_{mxm} = \begin{bmatrix} PA_{(1,1)} & \cdots & PA_{(1,j)} & \cdots & PA_{(1,m)} \\ \vdots & & \vdots & & \vdots \\ \vdots & & \vdots & & \vdots \\ PA_{(m,1)} & \cdots & PA_{(m,j)} & \cdots & PA_{(m,m)} \end{bmatrix}$$

If the j^{th} node is one of the edge routers as shown in Figure 3.1, ER_j will advertise the path attribute value of all routes ending at ER_j. This information is summarized in the j^{th} column of the PA matrix. In the current operation of OSPF-TE, the label switching routers (LSR)s at each end of a TE link advertise LSAs describing the link. Unlike regular routers inside the AS that only advertise the link attributes, ER_j will advertise all the information of the j^{th} column of the PA matrix of the associated AS using the proposed sub-TLVs of Update messages presented in Table 3.3, in addition to the link attribute of the external link.

Here, each edge router maintains two matrices. One from its associated AS which is to be advertised to the other AS, and the other which is received from another AS informing it about the conditions on the neighboring AS which can be flooded inside the AS. In the case of National Science Foundation Network (NSFNet) topology shown in Figure 3.3, the j^{th} edge router will advertise a path attribute sub-TLV of 14 PA values including the j^{th} column of the PA matrix.

Table 3.3 Proposed Path Attribute sub-TLV

PA Type	PA Length
$PA_{(1,j)}$	
$PA_{(2,j)}$	
……	
$PA_{(i,j)}$	
……	
$PA_{(m,j)}$	

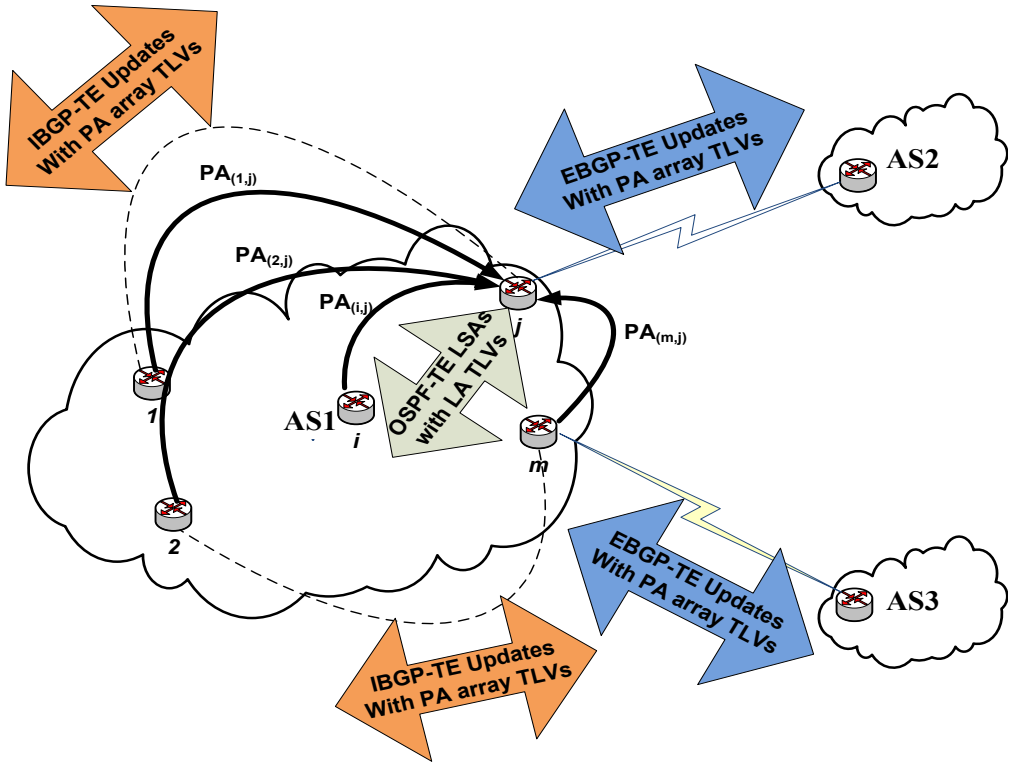


Figure 3.1 Inter-AS dynamic SLA-related packets dissemination

3.4 SCALABILITY ISSUES

Since the proposed mechanism in this chapter, to disseminate link/path attributes, may cause heavy control overheads in a dynamic environment such as the control plane of GMPLS-based networks, employing some alternative means of communication to reduce the overheads and resolve the possible scalability issues is a wise step. One way of reducing link states overhead is to use the concept of path state advertisement (PSA) [15] rather than LSA. An improved OSPF-TE protocol has been introduced in [15]. The proposed protocol in [15] not only has disseminated link state information very effectively, but also has advertised link information if necessary.

The parameters shown in Table 3.4 and Table 3.5 are proposed in this chapter to be carried using the path TLV payload and PSA sub-TLV proposed in [15]. The PA value change sub-TLV is the change of any desirable attributes for link or path in the lightpath, and the PA sub-TLV indicates the attribute, constraint or metric applied to all links.

Table 3.4 Path TLV payload format

Path Type	Path Length
PA value change Sub-TLV	
PA Sub-TLV (optional)	

As a special case discussed in [15], the "PA value change Sub-TLV" field, in path TLV payload presented in Table 3.4, is the increment or decrement of bandwidth in the lightpaths, and the "PA Sub-TLV" field represents the wavelengths used in all links. Theoretical analyses and simulation results in [15] have shown that the OSPF-TE's control overheads could be reduced between 3 and 7 times in networks studied compared to the conventional flooding mechanism. Based on the graphs presented in [15], the blocking probability has also been reduced, and the performance of optical networks has been improved significantly.

Table 3.5 PSA Sub TLV for the proposed path attribute

PA value change Type	PA value change Length
PA value change	
PA Type	PA Length
PA_1	
….	
PA_m	

In [15], an LSA update mechanism has been proposed in which:

1) The standard OSPF-TE LSAs are propagated periodically to advertise the total link resources or when a link is down or restored. These standard OSPF-TE messages advertise all detailed information about TE links including Link Type, Link ID, Traffic Engineering Metric, Maximum Bandwidth, Maximum Reservable Bandwidth, Administrative Group, Link Local/Remote Identifiers, Link Protection Type, Interface Switching Capability Descriptor, Shared Risk Link Group.

2) Otherwise the proposed PSAs are propagated as follows. For intra-domain communications, only source LSR floods PSAs, and for inter-domain negotiations, only edge routers flood PSAs. Assuming that not all LSRs flood PSAs, this mechanism can cope with the scalability issues by minimizing the number of flooded advertisements. In addition, to keep the control overhead small, PSAs notify PA changes on a lightpath, rather than notify how much resources are available on these links.

3.5 PERFORMANCE ANALYSIS

The network performance is evaluated from three different and important points of view:

1) The control overhead reduction employing the proposed method in [15] by which it is shown that the mechanism introduced in this chapter is easily scalable
2) An analysis of the propagation delay of the flooded information
3) The performance improvement that the proposed mechanism in this chapter brings to the network. The detailed results of this part of the study are also available in [44] as one of the published contributions of this thesis.

3.5.1 Control overhead analysis [15]

Since control overheads of update advertisements is the main concern, only network resources consumed by OSPF-TE messages are considered. Three types of LSA flooding mechanisms are compared in [15]. In period-based update (PU), all LSRs advertise their LSAs for a specific constant interval considered here 100μs. In threshold-based update (TU) when the variance of a link's state is below a threshold (T_h), LSA is not advertised. Otherwise, this LSA is flooded. In immediate PSA update (IU) which is the proposed mechanism in [15], the proposed PSAs are advertised immediately.

As the results shown in Figure 3.2, adopted from [15], the control overheads of conventional OSPF-TE has been compared to different schemes of update advertisements including the one introduced in [15]. The PU has constant control overheads. Since the PU's period is set to a large interval, T=5s, its control overheads are the smallest. The control overheads of TU and IU are proportional to loads. The simulation environment conditions employed in [15] are as follows:

1. Each link has 32 fibers. Each fiber has 2 wavelengths.
2. No Wavelength converter is deployed.
3. A Poisson process with arrival rate of β is considered for the arrival process of connection requests.

4. The holding time of the connection requests follows an exponential distribution mean $1/\mu = 60$s.
5. 5,000,000 events are simulated.
6. The confidential interval is considered 95%.
7. Route for each node pair is determined by a joint wavelength-route section (JWR) routing mechanism in which the route and the wavelength are determined in the same step.

As Figure 3.2 shows, TU has the largest control overhead. The control overheads of the conventional OSPF-TE are obtained when the threshold level $T_h = 1$, and they are about eight times more than IU's. When T_h=3, TU's control overheads are about 3 times as much as IU's. Figure 3.2 clearly shows the superiority of the PSA concept over LSA.

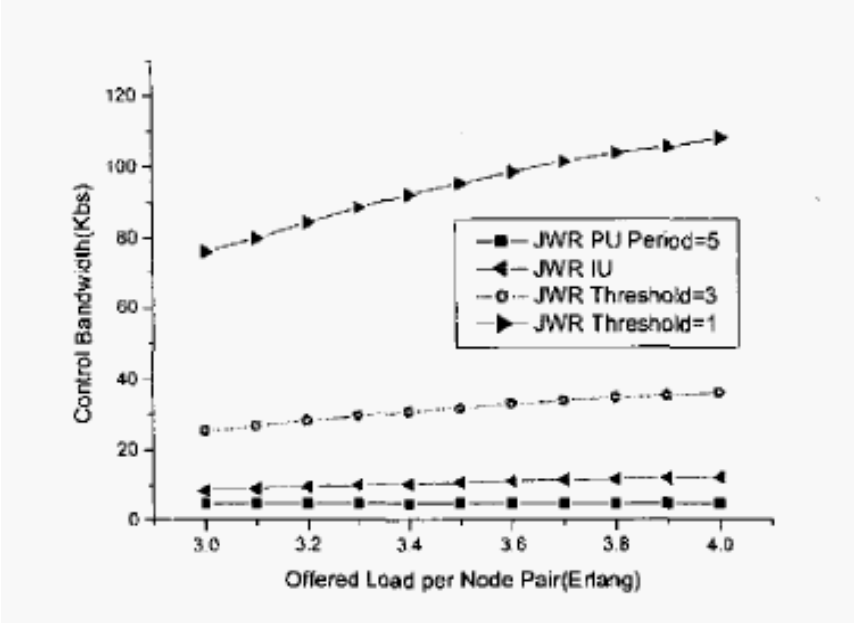


Figure 3.2 Control overheads for different update advertisement schemes [15]

3.5.2 Propagation delay analysis

The new link/path attributes should be flooded over the network after any changes to the requested connections including establishment and release. Depending on how frequently these changes take place and how long the flooded information may take to be

propagated, the validity of the information received by provisioning algorithms should be investigated. That is, an analysis comparing the maximum arrival rate of the connection with the propagation delay of the flooded advertisements should be studied. To clarify this issue, the following considerations including a numerical analysis are presented here.

First consideration: the proposed link and path attributes are propagated over the decision making nodes only rather than all nodes. The complexity of the data structure exchanged between the nodes is a function of the network size. That is, having a large number of decision making nodes in the network makes the propagated packets huge. The practical approach to this issue is employing the concept of the separation of the control plane from data plane in GMPLS networks. The decision making nodes in the control plane of such networks use the same protocols (OSPF and BGP) and sometimes the same infrastructure as the data plane uses. However, the number of the nodes propagating the information is much fewer than the number of the nodes in the data plane. In the case of NSFNet topology studied in this chapter, the decision making nodes are not 14 nodes, but much fewer.

Second consideration: benefiting from the PSA concept discussed in Section 3.4, for intra-AS communications, only source nodes flood PSAs, and for inter-AS negotiations, only edge routers flood PSAs. Since not all nodes flood PSAs, the number of the flooded advertisements is minimized. In addition, to keep the control overhead of the advertised packets small, the changes to the desirable attributes are advertised as increments or decrements values, rather than notifying the exact values of the available resources on links or paths.

Third consideration: The information regarding paths and related TE metrics among different ASs is exchanged using EBPG Update packets. The decision making nodes within an AS will advertise path attribute values for each destination to their neighbors that are located in other ASs benefiting from IBGP connections. The IBGP runs among routers within the same AS. According to IBGP with a TE extension, when a decision making node in an AS receives the TE path attribute for a destination from another AS, it

will send these externally learned paths to internal nodes. Accordingly, the BGP routing table is extended to keep the TE-related information regarding inside and outside of ASs.

Fourth consideration: assuming an average of 500km as the nodes distance, it takes 2.5ms for PSAs to be propagated on fiber traveling between two adjacent nodes. Since PSAs are advertised as the source-based packets and may take the data plane infrastructure to travel from one decision making node to another, and over NSFNet topology it may travel on average 2.8 nodes (this number is shown in AWPC performance in Figure 3.5 for a no protection scheme), the average propagation delay would be 7ms. Therefore, for the average events (including connection arrival or release) rate of less than 145 connections per second, the provisioning algorithms residing in the decision making nodes will be provided by fresh and valid information. The arrival rate considered for simulation purposes in this thesis is on average 40 connections per unit of time. Assuming that the only events causing information to be flooded are establishment or release of such connections, and the connections duration on average is one unit of time, on average 80 events per unit of time may trigger the flooding, which keeps the decision making nodes and the algorithms in the safe side in terms of receiving fresh and valid information.

Employing the above considerations, the fresh and valid information will always be available for the algorithms and decision making nodes in the network.

3.5.3 Network performance analysis

In this section, the blocking probability (BP), the availability satisfaction ratio (ASR), and the average assigned wavelengths per connection (AWPC) of the CSPP scheme are compared with the SSPP and NP schemes. BP denotes the percentage of blocked connection requests over all arriving requests. ASR represents the percentage of provisioned connections whose availability requirements are met over all provisioned connections (unblocked connections). AWPC shows the average number of assigned wavelength per connection.

Algorithms 3.1 and 3.2 introduce and compare the SSPP and CSPP schemes, respectively. Unlike the SSPP, the CSPP scheme considers links' availability as a constraint in the path calculation process. Unlike the SSPP and CSPP schemes, the NP scheme provides no backup paths for any established primary paths. The CSPP scheme receives the link availability information through the mechanism proposed in this chapter. The availability analysis and how link availability affects the path calculations were discussed in detail in Chapter 2 through Equations 2.3 to 2.11. Since at this point the main goal is to evaluate the effect of the proposed SLA parameter negotiation mechanism on the standard shared mesh protection scheme, discussions about routing and wavelength assignment mechanisms are deferred to the following chapters.

Algorithm 3.1 SSPP scheme

Input: Connection Request $\{C_n(s,d)\}$

Output: P-B pair of paths

1. $n \leftarrow 1$
2. Serve the n^{th} connection request $\{C_n(s,d)\}$
3. Apply Dijkstra's Algorithm based on free wavelengths on the links {to find the primary path P}
4. IF P exists THEN
   Assign free wavelengths to P AND
   Apply Dijkstra's Algorithm based on free wavelengths on the links {to find the link-disjoint backup path B}
   IF B exists THEN
   Assign new wavelengths to B if there is no sharable wavelengths
   ELSE
   Block the request AND Go to Step 6
   ELSE
   Block the request AND Go to Step 6
5. RETURN the P-B pair of paths
6. $n \leftarrow n+1$ AND Go to Step 2

Algorithm 3.2 CSPP scheme

Input: Connection Request $\{C_n(s,d)\}$

Output: P-B pair of paths

1. $n \leftarrow 1$
2. Serve the n^{th} connection request $\{C_n(s,d)\}$
3. Modify the link cost of the graph using Equation 4.2
4. Apply Dijkstra's Algorithm {to find the primary path P}
5. IF P exists THEN
   Assign free wavelengths to P AND
   Modify the link cost of the graph using Equation 4.3 AND
   Apply Dijkstra's Algorithm {to find the link-disjoint backup path B}
   IF B exists THEN
   Assign new wavelengths to B if there is no sharable wavelengths
   ELSE
   Block the request AND Go to Step 7
   ELSE
   Block the request AND Go to Step 7
6. RETURN the P-B pair of paths
7. $n \leftarrow n+1$ AND Go to Step 2

3.5.3.1 Simulation environment

The mechanism proposed in this chapter has been evaluated using a simulation environment developed in MATLAB. The topology selected for the simulation is NSFNet shown in Figure 3.3 with 14 nodes and 21 bidirectional fiber links of the same physical distance. The links have wavelength conversion capability with 8 wavelengths per link. To simulate a high-risk-network [23], the link availabilities are uniformly distributed between 0.99 and 0.9995 which is assigned per link prior to running the simulation. The average availability of different networks and topologies for various types of protection [45] shows the assumption made for link availability values are

reasonable. Connection availability requests are uniformly distributed between 0.99 and 1.0. A Poisson process with arrival rate of β is considered for the arrival process of connection requests. The holding time of the connections follows an exponential distribution with the mean value of μ=1. For simulation purposes, β is ranging from 20 to 70 to simulate the offered load of 20 to 70 Erlangs. The definition of offered load and Erlang are discussed in A.1 and A.2. No waiting queue has been considered for this process. For the sake of simplicity, it is assumed that all the primary paths whose backup paths share the resources are totally link disjoint and the failure of primary links at the same time is very unlikely. The level of protection is considered 100%. The protection level of a connection is defined in [46] as the percentage of the working bandwidth to be restorable by the protection path of this connection once the working path is interrupted regardless of the location of the failure pattern. Since the failure of primary paths at the same time is very unlikely, θ (see Chapter 2) is considered to be 1. To achieve a 95% confidence interval for the illustrative results, 10^5 connection requests are simulated in every experiment which may introduce a maximum error of $3x10^{-3}$, based on the error calculation presented in A.3.

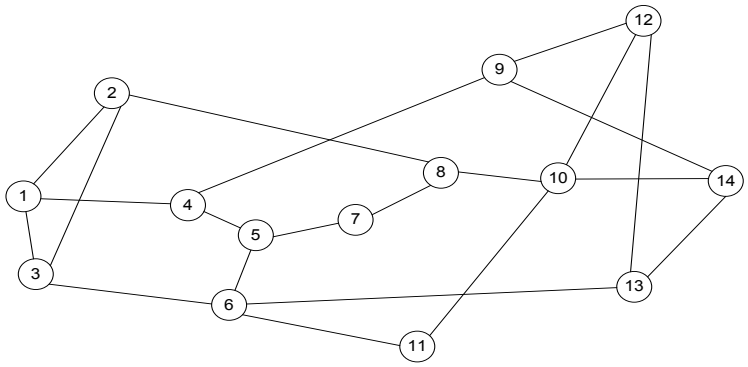


Figure 3.3 NSFNet network topology

3.5.3.2 Simulation results

Figure 3.4 shows how employing the negotiation mechanism proposed in this chapter affects the performance of the standard shared mesh protection scheme. Since the CSPP scheme benefits from the negotiation mechanism and uses link availability as a constraint in the path computation, it makes a significant improvement on the number of the

connections whose availability requests are satisfied. Clearly, the NP scheme has the worst ASR since it does not protect the paths. The ASR graphs in Figure 3.4 have an error ranging from ∓0.02% to ∓0.25%. For instance, for the arrival rate of β=40, the 95% confidence interval of ASR for the CSPP scheme is [89.8% 90.2%] which translates to a 0.2% relative error.

The CSPP scheme has better wavelength utilization (AWPC) than the SSPP scheme as shown in Figure 3.5 since the CSPP decreases the average number of assigned wavelengths to each path by 25% on average compared to the SSPP. However, the NP scheme has a lower wavelength usage in this case since it does not reserve any resources for backup path. As an estimate of error in graphs presented in Figure 3.5 and based on the standard deviation of the total number of wavelengths, for the NP scheme error deviates between ∓0.3 to ∓0.4 wavelengths and for the SSPP and CSPP varies from 0.12 to 0.2 wavelengths.

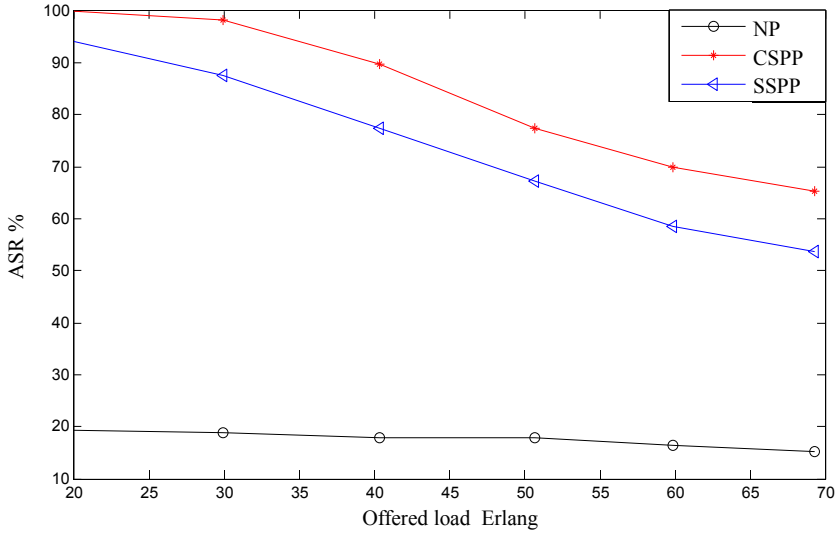


Figure 3.4 The effect of SLA negotiation on availability satisfaction rate over different protection schemes

Since the routing and wavelength assignment process for both the CSPP and SSPP schemes is the same, the CSPP is not expected to have a significant improvement in blocking probability compared to SSPP, as shown in Figure 3.6. Blocking probability of the NP is expected to be low since wavelength usage of this scheme is the lowest which

keeps the network resources free for future connection requests. The BP graphs in Figure 3.6 have an error ranging from $\mp 6x10^{-5}$ to $\mp 3x10^{-3}$.

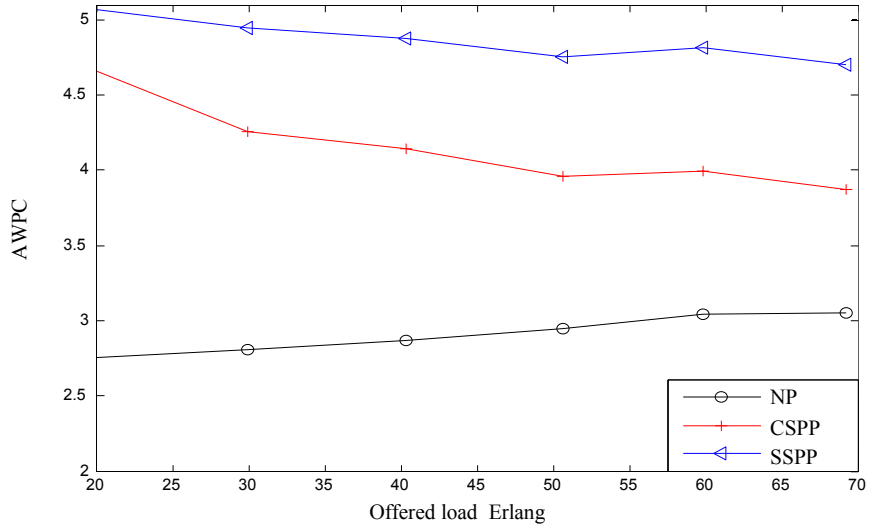


Figure 3.5 The effect of SLA negotiation on average wavelength usage over different protection schemes

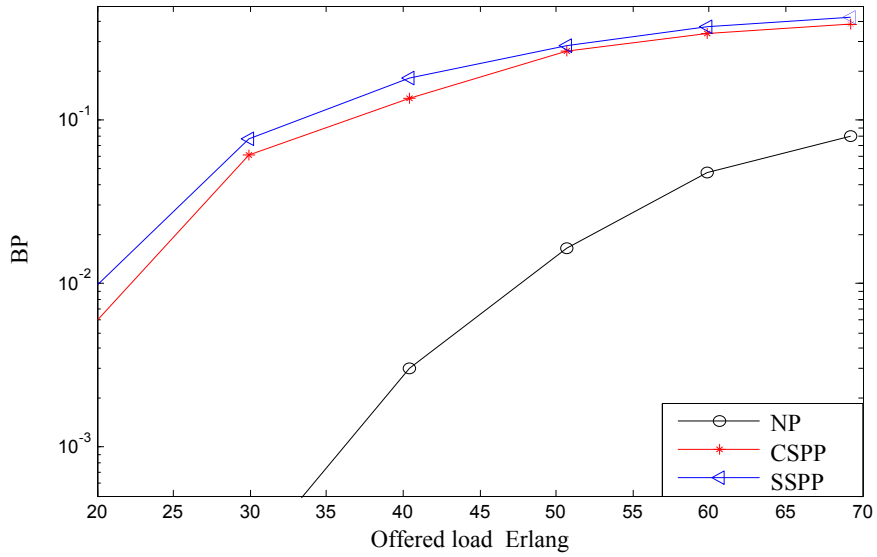


Figure 3.6 The effect of SLA negotiation on blocking probability over different protection schemes

3.6 SUMMARY

This chapter has presented a dynamic SLA negotiation mechanism for shared mesh optical networks. The proposed TE extensions applied to OSPF and BGP protocols consider both intra and inter domain communications. Link attributes as an SLA parameter have been negotiated via intra-domain mechanism and any new proposed SLA-based TE path attributes can be advertised through the inter-domain negotiation mechanism. The chapter has shown how an SLA parameter negotiation mechanism together with the proposed TE metric can improve the performance of different protection schemes or algorithms. Since the proposed mechanism in this chapter may cause heavy control overheads when disseminating link/path attributes, an alternative means of communication has been employed to reduce the overheads and resolve the possible scalability issues. The network performance has been evaluated from two different and important points of view: the control overhead reduction, and the network performance improvement. Performance analysis has shown that the proposed mechanism can be easily scalable using the path state advertisement concept, and also verifies that the scheme introduced in this chapter has a better network performance.

CHAPTER 4 STATICALLY PRE-PROVISIONED PRIORITY-AWARE MECHANISMS OVER SHARED MESH OPTICAL NETWORKS

4.1 INTRODUCTION

In WDM networks, every fiber link has multiple channels and each channel carries a high amount of traffic over each wavelength. Any failure on any link or wavelength causes an expensive loss for customers. Since failure in optical networks, specifically in the access layer is inevitable, protection and restoration schemes are a necessity for optical transport networks. To have an effective protection scheme, the customer and the service provider sides should be able to communicate with each other.

As previously mentioned in Chapter 3, it is not always possible for a network to accommodate a new request under an SLA. Here a traffic type driven algorithm is proposed as the first step to improve the accommodation performance of the incoming requests. It is assumed that a dynamic SLA negotiation mechanism, explained in detail in Chapter 3, can be implemented and the proposed algorithms can benefit from this facility to improve network performance.

The chapter is organized as follows: Section 4.2 identifies the motivations and objectives behind this chapter's discussion. Section 4.3 presents a novel SLA-based TE path attribute to provide a better picture of current status of the network. Section 4.4 introduces a novel priority-aware algorithm to better serve high-priority requests. In Section 4.5, simulation environments and performance analyses of the proposed algorithm are presented. Section 4.6 concludes with a summary of the chapter.

4.2 MOTIVATIONS AND OBJECTIVES

As the first challenge that customers may face, some requests cannot be accommodated as they violate the initial availability value offered by the network. This condition can be identified as an impossible request that is inappropriate to be counted as a blocked one and, therefore, should be treated in a different way. The algorithm proposed in this chapter looks for a remedy around this shortcoming. A path constraint considering the initial status of the network is introduced which is defined based on path availabilities. This parameter can represent the initial capacity of the network (when no traffic is applied to the network) for accommodating upcoming connection requests. Assuming that the parameter can be disseminated through the entire network, customers may have a more complete picture of the network and can make better decisions for requesting connections. By employing the path constraint, requests issued by customers who are beyond the initial capacity of the network will be modified to comply with the network initial conditions, otherwise they are blocked.

In this chapter, a pre-provisioned priority-aware algorithm is presented to accommodate higher priority requests over optical mesh networks. The proposed algorithm pre-provisions the requests and processes and modifies them before it applies the routing and wavelength assignment to any of them. This enables the service provider to provide fairly high quality connections at the lowest cost, based on the customers' requests.

4.3 NEW SLA-BASED TE PATH ATTRIBUTE: INITIAL MAXIMUM PATH AVAILABILITY (IMPA)

Definition (initial state of a network/initial network capacity)

The initial state of a network is the status of the network when no traffic has been applied to it. At this moment, all the network resources including links, wavelengths, bandwidth per wavelength, and links' availability are free to serve customers' requests. The initial network capacity is the available resource in the initial state.

The IMPA is defined as the maximum possible path availability between a pair of nodes *s* and *d* when no traffic has been applied to the network and is calculated based on the initial topology of the network when the resources are all free. The IMPA is pointed out in the equations in this chapter as A_{sdmax}. The value of A_{sdmax} is computed using Equation 4.1. Primary and backup paths can be calculated through Algorithm 4.2 defined in Section 4.4.2. A_{PB} formula was presented in Chapter 2 in Equation 2.6.

$$A_{sdmax} = A_{PB(s,d)} \Big|_{\text{all resources in the network are free}} \quad 4.1$$

If the network topology has no capability to accommodate a connection even in its initial state, there is no point for the request to get rejected. However, the customer should be informed of this shortage and so that a decision can be made on whether or not to forward the request to another service provider. If there is only one provider, the customer can come up with a new request based on the provider's offer given in the SLA negotiation. This method simply reduces the number of blocked connections which could be impossible to serve for the provider.

4.4 STATICALLY PRE-PROVISIONED PRIORITY-AWARE (SPA) ALGORITHM STRUCTURE

The SPA algorithm contains two modules, the pre-provisioning center and the routing and wavelength assignment module. The block diagram in Figure 4.1 shows the interaction between the pre-provisioning center and the routing and wavelength assignment module of the SPA algorithm.

As shown in the algorithm flowchart, including pre-provisioning center and routing and wavelength assignment module in Figure 4.2, the original request is processed by the pre-provisioning center to check if its availability requirement is met based on the maximum available network capacity at the initial state of the network. If it is not, the request is modified and is sent to the next module for computing the reliable paths. The pre-

provisioning center and routing and wavelength assignment module are discussed in Sections 4.4.1 and 4.4.2, respectively.

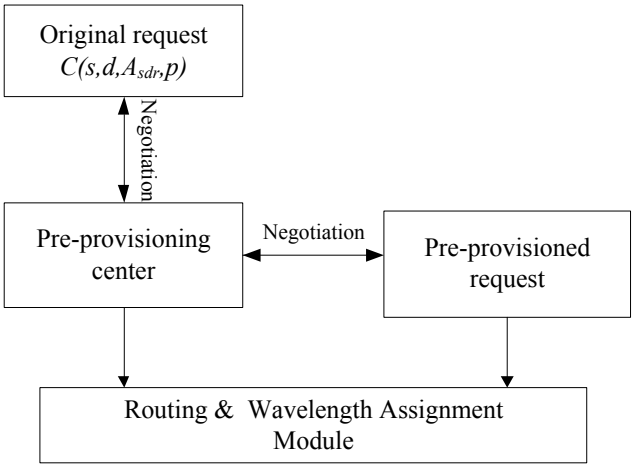


Figure 4.1 SPA algorithm block diagram

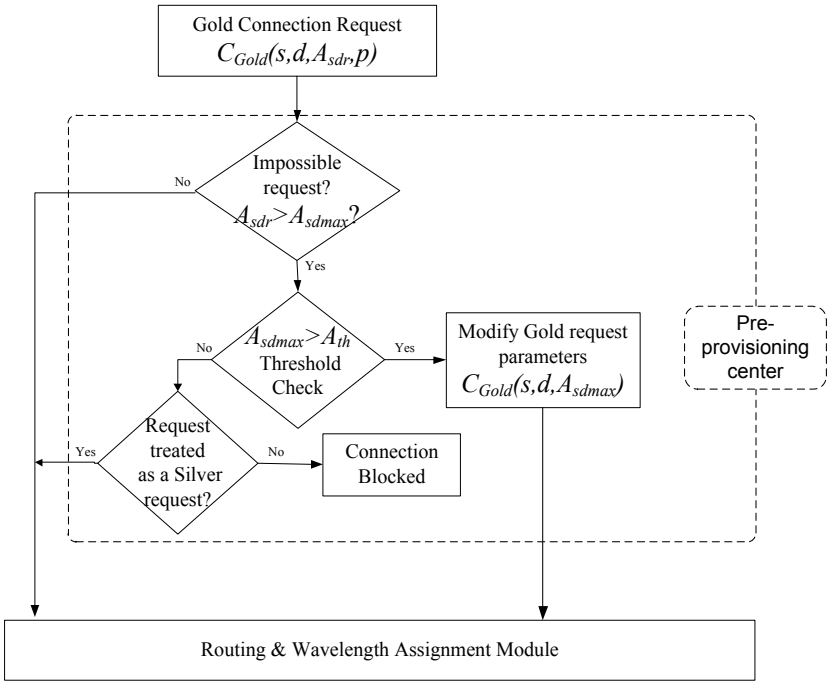


Figure 4.2 SPA algorithm flowcharts

Clearly, for a multi-homed network, as shown in Figure 4.3, the maximum offer sent by the service providers will be counted as the IMPA value for the customer since it is the initial maximum available network capacity at the initial state of the network.

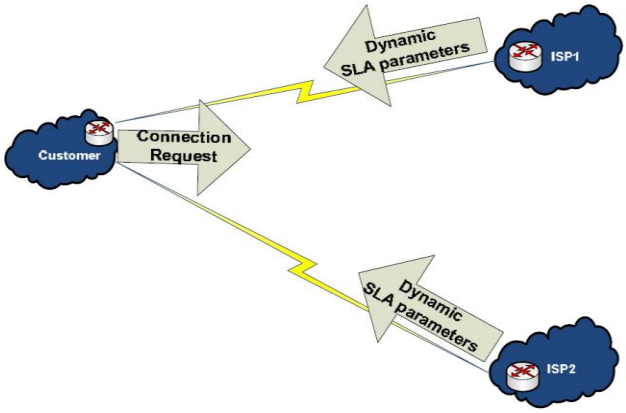


Figure 4.3 Multi-homed network topology

4.4.1 Pre-provisioning center

In the pre-provisioning center the connection requests are checked for whether they are beyond the maximum capability of the network. The way the SPA algorithm treats these kinds of connection requests is to modify the requests' parameters to comply with the available capacity of the network based on the link availabilities and the topology of the network. The availability requested by the customer for a specific pair of source and destination, A_{sdr}, is compared to the associated element of the matrix of path availabilities related to the same pair of source destination value. Each element of the $A_{(init)max}$ matrix, A_{sdmax}, can be calculated based on the initial topology of the network when no traffic is injected into the network and the resources are all free. $A_{(init)max}$ is in the following form in which clearly for all values of s=d : $A_{(s,d)max}$=0.

$$A_{(init)max} = \begin{bmatrix} 0 & \cdots & A_{(1,d)max} & \cdots & A_{(1,14)max} \\ \ddots & & \ddots & & \ddots \\ A_{(s,1)max} & \cdots & A_{(s,d)max} & \cdots & A_{(s,14)max} \\ \ddots & & \ddots & & \ddots \\ A_{(14,1)max} & \cdots & A_{(14,d)max} & \cdots & 0 \end{bmatrix}$$

If the availability requirement is met, the request is sent to the routing and wavelength assignment module. However, if the availability requirement is not met, the pre-provisioning center starts negotiating with the customer to offer the highest possible availability based on the statically calculated $A_{(init)max}$. Before the negotiation occurs, the pre-provisioning center checks if the maximum availability matrix element, A_{sdmax}, is higher than A_{th}, the threshold availability. The threshold availability is a parameter by which the pre-provisioning center decides to offer either a Gold or Silver connection to a potentially blocked Gold request.

Definition: Threshold availability

Threshold availability is a boundary value for the path availability. Customers use this value as a criterion to make a decision on choosing the path availability offered by service providers as a Gold or Silver path. That is, if the requested path availability is beyond the initial maximum path availability offered by the service provider, and if the offered value by service provider is beyond the threshold value, it can be treated as a Gold request, otherwise, the request have a chance to be treated as Silver. The value of threshold availability can be defined by the customer and keeps the customer's options open either to accept the service provider's offer or to reject it.

To explain how the mechanism works, an example is discussed here. For instance, suppose that the requested connection between source *s* and destination *d* is a Gold request with the requested availability of A_r=0.9999, and the pre-determined threshold availability of A_{th}=0.9997. In this case, if the IMPA of this pair of nodes, A_{sdmax} = 0.9998, is bigger than the threshold, the pre-provisioning center will offer this value as the new possible availability for the connection request and treats the new connection request as a Gold class request. If A_{sdmax} = 0.9996, and is smaller than A_{th}, the pre-provisioning center will offer this value as the new possible availability for the connection request but treats the new connection request as a Silver class request. However, the latter case relies on the acceptance of the offer by the customer. If the customer rejects the offer, the connection is blocked. The simulation results shown in Section 4.5.2 proves that the proposed mechanism improves the network performance by pre-provisioning high-priority requests

rather than only adjusting the requested SLA parameters to the values offered by the service provider.

The threshold of the availability for this case is considered 0.9997. The value considered for A_{th} is rational since [45] discusses the improved average availability of the different topologies under shared path protection, and those networks having less than 5 hours of down time per year give an average availability of 0.9997. Algorithm 4.1 presents the pseudo code for the SPA algorithm.

Algorithm 4.1 SPA algorithm

Input: Sequence of connection requests with threshold availability 0.9997 $\{C_n(s,d,A_{sdr}), A_{th}=0.9997\}$

Output: Negotiated Connection $\{C_n(s,d,A_{sdmodified})\}$

1. $n \leftarrow 1$
2. Serve n^{th} connection request $C_n(s,d,A_{sdr})$
3. IF $A_{sdr}<A_{sdmax}$ THEN
   Call algorithm 4.2 {Routing and wavelength assignment module}
   ELSEIF $A_{sdmax}>A_{th}$ THEN
   Modify the request $C_{Gold}(s,d,A_{sdmax})$ AND
   Call algorithm 4.2 {Routing and wavelength assignment module}
   ELSEIF $A_{sdmax}<A_{th}$ AND {the request is accepted to be treated as a Silver request} THEN
   Modify the request parameters $C_{Gold}(s,d,A_{sdrSilver})$ AND
   Call Algorithm 4.2 {Routing and wavelength assignment module}
   ELSEIF $A_{sdmax}<A_{th}$ AND {the request is not accepted to be treated as a Silver request} THEN
   Block the request connection AND
   $n \leftarrow n+1$ AND Go to Step 2
4. RETURN the Negotiated Request $\{C_n\}$
5. $n \leftarrow n+1$ AND Go to Step 2

4.4.2 Routing and wavelength assignment module of the SPA algorithm

After parameters of a connection request are negotiated and accepted by a customer, a request is sent to the routing and wavelength assignment module for further processing. As the block diagram of the routing and wavelength assignment module in Figure 4.4 shows, the output of the pre-provisioning center is either the original request whose requirements are met, or the pre-provisioned request with a new availability parameter, or a blocked request connection. The order of the processes in Figure 4.4 is numbered for the easier follow-up.

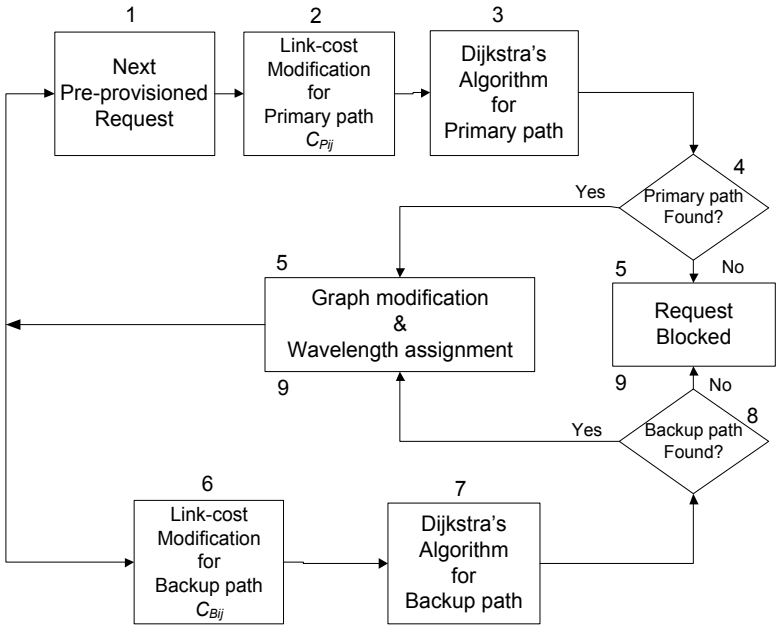


Figure 4.4 Block diagram of the routing and wavelength assignment module of the SPA algorithm

The routing scheme which has been used to determine the primary and backup path is adaptive routing [39]. The adaptive routing strategy has been discussed in Chapter 2. Before a path computation algorithm, e.g. the Dijkstra algorithm [47], is applied to the pre-provisioned request to find the primary path, the cost of the links of the graph is modified by the cost function presented in Equation 4.2. Based on the cost function, if

there is no wavelength available on the link, the link is removed from the graph; otherwise the cost of the link is a function of the link availability. As discussed in [34], by applying multiplication-to-summation conversion technique using logarithmic calculation of the path availability [34], the cost function is now additive and the path with maximum availability will be the path with minimum cost. Using this technique, a standard shortest-path algorithm can easily be applied for path computation.

$$C_{Pij} = \begin{cases} \infty, & \omega_{ij} = 0 \\ -ln(A_{ij}), & \omega_{ij} > 0 \end{cases} \quad 4.2$$

where C_{Pij} is the cost of the link *(i,j)* for the primary path *P* and is a function of the link availability, ω_{ij} is the number of free wavelengths in the link (*i,j*), and A_{ij} is the availability of the link.

The wavelength assignment of the primary paths follows the First-Fit (FF) algorithm [39]. The FF technique has been discussed in Chapter 2.

After calculating the primary path and having totally link-disjoint primary-backup path pairs, the graph is modified by removing the links forming the primary path. Following this step the wavelengths are assigned to the path based on the per-link basis. If the path computation finds no way from *i* to *j*, the request is blocked.
Before calculating the backup path, the cost of the links of the graph are changed one more time based on Equation 4.3.

$$C_{Bij} = \begin{cases} \infty & \omega_{ij} = 0 \\ -ln(A_{ij}) * \omega_{ij} & \omega_{ij} > 0,\ \omega_{rsvd} > \omega_B \\ -ln(A_{ij}) * \omega_{ij} + 1 & \omega_{ij} > 0,\ \omega_{rsvd} \leq \omega_B \end{cases} \quad 4.3$$

where C_{Bij} is the cost of the link *(i,j)* for calculating backup path *B*, A_{ij} is the availability of the link *(i,j)*, ω_{rsvd} is the number of the reserved wavelengths on the link for all shared backup paths, ω_B is the number of required wavelengths in case one of the links forming the primary path fails, ω_{ij} is the number of free wavelengths on the link.

As indicated by Equation 4.3, the algorithm looks for the paths with the highest available resources and lowest number of shared paths on each link to set up a backup path. The wavelength assignment of the backup paths follows the resource allocation scheme discussed in [24]. As the first step, the algorithm checks if the backup path can share any wavelength considering link-disjointness constraint. In the second step, it follows the FF technique to allocate a wavelength to the links forming the path. As the last step, it checks whether the availability of the connection is met based on the request's class of service. The joint availability formulas are presented in Equations 2.7 and 2.8, and are used to calculate the availability of Gold and Silver requests respectively. The Algorithm 4.2 presents the pseudo code regarding the routing module of the SPA algorithm. As shown in the Algorithm 4.2, the routing module is responsible for routing, wavelength assignment, and graph update.

Algorithm 4.2 Routing and wavelength assignment module

Input: Negotiated Request $\{C_n(s,d,A_{sdmodified})\}$

Output: Optimal P-B pair of paths

8. Modify the link cost of the graph using Equation 4.2
9. Apply Dijkstra's Algorithm to find the primary path P
10. IF P exists THEN
    Assign the wavelengths to P using the FF technique AND
    Update the graph and wavelength matrices AND
    Modify the link cost of the graph using Equation 4.3 AND
    Apply Dijkstra's Algorithm to find the backup path B
    IF B exists THEN
        Assign the wavelengths to B using the FF technique AND
        Update the graph and wavelength matrices
    ELSE
        Block the request AND Go back to Step 5 in Algorithm 4.1
  ELSE
    Block the request AND Go back to Step 5 in Algorithm 4.1
8. RETURN Optimal P-B pair

4.5 PERFORMANCE ANALYSIS OF THE SPA ALGORITHM

To have a fair performance analysis, the ASR, the blocking rate (BR), and the number of pre-provisioned blocked connections (PPBC) of the SPA algorithm are to be studied and compared with the standard and existing methods.

The ASR in this study represents the percentage of provisioned connections whose availability requirements are met over all provisioned connections. The BR denotes the percentage of blocked connection requests over all arriving requests. The PPBC shows the ratio of the number of those connections which are potentially blocked by other schemes while they are pre-provisioned by the proposed mechanism over the total number of potentially blocked connections. Some results of the performance evaluation of this study have been published in [48].

4.5.1 Simulation environment

The SPA algorithm has been evaluated based on the simulation environment discussed in Chapter 3, Section 3.5.3.1. Slight changes are applied to the injected traffic as follows: Connection availability requests are uniformly distributed between two classes of traffic: Gold class with the availability of 0.9999 and Silver class with the availability of 0.999. The threshold availability value is considered: $A_{th} = 0.9997$ (see Section 4.4.1).

4.5.2 Simulation results

The simulation was performed to compare the performance of the SSPP scheme [11], [12] and the priority-aware algorithm (PAA) presented in [22] with the SPA, and the results show considerable improvements on the connections with higher class of traffic. To simulate a real-world scenario, in this part of the thesis, dynamic traffic pattern has been studied (see Chapter 2).

As shown in Figure 4.5, the proposed SPA algorithm makes a significant improvement on the high-priority requests whose requirements are met. That is, the Gold connection requests are accommodated more in the SPA algorithm than in any other priority-aware

algorithms. As Figure 4.5 shows, for a specific offered load value of 40 Erlang, the SPA algorithm improves ASR performance of Gold connections by 36% on average compared to Gold connections of the two other schemes. Although the SPA algorithm has no significant effect on the lower priority traffic flows, Silver connection requests, in terms of ASR comparing with PAA algorithm [22], it still has better performance than the conventional scheme. The ASR graphs in Figure 4.5 have an error ranging $\mp 2 \times 10^{-3}$-3×10^{-3}. For the arrival rate of β=40, the 95% confidence interval of ASR for the SPA algorithm is [59.7% 60.3%] which translates to a 0.5% relative error.

As shown in Figure 4.6, the algorithm does not improve the blocking rate performance significantly and has almost the same BR as the PAA algorithm [22]. This fact together with the results shown in Figure 4.5 proves that the proposed mechanism improves the network performance by pre-provisioning high-priority requests rather than only adjusting the requested SLA parameters to the values offered by the service provider. In other word, the SPA algorithm increases the level of the priority awareness compared to other algorithms by provisioning more Gold requests than Silver requests. The graphs in Figure 4.6 have an error ranging from $\mp 6 \times 10^{-4}$ to $\mp 2.5 \times 10^{-3}$. For the arrival rate of β=40, the 95% confidence interval of BR for the SPA algorithm is [0.098 0.102] which translates to a 1.2% relative error.

As observed from Figure 4.7, on average 60% of high-priority connections, Gold class, which were impossible to be accommodated by the PAA algorithm [22] are pre-provisioned and are not blocked. The graphs in Figure 4.7 have a maximum error of $\mp 0.3\%$.

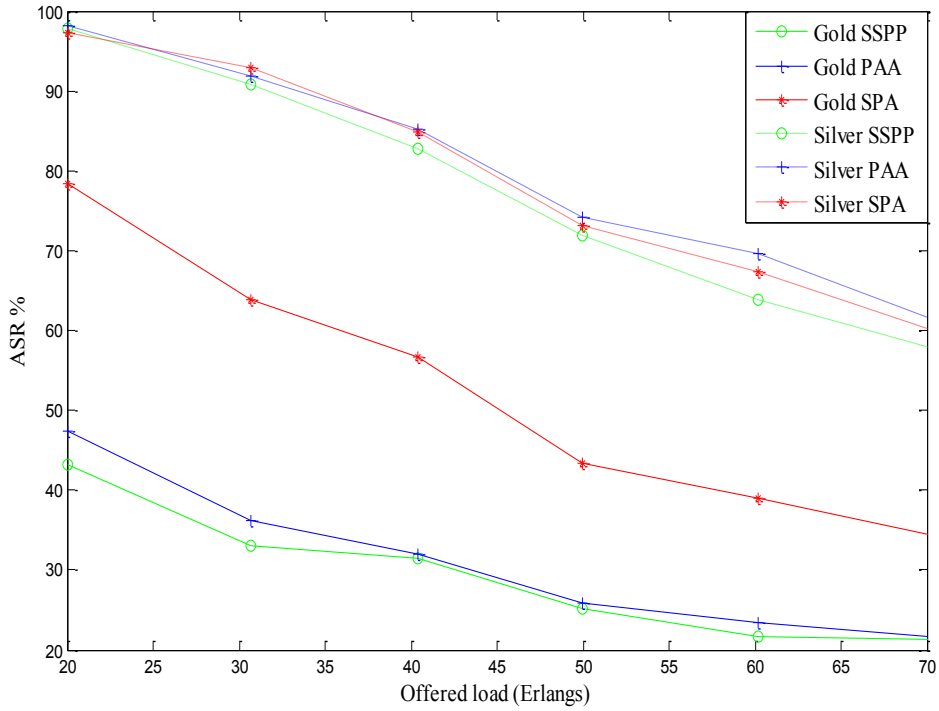


Figure 4.5 Availability satisfaction ratio performance analysis of SSPP, PAA, and SPA algorithms for different classes of traffic

Table 4.1 shows that the SPA algorithm does not apply more overhead to the service provider network in terms of the total number of allocated wavelengths than the SSPP and PAA algorithms. The total number of assigned wavelengths is calculated for the first 5000 requests.

Table 4.1 Comparison of total number of assigned wavelengths of SSPP, PAA, and SPA algorithms

Algorithms	SSPP	PAA	SPA
Wavelengths	17917	18419	17863

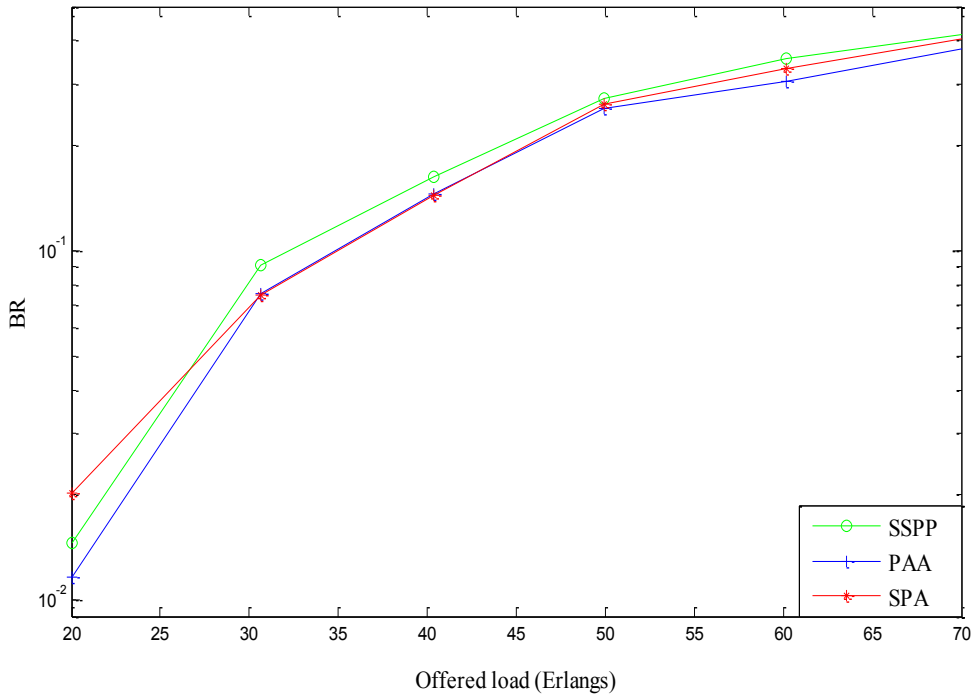


Figure 4.6 Blocking rate comparisons of SSPP, PAA, and SPA algorithms

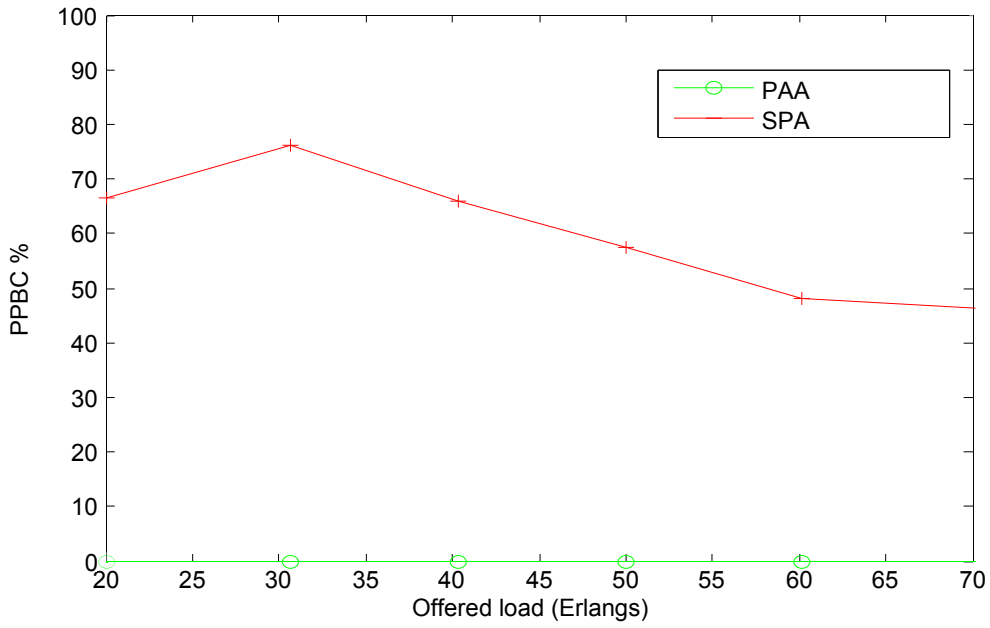


Figure 4.7 Number of pre-provisioned connections comparisons of PAA and SPA algorithms

4.6 SUMMARY

This chapter has been the first step of the mutual and bidirectional negotiation communications process between customers and service providers based on the SLA parameters. This work has employed a dynamic mechanism by which customers and service providers can negotiate some vital SLA parameters before they actually place the order and establish the requests. The work has looked for approaches by which services can be negotiated dynamically rather than being just requested unilaterally by the customer. Clearly, the lowest cost and load for service providers have been considered in designing such mechanisms.

The algorithm proposed in this chapter has looked for a remedy around the shortcomings of the existing mechanisms. The path constraint considering the initial status of the network in terms of the path availabilities has been introduced. This parameter has represented the maximum initial capacity of the network for accommodating upcoming connection requests. Assuming that the parameter can be disseminated through the entire network as the routing protocol parameters are, customers will have a better picture of the network status and can make better decisions for requesting the connections. By employing the path constraint, the requests issued by customers which are beyond the initial capacity of the network may be either modified to comply with the network initial conditions or blocked. As the simulation results show, the algorithm proposed in this chapter better accommodates the high-priority connections than the lower priority connection requests.

CHAPTER 5 DYNAMICALLY PROVISIONED PRIORITY-AWARE ALGORITHMS OVER SHARED MESH OPTICAL NETWORKS

5.1 INTRODUCTION

This chapter explores the need for taking the most advantage of a dynamic mechanism to propagate and refine the requirements requested by customers through SLA contracts. The study develops the algorithms and path constraints that are capable of working in such dynamic environments and carrying the important characteristics of the paths. The chapter discusses how the proposed algorithms benefit from dynamic negotiating mechanisms (see Chapter 3) to affect network performance and to develop new priority-aware algorithms which focus on SLA parameters including link and path availabilities as well as newly proposed path constraints. This chapter introduces two priority-aware algorithms, one for static and the other for dynamic traffic for different levels of priority. In addition to the proposed algorithms, a novel path constraint is introduced. The new path constraint helps the proposed algorithms to improve the performance of high-priority requests by reducing blocking probability, increasing availability satisfaction rate, and with better utilizing network resources.

In a multi-homed network topology (see Figure 4.3) over a shared mesh optical network which is capable of negotiating SLA parameters (see Figure 3.1), the path availability information can be communicated using dynamic SLA negotiation mechanisms [44], [49], and [50]. The customer side of this type of network is exposed to SLA information from all the service providers to which it is connected. The customer has the choice to pick the service provider that is the most suitable for satisfying the requested connection. The novel path constraint paves the way for employing a dynamic negotiation environment between customers and service providers and provides a better dynamic picture of network status based on the SLA parameters.

In a shared mesh network topology, the introduced algorithms, together with the proposed path constraint, can help the customers to modify, refine, and further process connection requests to better comply with service providers' network capacity. The simulation results will show improvements on preserving the high-priority class of traffic for both static and dynamic traffic compared to other protection schemes in shared mesh optical networks. The two novel algorithms will improve the availability of high-priority connection requests over a shared mesh optical network being capable of negotiating SLA parameters (see Figure 3.1). The proposed algorithms are a complementary study to the SPA algorithm presented in Chapter 4. To analyze the proposed algorithms' performance, two different simulation environments, static and dynamic, will be developed and evaluated.

Although the study is employed over an environment with dynamic SLA parameter negotiation, the chapter focuses on the priority-aware algorithms rather than the dynamic SLA negotiation mechanism, and it is assumed that there is an automatic mechanism for SLA parameters negotiation between service providers and customers' facilities to improve network performance as discussed in Chapter 3.

As discussed in [1], the routing and wavelength assignment problem is an optimization problem which uses ILP formulation to optimize a function of wavelength over some pre-defined constraints. However, these problems are NP-hard, and heuristics are required to find a solution.

The chapter is organized as follows: Section 5.2 identifies the motivations and objectives behind this chapter's discussion. Section 5.3 introduces a novel SLA-based traffic engineering path constraint. The proposed algorithms, which work together with the newly proposed path metric, are introduced in Sections 5.4 and 5.6 for static and dynamic maximum path availability algorithms, respectively. Simulation environments and performance analyses of the proposed algorithms are presented in Sections 5.5 and 5.7 for static and dynamic traffic respectively. Section 5.8 summarizes the chapter.

5.2 MOTIVATIONS AND OBJECTIVES

A large number of connection requests are sometimes sent to service providers over a very short period of time. This type of traffic can be considered as static traffic since the traffic characteristics are known in advance [21]. Service providers are able to sort the received requests based on the requests' characteristics and to further process them statically. This is the motivation to develop a new algorithm for static traffic which takes advantage of the new path constraint introduced in this chapter which has a dynamic nature to further process static traffic.

However, in a real-world scenario only one request is processed at a time in the order in which the requests are received, and the algorithm has no knowledge of the next request (dynamic traffic). After each request is processed, the graph topology and link-wavelengths usage matrices should be updated and new conditions and network status should be applied to the upcoming request. Since in a real-world scenario the algorithm has no prior knowledge of upcoming requests, considering the static traffic is not a good and precise assumption for the traffic type. This is the motivation for having another new mechanism for dynamic traffic. In addition to considering the real-world scenario, the other motivation for developing a new algorithm based on dynamic traffic is the presence of the newly defined path constraint. Since the new metric can be disseminated through the entire network, developing a mechanism which is able to take advantage of this metric will potentially lead to better serve high-priority dynamic flows of traffic.

5.3 NEW SLA-BASED TE PATH CONSTRAINT: MAXIMUM PATH AVAILABILITY (MPA)

In a multi-homed network in which the customer can be served by several service providers, as shown in Figure 4.3, the MPA algorithm, presented here, dynamically calculates the highest path availability offered by an autonomous system for any given source and destination pairs of the LSRs at any time that a request is received. This parameter can be advertised in an autonomous system through an SLA negotiation

mechanism as the maximum path availability of any source and destination pair in the connection request matrix (CRM). The MPA TE metric helps decision making nodes to manage customers` requests, specifically high-priority requests, based on the network offered status. This will help to increase the chance of accommodating more high-priority connection requests compared to existing shared-mesh protection algorithms over WDM optical networks.

Definition: Connection request matrix (CRM)

CRM is a 2nxm matrix of connection requests which is created for simulation purposes in which n is the number of the connection requests, 2n is the total number of establish and release requests, and m is the number of connection related parameters. Out of m connection parameters, connection sequence number (C_i), source node (S_i), destination node (D_i), requested availability (A_{ri}), arrival time ($T_{Arrivali}$), holding time ($T_{Holdingi}$), class of traffic/priority level (P_i=Gold/Silver), and type of the request (establish/release) are counted as connection parameters. The matrix of connection requests is in the following form.

$$CRM_{2nxm} = \begin{bmatrix} C_1 & S_1 & D_1 & A_{r1} & T_{Arrival1} & T_{Holding1} & \frac{Gold}{Silver} & \frac{Establish}{Release} \\ \vdots & & & & & & & \vdots \\ C_n & S_n & D_n & A_{rn} & T_{Arrivaln} & T_{Holdingn} & \frac{Gold}{Silver} & \frac{Establish}{Release} \end{bmatrix}$$

The MPA algorithm dynamically updates the MPA matrix (see the following definition) in every iteration after a connection change, a connection request, or a connection release. The MPA algorithm is a generalized case of the IMPA calculation in the SPA algorithm presented in Section 4.4.1. In the SPA algorithm, it was assumed that the network had no traffic load when the IMPA was calculated and the IMPA was calculated once, and was not updated during the network operation. Assuming that the dynamically updated MPA metric is propagated through the network by a dynamic SLA negotiation mechanism (discussed before in Chapter 3), all nodes in the network will have a unique and updated

picture of the current status of the network resources in terms of the MPA matrix at any time and after any changes to the network.

Definition: MPA matrix

Algorithm 5.1 calculates an mxm matrix of the following form in which m is the number of nodes in the network. Clearly, for all values of m, $MPA_{(m,m)}=0$. $MPA_{(i,j)}$is the maximum path availability between the pair of nodes i and j. The way this value is calculated is discussed in detail in Algorithm 5.1.

$$MPA_{mxm} = \begin{bmatrix} MPA_{(1,1)} & \cdots & MPA_{(1,j)} & \cdots & MPA_{(1,m)} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ MPA_{(m,1)} & \cdots & MPA_{(m,j)} & \cdots & MPA_{(m,m)} \end{bmatrix}$$

The MPA algorithm is responsible for dynamically calculating the highest path availability offered by the service providers for any given source and destination pairs. The parameter advertised in the dynamic SLA mechanism is the availability of the links forming the graph. However, proper SLA negotiation needs the information about availability of all possible paths for any source and destination pair. This is accomplished by applying the MPA algorithm. The MPA algorithm uses primary and backup paths availability formulas presented in Chapter 2 through Equations 2.4 and 2.5 to calculate the path availability of the primary and backup paths. Unlike the path attribute presented in Chapter 4 by which the initial status of the network was advertised and consequently had a static nature, the MPA attribute introduced in this chapter has a dynamic nature and is updated after any changes to connections including the connection establishment or connection release.

Equation 5.1 results in the maximum offered path availability between any requested source and destination pair using path availabilities for primary and backup paths. If the value of $MPA_{(s,d)}$ is zero, this means the network has no capacity at that time for serving the request and the request is considered blocked.

$$MPA_{(s,d)} = A_{pC_n} + A_{bC_n} - A_{pC_n}.A_{bC_n} \qquad 5.1$$

where A_{pCn} and A_{bCn} are the path availabilities of the primary and backup paths respectively (see Equations 2.4 and 2.5), $MPA_{(s,d)}$ is the maximum offered path availability for a source-destination pair in the n^{th} connection request C_n, and the n^{th} connection request is in form $C_n(s,d,A_r,p)$.

Definition: Graph topology matrix

A graph topology matrix is an mxm matrix of zeros and ones for a network of m nodes in which a one represents a direct link between nodes i and j, and a zero means nodes i and j are not connected directly. The graph topology matrix, GT, can be shown in following form for the network topology of NSFNet in Figure 3.3.

$$GT = \begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \end{bmatrix}$$

Definition: Wavelength usage matrix

A wavelength usage matrix is an mxm matrix in which each element of the matrix, $\lambda_{(i,j)}$, is either a zero or a specific value showing the number of free wavelengths in the link between nodes i and j. The initial value of a wavelength usage matrix, W_{init}, can be shown as follows in which ω is the number of available wavelengths in each link when no load has applied to the network, and GT is the graph topology matrix defined above.

$$W_{init} = \omega \times GT$$

The wavelength usage matrix, W, can be shown in following form in which $\lambda_{i,j}$ is the updated number of free wavelengths for the network topology of NSFNet in Figure 3.3.

$$W = \begin{bmatrix} 0 & \lambda_{1,2} & \lambda_{1,3} & \lambda_{1,4} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \lambda_{2,1} & 0 & \lambda_{2,3} & 0 & 0 & 0 & 0 & \lambda_{2,8} & 0 & 0 & 0 & 0 & 0 & 0 \\ \lambda_{3,1} & \lambda_{3,2} & 0 & 0 & 0 & \lambda_{3,6} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \lambda_{4,1} & 0 & 0 & 0 & \lambda_{4,5} & 0 & 0 & 0 & \lambda_{4,9} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \lambda_{5,4} & 0 & \lambda_{5,6} & \lambda_{5,7} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \lambda_{6,3} & 0 & \lambda_{6,5} & 0 & 0 & 0 & 0 & 0 & \lambda_{6,11} & 0 & \lambda_{6,13} & 0 \\ 0 & 0 & 0 & 0 & \lambda_{7,5} & 0 & 0 & \lambda_{7,8} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \lambda_{8,2} & 0 & 0 & 0 & 0 & \lambda_{8,7} & 0 & 0 & \lambda_{8,10} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \lambda_{9,4} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \lambda_{9,12} & 0 & \lambda_{9,14} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \lambda_{10,8} & 0 & 0 & \lambda_{10,11} & \lambda_{10,12} & 0 & \lambda_{10,14} \\ 0 & 0 & 0 & 0 & 0 & \lambda_{11,6} & 0 & 0 & 0 & \lambda_{11,10} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \lambda_{12,9} & \lambda_{12,10} & 0 & 0 & \lambda_{12,13} & 0 \\ 0 & 0 & 0 & 0 & 0 & \lambda_{13,6} & 0 & 0 & 0 & 0 & 0 & \lambda_{13,12} & 0 & \lambda_{13,14} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \lambda_{14,9} & \lambda_{14,10} & 0 & 0 & \lambda_{14,13} & 0 \end{bmatrix}$$

Algorithm 5.1 shows the pseudo code of the MPA algorithm. This algorithm calculates an *m* x *m* matrix, the MPA matrix, for a network topology of *m* nodes. The MPA algorithm first modifies the cost of the links based on the links availabilities and then applies Dijkstra's algorithm [51] to find the primary path for a given source-destination pair. If the primary path is found, the MPA algorithm updates wavelength, graph, and link availability matrices, and looks for a backup path the same way it does for primary path. The algorithm returns the MPA value of a given source-destination pair by applying Equation 5.1 to the primary-backup pair.

Algorithm 5.1 MPA algorithm

Input: $C_n(s,d,A_r,p)$, GT matrix, W matrix, W_{int}

Output: the MPA matrix

1. s ← 1 AND d ← 1
2. IF $s=d$ THEN

   $MPA_{(s,d)} \leftarrow 0$
3. WHILE $s \leq m$ AND $d \leq m$

   DO Steps 4-15

   4. FOR all values of $i, j \in \{1,2,...,m\}$ AND $s,d \in \{1,2,3,...,m\}$

      Modify cost of the links of the graph using Equations 4.2 and 4.3
   5. Run *Dijkstra's* algorithm [51] to calculate the primary path for the given source, destination, and the pre-calculated cost function in Step 4

6. IF no primary path is found THEN

   $MPA_{(s,d)} \leftarrow 0$

   Else

   Go to Step 7

7. FOR all links forming primary path

   Update W matrix AND

   Save it as a new matrix {to be used by backup path calculation process}

8. IF any elements of new link-wavelength matrix is zero $\{\lambda_{ij} \leftarrow 0\}$ THEN

   Same elements on the link-availability matrix is zero $\{A_{ij} \leftarrow 0\}$

9. Save the modified link-availability matrix in a new matrix
10. REPEAT Steps 4, 5 with the new link-availability matrix to find the backup path
11. IF no backup path is found THEN

    $MPA_{(s,d)} \leftarrow 0$

    Else

    Go to Step 13

12. Calculate the path availabilities through Equation 2.6 for all links forming primary and backup paths
13. Compute $MPA_{(s,d)}$ for a specific pair of source-destination in the n^{th} connection request using Equation 5.1
14. $s \leftarrow s+1$ AND $d \leftarrow d+1$
15. END

16. RETURN the matrix MPA

5.3.1 Dynamic negotiation mechanism of the MPA attribute

The negotiation mechanisms and protocols for path attributes propagation have been discussed in Chapter 3 in detail. Here it is shown how the MPA attribute is propagated through the entire network. The new path-attribute sub-TLV in BGP-TE Update packets

is presented in Table 5.1. This attribute carries MPA value which is calculated in an ER from any node inside the corresponding AS (including the other ERs). Figure 5.1 shows how the mechanism disseminates the TE-related SLA-based packets, in this case MPA information.

The packet routed from one AS to another AS is routed through one of the edge routers. The routers inside an AS advertise the link availability of the associated links into the AS. Using this information, the MPA matrix is built in all routers inside an AS including edge routers. Then all the edge routers of an AS have the matrix of the form below:

$$MPA_{mxm} = \begin{bmatrix} 0 & \cdots & MPA_{(1,j)} & \cdots & MPA_{(1,m)} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ MPA_{(m,1)} & \cdots & MPA_{(m,j)} & \cdots & 0 \end{bmatrix}$$

If the j^{th} node is one of the edge routers as shown in Figure 5.1, the ER_j will advertise the MPA value of all routes ending at the edge router. This information is summarized in the j^{th} column of the MPA matrix. Unlike regular routers inside the AS that only advertise the link availabilities, ER_j will advertise all the information of the j^{th} column of the MPA matrix of the associated AS through the proposed sub-TLVs of Update message presented in Table 5.1. The total maximum path availability of a path traveling from an ER in the n^{th} AS, AS_n, to an ER in the p^{th} AS, AS_p, will be calculated through Equation 5.2 in which MPA is the maximum path availability matrix in an AS, and MPA_{AS_k} is the maximum path availability value of the k^{th} AS from an ingress edge router ER_i to an egress edge router ER_j as shown in Equation 5.3.

$$MPA_{total} = MPA_{AS_n}(s,t) * \prod_{k=n+1}^{p-1} MPA_{AS_k} * MPA_{AS_p}(q,d) \qquad 5.2$$

For all nodes in AS_k:

$$MPA_{AS_k} = Max\{\, MPAs\ calculated\ between\ all\ possible\ edge\ routers\} \qquad 5.3$$

where AS_k is the k^{th} autonomous system, s is a source node in AS_n, d is a destination node in AS_p, t is an edge router in AS_n, q is an edge router in AS_p, k represents the number of autonomous systems between AS_n and AS_p.

In the case of the NSFNet network topology, the j^{th} edge router will advertise an MPA sub-TLV of 14 MPA values including the j^{th} column of the MPA matrix plus MPA_{total}.

Table 5.1 New MPA sub-TLV

MPA Type	MPA Length
$MPA_{(1,j)}$	
$MPA_{(2,j)}$	
……	
$MPA_{(i,j)}$	
……	
$MPA_{(m,j)}$	
MPA_{total}	

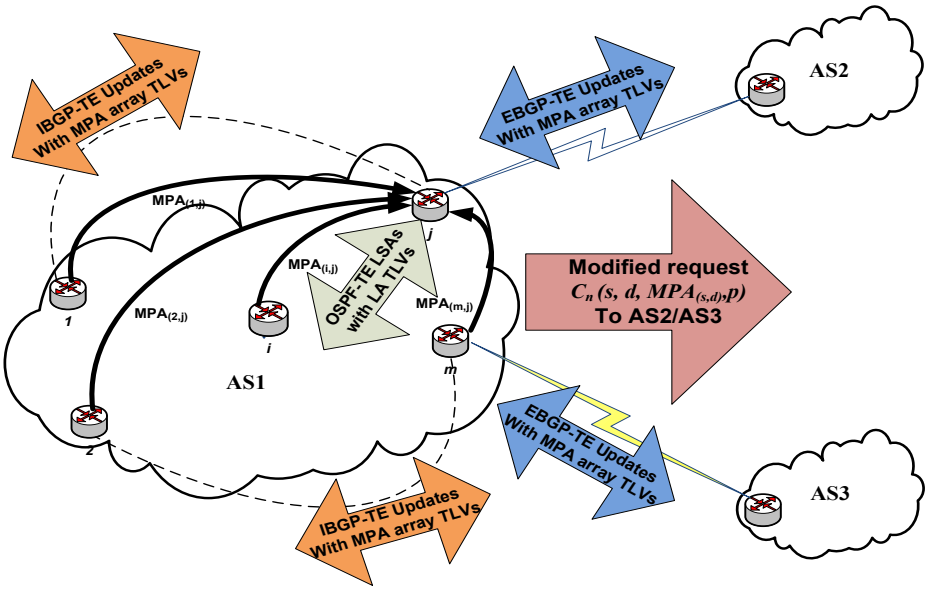


Figure 5.1 Inter-AS dynamic MPA attribute dissemination

5.4 STATIC MAXIMUM PATH AVAILABILITY ALGORITHM (SMPA)

In this section and as the second contribution of this chapter, an algorithm is presented which benefits from the proposed traffic engineering path constraint, MPA, defined in Section 5.3, to further process static traffic. Using the proposed algorithm, the service provider will be able to prioritize the request based on their level of importance and route them regarding the offered MPA. Since the goal of the mechanism is to serve the high-priority requests before any other traffic flows, the mechanism first sorts the traffic based on the priority levels. It then routes the higher priority requests whose requirements are met based on i) what is requested in the SLA and ii) what it is best offered by the service provider calculated through the MPA algorithm. The SMPA algorithm provides a mechanism as a priority-aware algorithm to dynamically provision high-priority requests of static traffic over shared mesh optical networks.

5.4.1 The SMPA structure

The SMPA algorithm is designed, and works best, for static traffic as mentioned above. In some related work and references, the static traffic is referred as offline traffic [21] as well since it is permanently fixed and does not have online characteristics [22]. For static traffic, it is assumed that the connection requests are known *a priori*. Each request is characterized by source, s, destination, d, requested availability for the n^{th} connection, A_{rn}, and requested traffic priority level, p. The n^{th} request can be shown as C_n *(s, d,* A_{rn}*, p).* The block diagram of the proposed SMPA algorithm is presented in Figure 5.2.

As shown in the block diagram of the SMPA algorithm in Figure 5.2, the algorithm consists of three main modules: connection prioritizing module, routing and wavelength assignment (RWA) module, and maximum path availability module. Algorithm 5.2 describes the proposed mechanism later in this section. The following subsections will explain all the SMPA algorithm modules in detail. Since the MPA algorithm has been

discussed in detail in Section 5.3 through Algorithm 5.1, it is not repeated again. The parameters and variables used in Algorithm 5.2 are explained in the following section.

After initialization of MPA, W, and GT matrices, Algorithm 5.2 calls the connection prioritizing module to sort the connections based on their priorities and prioritize those connections which meet the SLA requirements into separate sets of connections based on their priorities. After creating the prioritized sets, S_{PP}, the algorithm starts serving the first requests of the first priority level (highest priority level) set by calling the RWA module and MPA algorithm repeatedly. It continues this process until all the requests are served (established or blocked).

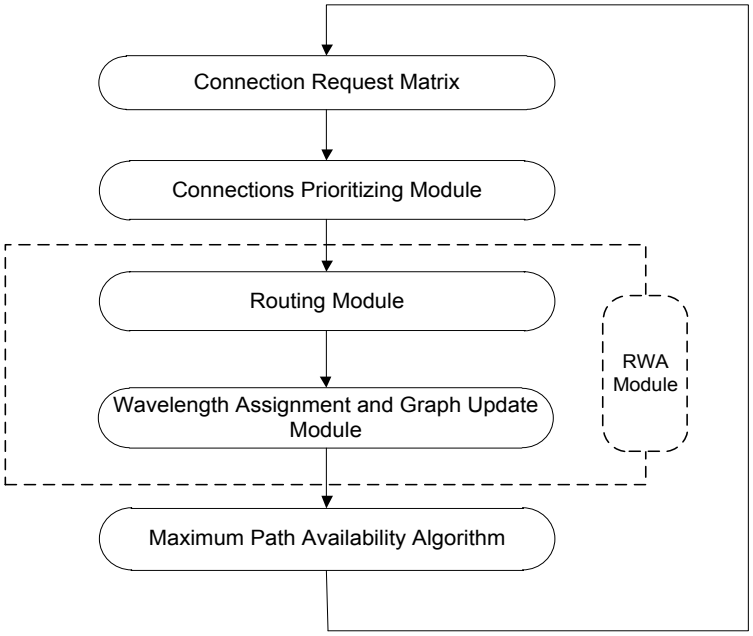


Figure 5.2 The SMPA algorithm block diagram

Algorithm 5.2 SMPA Algorithm

Input: Sorted connections in the CRM matrix based on their priorities

Output: Optimal pair of P-B paths

1. $p \leftarrow 1$ AND $n \leftarrow 1$
2. Initialize MPA matrix to zero AND initialize W matrix to W_{init} AND initialize GT matrix

3. Call Algorithm 5.3 {Connection prioritizing module}
4. WHILE $S_{PP} \neq Ø$ AND all priority levels smaller than 3 $\{p \leq 3\}$

    DO Steps 5-10

    5. Serve the n^{th} sorted request from the set S_{PP} $\{C_n (s, d, A_{rn}, p) \in S_{PP}\}$
    6. Call Algorithm 5.4 {Routing module}
    7. Call Algorithm 5.5 {Wavelength assignment module}
    8. Call Algorithm 5.1 {MPA algorithm}
    9. Remove C_n from S_{PP}
    10. $n \leftarrow n+1$

11. END
12. $p \leftarrow p+1$ AND $n \leftarrow 1$ AND Go to Step 4
13. RETURN Optimal pair of P-B paths

5.4.2 The connection prioritizing module

First, the requests are sorted based on their priorities to find the highest priority request which meets the path availability requirements. The requests are stored in the CRM matrix, and are sorted in descending order of the requests' priorities. The first request in the CRM whose availability is met is sent for further processing. Secondly, the RWA module is applied to the request to find the most optimal paths. The most optimal path is the path which costs the least for service provider while it meets the customer requirements. This module finds the primary-backup pair of paths, assigns the wavelengths to the calculated paths, and eventually updates the link-wavelength status and the graph topology.

The steps by which the connections prioritizing module of the SMPA algorithm affects the connection request matrix are shown in Figure 5.3. Three levels of priorities, *p=1, 2, 3*, have been defined as Gold, Silver, and Bronze services respectively. The different levels of priorities are identified by assigning different requested availabilities for each class of traffic. The requests belonging to each level of priority are stored in a corresponding set; S_p. S_p is a set of candidate requested paths whose level of priority are

p. Based on the prioritizing module presented in Figure 5.3, the requests, C_{np}, with the highest priority are served first. C_{np} is at the top of the stack in S_p whose p is higher than other S_p sets.

As long as there are requests in the highest priority level set which can meet the path availability requirements, for instance S_{Gold}, the SMPA will not process the lower priority sets, S_{Silver}. Those requests which can be satisfied, i.e., the requested availability of the requests (A_{rCn}) is lower than the offered availability (A_{oCn}) are kept in another set associated with the same priority level, S_{pp}, and are sent to the service provider network to be served and established. The offered availability (A_{oCn}) has been used here interchangeable with MPA value offered by service providers. Those requests which do not meet the requirements requested in the SLA are left for possible future opportunity, and the next request in the same set will be processed. If the set regarding a certain level of priority is empty or the existing requests cannot be served, the next lower priority level set will be considered for further processing. The pseudo code for the connections prioritizing module is shown in Algorithm 5.3.

Algorithm 5.3 Connection prioritizing module of SMPA algorithm

Input: Sorted connections in the CRM matrix based on their priorities
Output: S_{PP}

1. n ← 1 AND m ← 1
2. FOR all values of priority levels {$p \in \{1, 2,3\}$}
   Initialize S_P: $S_P \leftarrow$ {all connections, C_n in the sorted CRM ⎪ P= priority level}
   AND $S_{PP} \leftarrow \emptyset$
3. $p \leftarrow 1$
4. WHILE $p \leq 3$ AND $S_P \neq \emptyset$
   DO Steps 5-10
   5. $n \leftarrow 1$
   6. WHILE $n \leq$ Size(S_P)
      DO Steps 7-9
      7. Serve the n^{th} sorted request $C_n \in S_P$
      8. IF $A_{rCn} \leq MPA_{Cn}$ THEN

Place the request in associated S_{PP} set $\{S_{PP}[m] \leftarrow C_n\}$

9. $m \leftarrow m+1$

10. END

11. END

12. RETURN S_{PP}

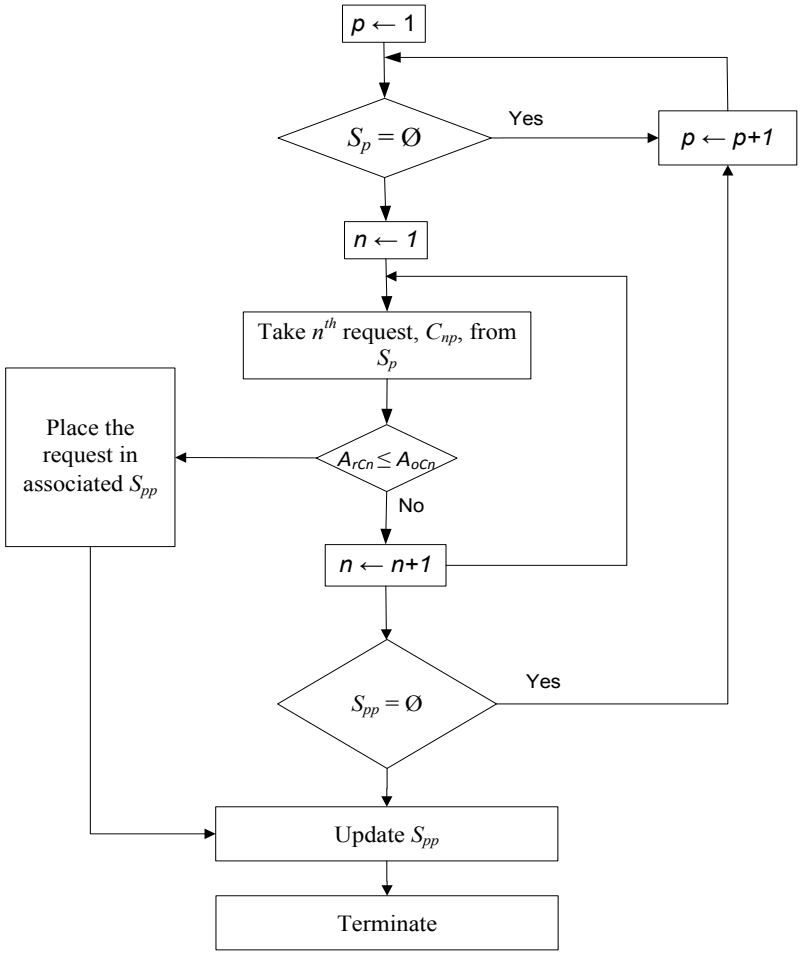


Figure 5.3 Connection prioritizing module of SMPA algorithm

5.4.3 The RWA module

The RWA module consists of routing module and wavelength assignment and graph matrices update module. The output of the prioritizing module saved in S_{pp} is a request which will be processed by the RWA module to be established as a connection. The connection requests in the S_{pp}, which are sent to the RWA module for further processing,

are permanently removed from the S_{pp} set. The routing module basically follows the dynamic constraint shared path protection algorithm discussed in [23] and the wavelength assignment module follows the approach presented in [21].

5.4.3.1 The routing module

The routing module presented in Chapter 4 is a simple routing algorithm by which a pair of primary-backup paths is assigned for each request. However, the routing module selected for the SMPA algorithm looks for the optimal paths based on specific minimal path costs. There are two main differences between the routing module applied in the SPA algorithm proposed in Chapter 4 and the routing module applied to the SMPA mechanism introduced here: i) To save the network resources as much as possible, the selected routing module does not assign any backup path to those primary paths which meet the SLA requirements. Only when the primary paths cannot fulfill such requirements, does the algorithm look for a backup path. ii) The path or the pair of paths which satisfy the new minimal path cost function presented in this chapter will be selected as the protected paths.

The routing scheme which is used in the routing module to determine the primary and backup paths follows the adaptive routing approach [39]. The Algorithm 5.4 shows the pseudo code for the routing module of the SMPA algorithm. The following assumptions have been made:

- The values of n and p have already been initialized
- The n^{th} connection request of the highest available priority p is being served
- The path availability of different level of priority, A_{Pm} and A_{Bm}, is calculated based on Equations 2.4 and 2.5
- Joint path availability of primary-backup pair, $A_{(Pm\ ,\ Bm)}$, is calculated using Equation 2.6
- The optimal path is obtained using Equations 5.4 and 5.5 (described later in this section)

Algorithm 5.4 Routing module of SMPA algorithm

Input: GT, W, CRM matrices, S_{ω}
Output: Optimal pair of P-B paths

1. $n \leftarrow 1$ AND $p \leftarrow 1$
2. FOR all connections in S_{PP} $\{\forall C_n \in S_{PP}\}$

   Serve n^{th} connection request $\{C_n\}$
3. WHILE the request type is Establish {CRM (n, 8) = Establish}

   DO Steps 4-23

   4. Initialize the sets: primary $\leftarrow$ Ø AND backup $\leftarrow$ Ø
   5. Modify link cost of the graph using Equation 4.2 {to calculate primary paths}
   6. Apply k-shortest path algorithm [52] AND primary $\leftarrow \{P_m \mid m \leq k\}$
   7. IF primary = Ø THEN

      Block the request AND Terminate the subroutine
   8. FOR all the paths in P_m $\{\forall P_m \in$ primary$\}$

      IF A_{Pm} < CRM (n, 4) THEN

      Remove P_m from primary set and place them in the backup set

      $\{\forall P_m \notin$ primary: backup $\leftarrow \{P_m \mid P_m \notin$ primary & $m \leq k\}\}$
   9. IF primary $\neq$ Ø THEN

      FOR all the paths in P_m $\{\forall P_m \in$ primary$\}$

      Choose the optimal path from primary set using Equation 5.4

      ELSE

      Block the request AND Terminate the subroutine
   10. Assign wavelength for primary path using the FF technique
   11. Update W & GT matrices
   12. IF the primary and backup sets are empty {primary = Ø AND backup = Ø} THEN

      Block the request
   13. WHILE the primary set is empty AND the backup set is not empty

      FOR all paths in the backup set {primary = Ø AND backup $\neq$ Ø AND $\forall P_m \in$ backup}

DO Steps 14-19

14. Remove the links forming P_m from graph to have link-disjoint backup path
15. Update W and GT matrices
16. Modify link cost of updated graph using Equation 4.3 for backup calculation
17. Apply Dijkstra algorithm [51]
18. Make up the backup set as:

    backup $\leftarrow$ $\{(P_m , B_m) \mid P_m \in$ backup AND $B_m =$ backup path calculated by Dijkstra algorithm$\}$
19. IF $A_{(Pm , Bm)} <$ CRM (n, 4) THEN

        Remove (P_m, B_m) pair from backup

20. END
21. IF the backup set is empty {backup $\neq \emptyset$} THEN

        FOR all pairs of paths in the backup set $\{\forall(P_m, B_m) \in$ backup$\}$

            Choose the optimal pair of paths from backup set using Equation 5.5

    ELSE

        Block the request

22. Call Algorithm 5.5 to assign wavelength for the backup path
23. Update W and GT matrices and S_ω set

24. END
25. WHILE the request type is Release {CRM (n, 8) = Release}

    DO Steps 26-27

    26. Release the resources taken by C_n
    27. Update W and GT matrices

28. END
29. RETURN optimal pair of P-B paths

The equations regarding minimal path cost calculation of the eligible paths, Equations 5.4 and 5.5, have been adopted from [23]. α is a constant which considers a balance between resource utilization and link availability. In these equations, α is considered to be $\alpha \leq 1$,

λ_{ij} is the number of assigned wavelengths on link (i,j), A_{pm} is the path availability of the primary path, $A_{(Pm,Bm)}$ is the joint availability of the primary-backup pair paths, C_P represents the minimal path cost for primary paths, and C_{PB} denotes the minimal path cost for a pair of primary-backup paths.

$$C_P = \left((1-\alpha) \times \sum_{(i,j)\in P_m} \lambda_{ij} \right) + \alpha A_{P_m} \quad 5.4$$

$$C_{PB} = \left((1-\alpha) \times \sum_{(i,j)\in P_m \cup B_m} \lambda_{ij} \right) + \alpha A_{(P_m,B_m)} \quad 5.5$$

5.4.3.2 The Wavelength assignment module

The wavelength assignment for the primary path is the same as for the unprotected and dedicated-protection strategies in the shared-protection strategy. The wavelength assignment of the primary/backup paths for no protection and dedicated protection schemes follows the First-Fit (FF) algorithm [39]. However, in the shared schemes, a single WDM channel can be shared with other paths. To exploit this property, the wavelength assignment scheme for priority-aware mechanisms proposed in [21] is employed here. The wavelength assignment algorithm applied here is different than the FF technique used in Chapter 4 based on the following facts: i) The algorithm check the sharability of resources on any given link, ii) The algorithm considers the link disjoint-ness constraint during the backup resource assignment, and iii) The algorithm checks whether sharing backup resources do not degrade the availability of other high-priority connections by re-computing the path availabilities using new path availability formulas presented in Equations 2.12 and 213. Algorithm 5.5 describes how wavelengths are assigned to connection *C*'s backup links. In this algorithm, the following notations are used:

- S_ω is a set of all connections protected by ω_j on link l_i [21].

- $S_{sh}(C_i)$ is a set of all connections sharing at least one backup wavelength on some link with a specific connection C_i called sharing group of C_i [21].

- S_{asgn} is a set of all connections protected by the assigned wavelength [21].

Algorithm 5.5 Wavelength assignment of backup links in priority-aware algorithms

Input: S_ω
Output: $S_{sh}(C_n)$

1. FOR all links in B_m and all wavelengths of the link l_i $\{\forall\ l_i \in B_m\ \&\ \forall\ \omega_j \in l_i\}$
   Check whether C_n can share ω_j with connections in S_ω considering link-disjointness constraint
2. FOR all links in B_m and all wavelengths of the link l_i and all connections in S_{asgn} $\{\forall\ l_i \in B_m\ \&\ \forall\ \omega_j \in l_i\ \&\ \forall\ C_i \in S_{asgn}\}$
   Check whether sharing backup resources do not degrade the availability of the other connection. Re-compute A_{Ci} based on Equations 2.12 and 2.13
3. IF conditions in Steps 1 & 2 are satisfied THEN
   Assign the lowest-numbered wavelength to connection C_n for link l_i AND
   Update $S_{sh}(C_n)$ and S_{asgn} sets AND Go to Step 5
   ELSE
   FOR all connections in S_{asgn} set $\{\forall\ C_i \in S_{asgn}\}$
   Place the connection C_n into $S_{sh}(C_i)$ set AND Go to Step 5
4. IF none of the existing backup wavelengths is qualified THEN
   Assign the next lowest numbered wavelength to C_n for link l_i AND
   Update S_{asgn} and $S_{sh}(C_n)$ sets
5. RETURN $S_{sh}(C_n)$

5.5 PERFORMANCE EVALUATION OVER STATIC TRAFFIC ANALYSIS

Static traffic (see Chapter 2) is used for performance evaluation of the SMPA algorithm. The characteristics of static traffic are known *a priori* and are considered as a matrix of

requests with known parameters including source, destination, requested availability, and requested level of priority. To simulate a priority-aware environment, the traffic is classified to three different priority traffic classes, Gold, Silver and Bronze.

The performance in terms of blocking probability of different classes of traffic, Gold, Silver, and Bronze for the static traffic case is referred as BP-G, BP-S, and BP-B respectively. In addition, the AWPC for fulfilling the connection requirement and the HPPR are evaluated by the SMPA in this chapter. Several protection schemes are studied over the static traffic analysis: the NP scheme, the SSPP scheme [11] and [12], the priority-aware PAA algorithm [21], and the SPA algorithm introduced in Chapter 4. All existing schemes are compared with two mechanisms proposed in this chapter: the SMPA and SMPA+SPA algorithms. The SMPA+SPA algorithm is a modified version of SMPA mechanism through which the SPA algorithm is called before the SMPA mechanism is applied. Some results of this part of the thesis are also available in [53] as one of the published contributions of this thesis.

5.5.1 Simulation environment

The SMPA algorithm has been evaluated based on the simulation environment discussed in Section 3.5.3.1. Slight changes are applied to the injected traffic as follows: The availability of connection requests is uniformly distributed between three classes of traffic: Gold class with the availability of 0.9999, Silver class with the availability of 0.9990, and Bronze class with no availability significance. For the SPA and SMPA+SPA algorithms, the threshold availability value is considered: A_{th} = 0.9997, based on practical values for different protection schemes and several network topologies presented in [45]. Since the RWA problem discussed here is a static RWA approach and the static approach assumes a stable traffic pattern over a long time [1], the total number of Gold, Silver, and Bronze requests among all possible connection requests is dictated by the network topology presented in Figure 3.3. This chapter uses the same network topology used in other existing algorithms in [48], [21], [22] , and [23] for the sake of consistency and fair comparison of the results.

5.5.2 Simulation results

Table 5.2 shows that the SMPA algorithm improves the blocking probability of Gold requests at least 40% compared to the SPA algorithm and more for other protection schemes. The SMPA algorithm also brings 11%-16% improvement compared with different protection schemes. Applying the SPA algorithm together with the SMPA brings 18% more improvement on preserving Gold requests, but it increases the blocking probability of Silver requests. However, the blocking probability of the SMPA+SPA algorithm for the Silver class of traffic is still comparable with other existing algorithms and is therefore acceptable. The blocking probability of Gold requests in the NP scheme is 100% since the requested availability is high and not met by assigning just a primary path. The joint availability of the primary-backup paths increases the path availability and consequently the chance of satisfying the requirements.

Table 5.2 Blocking probability percentage comparison for several protection schemes and algorithms

	NP	**SSPP**	**PAA**	**SPA**	**SMPA**	**SMPA+SPA**
BP-G	100	89	81	65.5	47	29
BP-S	97	66	61	64	50	66
BP-B	32	68	26	35	62	65

Furthermore, the 40% improvement in decreasing the BP for Gold class of traffic does not degrade the resource utilization performance. Figure 5.4 shows that although no improvement in bandwidth allocation is seen in either SMPA or SMPA+SPA algorithms, the average number of allocated wavelengths per connection is almost the same for different priority-aware algorithms. That is, SMPA and SMPA+SPA algorithms bring a fairly good tradeoff between resource consumption and blocking probability so that

improvement in one does not have a detrimental effect on the other. However, the NP scheme has the minimum amount of bandwidth consumption, which is, obviously, because of providing no protection paths as backup for primary paths. In addition, since the SSPP scheme does not take the link availabilities into account as a constraint in the path calculation, it has the maximum bandwidth consumption among all studied protection schemes.

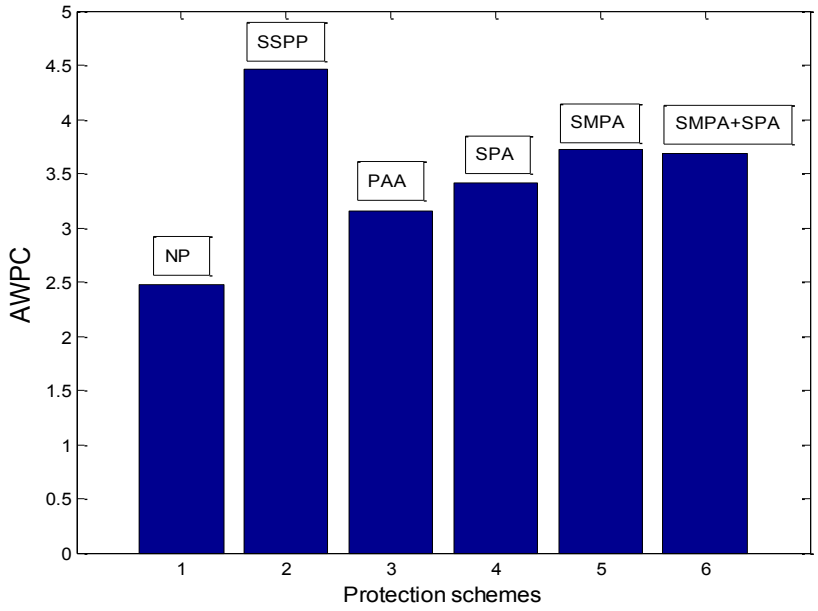


Figure 5.4 Average number of allocated wavelengths per connection with respect to different protection schemes

Figure 5.5 shows an increase in the percentage of high-priority provisioned requests including Gold and Silver which are served by either SMPA or SMPA+SPA algorithms compared to other schemes. It is indicated that 52% of high-priority requests which could be blocked in other protection schemes are now provisioned by the proposed mechanisms. The SMPA+SPA algorithm works just as well as the SMPA, but it works better for Gold requests. However, as Figure 5.5 shows, the SMPA+SPA algorithm has a 12-28% improvement in HPPR in comparison to the other existing algorithms. Since the SMPA algorithm works based on the traffic priority, the Bronze traffic clearly gets the minimum attention.

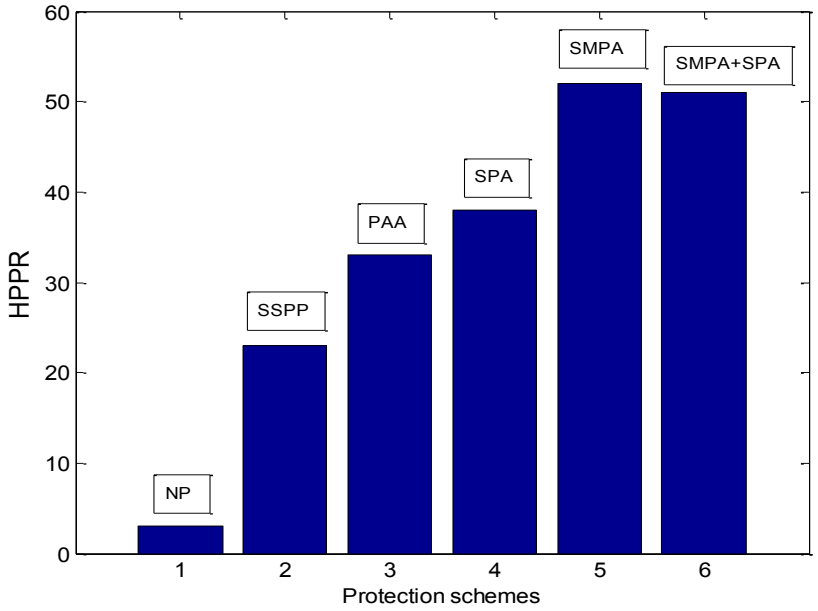


Figure 5.5 Percentage of high-priority requests provisioned by different protection schemes

5.6 DYNAMIC MAXIMUM PATH AVAILABILITY ALGORITHM (DMPA)

In dynamic traffic, only one request is processed at a time in the order the requests are received, and the algorithm has no knowledge of the next requests. After each request is processed, wavelengths are assigned, primary-backup paths are established, and the graph topology and wavelength usage matrices are updated. Each request may be established, blocked, or buffered for further processing. Therefore, to have a more realistic simulation environment and closer assumptions to the real world networks, service providers should also be able to route and provision high-priority requests based on a dynamic (online) [22] traffic pattern, in addition to the static type. The DMPA algorithm has been developed for this reason.

5.6.1 DMPA mechanism structure

The proposed DMPA mechanism consists of three main modules:

1) The MPA algorithm which is responsible for calculating $MPA_{(s,d)}$ for any pair of source and destination of n^{th} connection request requested in C_n *(s, d,* A_r*, p)* for a network topology of *m* nodes in a dynamic manner. This module is as same module in the SMPA mechanism. This algorithm has been discussed in Section 5.3 in detail.

2) The RWA module consists of a routing module and a wavelength assignment and graph matrix update module. The RWA module calculates the primary and backup paths for the requested connection, and assigns the wavelengths to the primary and backup paths. This module is as same module in the SMPA mechanism. The graph and wavelength matrices update module modifies the topology and wavelength usage matrices dynamically based on the current status of the network discussed in Section 5.4.3.2 in detail.

3) The provisioning module is responsible for provisioning the high-priority connection requests to bring the blocking probability of such requests as low as possible. The provisioning module of DMPA algorithm is discussed in detail in the following section. This is the new module which is different than the SMAP mechanism. In the SMPA mechanism the connection prioritizing module was responsible for serving static traffic. However, in DMPA mechanism a new module take care of dynamic traffic.

5.6.2 Provisioning module of DMPA algorithm

The n^{th} connection request can be considered in the form C_n *(s, d,* A_r*, p)* with the requested parameters source, *s*, destination, *d*, requested availability, A_r, and the requested priority level, *p*, respectively. Since each established connection changes the link-wavelength usage matrix and consequently may change the graph topology matrix, after processing any request, the cost matrix of the entire network is updated through Equation 4.2.

After the cost modification based on the link availabilities, the MPA algorithm calculates the best possible availability offered by the service providers for all possible paths through the network. As described in Section 5.3, the MPA algorithm uses Equations 2.4, 2.5, and 5.1 to calculate the path availability of the primary and backup paths and the maximum offered path availability between any requested pair of source and destination. If the value of $MPA_{(s,d)}$ is zero, this means the network has no capacity at that time for serving the request and the request is not sent to the service providers and is considered blocked. Typically, in the real world scenario, such calculations can take place in the customer premises to reduce the overhead of the control plane in transport optical networks like GMPLS environments. This can be counted as another advantage of the proposed algorithm.

As shown in Figure 5.6, if the requested availability is lower than the offered one, the requirements requested by the customer are met, and the original request will be sent to the service provider for further processing including routing, wavelength assignment, wavelength usage update, and graph topology modification modules. If the requested availability is higher than the offered one, the best availability offer from service providers will replace the requested one if it meets the threshold requirements. If so, the modified request is now sent to the service provider which is capable of serving the request while satisfying the requested SLA requirements.

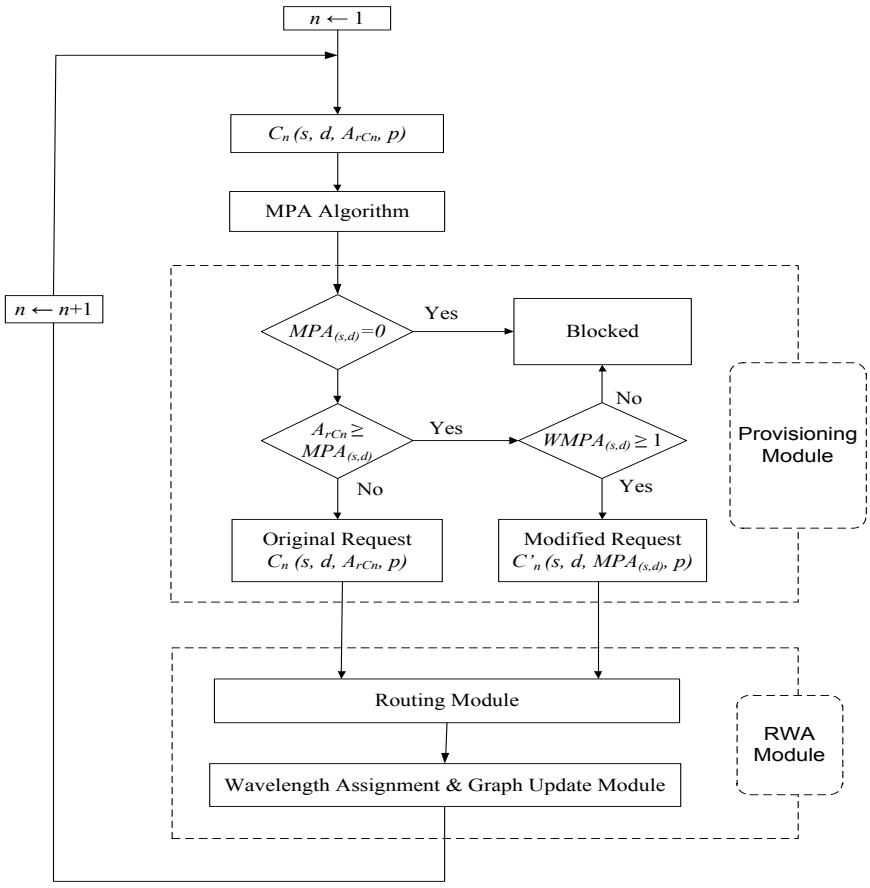


Figure 5.6 DMPA algorithm building blocks

The DMPA algorithm considers two availability threshold parameters at each level of priority for the customer, the lower bound availability threshold (A_{thpLB}) and the higher bound availability threshold (A_{thpHB}). Using these threshold parameters, a customer will be able to decide whether or not to accept the offered parameters for a certain level of priority. The threshold parameters depend entirely on the customer and are different for all levels of priorities. Some statistical research in [45] shows that the presented numerical values for the improved average availability of the different topologies can be used as threshold levels and are, therefore, used in Section 5.7 The results presented in [45] are a proper resource for choosing thresholds that are close enough to the real world parameters. However, the threshold values may vary based on the customer needs and the charging fees of the associated services.

The offered availability should be in the range of pre-defined threshold availabilities, as is shown in Equation 5.6. If Equation 5.6 is satisfied, the request is modified by new parameters and is sent to the routing module for further processing, otherwise it is blocked. Equation 5.6 can be written as Equation 5.7. Equation 5.8 introduces $WMPA_{(s,d)}$ as the weighted maximum path availability for a pair of source and destination, *s* and *d*. In Equation 5.9, WA_{thp}, weighted availability thresholds of LB and HB for a specific level of priority, *p*, are defined. Then Equation 5.7 can be summarized as Equation 5.10.

$$A_{thpLB} \leq MPA_{(s,d)} \leq A_{thpHB} \tag{5.6}$$

$$1 \leq \frac{MPA_{(s,d)}}{A_{thpLB}} \leq \frac{A_{thpHB}}{A_{thpLB}} \tag{5.7}$$

$$WMPA_{(s,d)} = \frac{MPA_{(s,d)}}{A_{thpLB}} \tag{5.8}$$

$$WA_{thp} = \frac{A_{thpHB}}{A_{thpLB}} \tag{5.9}$$

$$1 \leq WMPA_{(s,d)} \leq WA_{thp} \tag{5.10}$$

Since the connections are determined, and treated, based on their priority levels, *p*, A_{thpHB} can be considered 1 for all priority level traffic. With this assumption, for all values of *s* and *d,* the $MPA_{(s,d)}$ value is always less or equal to one which is a valid statement, and shows the assumption is a reasonable assumption. Then Equation 5.10 can be simplified as Equation 5.11. Equation 5.11 is the final constraint for the customer to either accept or refuse the service provider's offer. If the traffic belongs to the class of Gold services and the weighted offered availability requirement presented in Equation 5.11 is not met, the request is either refused or buffered for further processing. However, in this chapter, for the sake of simplicity, it is assumed that no request is buffered; they are either established or blocked. Algorithm 5.6 shows the pseudo code for the DMPA algorithm.

$$WMPA_{(s,d)} \geq 1 \tag{5.11}$$

Algorithm 5.6 DMPA algorithm

Input: CRM matrix

Output: Optimal P-B pair of paths

1. $n \leftarrow 1$
2. WHILE n is smaller than the number of rows in CRM matrix $\{n \leq \text{size}(CRM_{rows})\}$

   DO Steps 3-9

   3. Serve n^{th} connection request
   4. Call Algorithm 5.1 {MPA algorithm}
   5. IF $MPA_{(s,d)} = 0$ THEN

      Block the request C_n AND Go to Step 9

      ELSE

      Go to Step 6
   6. IF the requested availability is higher than the offered one $\{A_{rCn} \geq MPA_{(s,d)}\}$

      IF $WMPA_{(s,d)} \geq 1$ THEN

      $A_{rCn} \leftarrow MPA_{(s,d)}$

      ELSE

      Block the request C_n AND Go to Step 9
   7. Call Algorithm 5.4 {Routing module}
   8. Call Algorithm 5.5 {Wavelength assignment and graph update module}
   9. $n \leftarrow n+1$
10. END
11. RETURN Optimal P-B pair of paths

5.7 PERFORMANCE EVALUATION OVER DYNAMIC TRAFFIC ANALYSIS

As mentioned before, in contrast to static traffic, the lightpaths in the dynamic traffic pattern are requested dynamically with randomly generated availability requests so that the algorithm has no knowledge about the characteristics of the upcoming request.

In dynamic traffic analysis, the ASR, the BP, and the AWPC of the DMPA algorithm are compared to other existing algorithms. Based on the definition in [35], ASR represents the fraction of the connections whose availability requirements have been satisfied through different schemes over all provisioned connections. BP denotes the percentage of blocked connection requests over all arriving requests. AWPC shows the average number of wavelengths allocated for each connection. The performance of the proposed algorithm for dynamic traffic is compared with the schemes in which there are either no automatic SLA negotiations such as SSPP [11] and [12] or just static negotiation like SPA [48]. Some results of this part of the thesis are also available in [53] as one of the published contributions of this thesis.

5.7.1 Simulation environment

The DMPA algorithm has been evaluated based on the simulation environment discussed in Section 3.5.3.1. Slight changes are applied to the injected traffic as follows: Based on practical values for different protection schemes and several network topologies presented in [45], for simulation purposes, A_{thpLB} has been considered 0.9997 and 0.9988 for Gold and Silver traffic respectively. However, the values can marginally vary depending on the customer needs.

5.7.2 Simulation results

Since the dynamic RWA deals with dynamic changes of traffic pattern and the network state evolves all the time and consequently a tentative wavelength assignment may be blocked at a node, the main objective for assessing the performance of a dynamic RWA algorithms is the connection setup blocking probability [1]. The following graphs show superiority of the DMPA algorithm in terms of network performance compared to other existing schemes. There are three main reasons for the significant network performance improvement of the proposed mechanism compared to other existing schemes: i) employing a priority-aware wavelength assignment algorithm by which high-priority requests get more reliable shared resources than other requests, ii) applying a new routing mechanism by which an optimal path is selected based on the number of assigned

wavelengths to the path and the path availability, and iii) negotiating and revising requested SLA parameters to comply with the service provider capacity while satisfying the customer boundary thresholds.

Figure 5.7 compares the BP of the DMPA algorithm to the SSPP and SPA algorithms based on the offered load in Erlangs. Definitions for offered load and Erlang have been provided in A.1 and A.2. As Figure 5.7 shows, the BP of the DMPA algorithm is improved compared to two other algorithms, the SSPP and SPA schemes. Figure 5.7 shows a 47% decrease on average in connection blocking probability of the DMPA algorithm in comparison to the SSPP and SPA algorithms. Regarding the assumption for the link availability distribution, a high risk network (see Chapter 2) has been simulated for this part of the analysis to simulate the network as the access layer. Therefore, the BP is expected to be fairly high for all the studied schemes. The graphs in Figure 5.7 have an error ranging from $\mp 1.5\text{x}10^{-4}$ to $\mp 3\text{x}10^{-3}$. For the arrival rate of β=40, the 95% confidence interval of BP for the DMPA mechanism is [0.049 0.051] which translates to a 1.3% relative error.

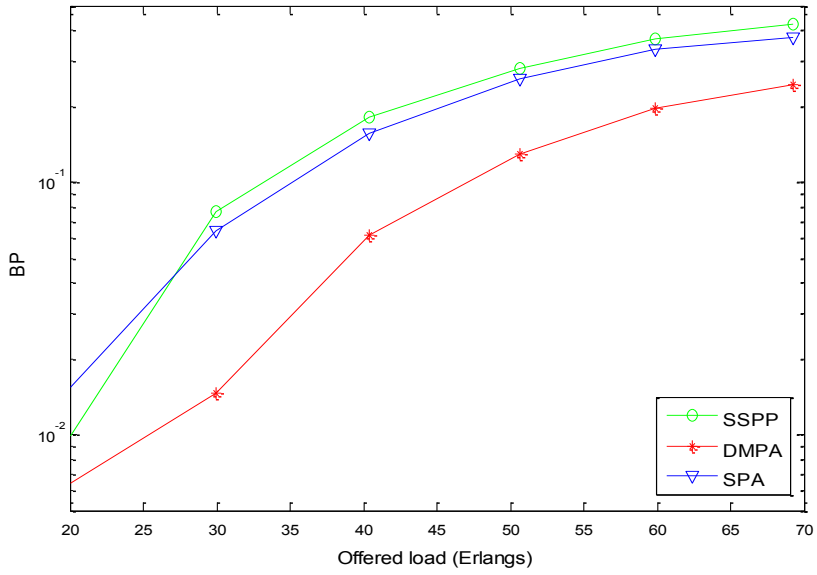


Figure 5.7 Blocking probability performance of the DMPA algorithm compared to the SSPP and SPA algorithms

Figure 5.8 compares the ASR of the DMPA with the SSPP and SPA algorithms based on the offered load in Erlangs. Simulation results in Figure 5.8 shows a 15% increase in ASR performance of the DMPA algorithm compared to the SSPP and SPA algorithms. The graphs in Figure 5.8 have a maximum error of $\mp$0.3%. For the arrival rate of β=40, the 95% confidence interval of ASR for DMPA mechanism is [94.8% 95.2%] which translates to a 0.15% relative error.

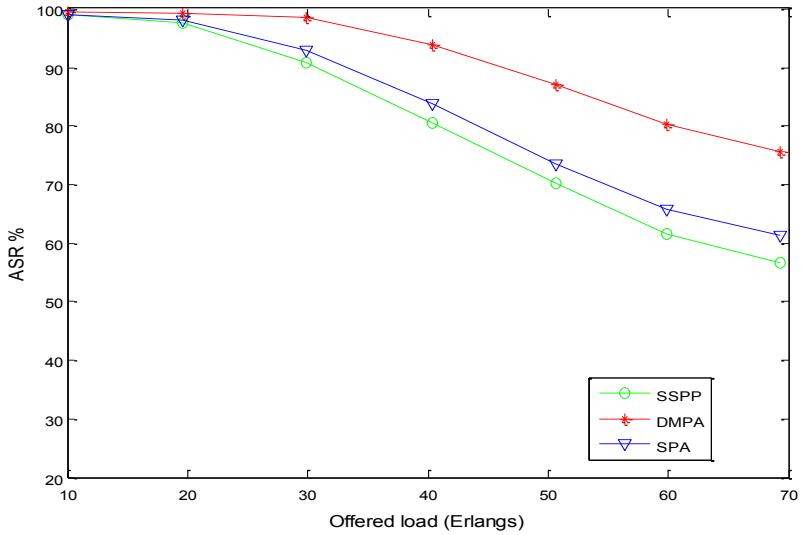


Figure 5.8 Availability satisfaction rate performance of the DMPA algorithm compared to the SSPP and SPA algorithms

Figure 5.7 and Figure 5.8 show that although the SPA algorithm presented in Chapter 4 improves the ASR compared to the SSPP scheme, it does not improve the BP. In contrast, the DMPA algorithm proposed in this chapter improves both the ASR and BP.

Figure 5.9 shows how much better the DMPA algorithm utilizes the network resources in terms of the number of assigned wavelengths per connection when compared to the SSPP and SPA algorithms. The AWPC for the DMPA is around 4.0 wavelengths while it is 4.6 for the SPA and 4.70 for the SSPP. Since the number of connection requests is large, the DMPA algorithm saves a significant amount of network resources. In addition, Figure 5.9 shows that the performance of SPA in terms of AWPC is degraded for small values of offered loads. However, the DMPA has a good performance for both small and large

offered loads. The graphs in Figure 5.9 have an error ranging from ∓0.12 to ∓0.2 wavelengths.

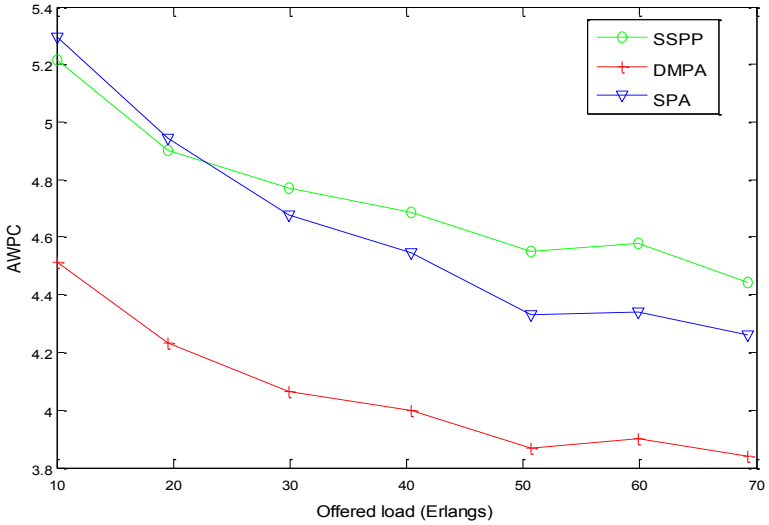


Figure 5.9 Average number of allocated wavelengths per connection of the DMPA algorithm compared to the SSPP and SPA algorithms

5.8 SUMMARY

The main contribution of this part of the study can be summarized in three parts. In the first part, a new traffic engineering path attribute, MPA, has been introduced. The MPA algorithm has been proposed to calculate and dynamically update the proposed path attribute. The second and third parts of the contribution are two algorithms which take advantage of the path constraint presented in the first part of the contribution to improve the network performance. Since an SLA negotiation mechanism needs proper information about availability of all possible paths for any pair of source and destination, the MPA algorithm has been developed to provide this type of information as the first part of the study. The MPA attribute is a generalized case of the IMPA metric presented in Chapter 4. As the second step, two priority-aware algorithms have been introduced over shared mesh survivable WDM networks. The SMPA and DMPA algorithms have been introduced to improve the network performance for static and dynamic traffic respectively. Employing the MPA path constraint, the proposed algorithms have improved the performance of high-priority connection requests.

CHAPTER 6 ADAPTIVE SLA-AWARE PROVISIONING MECHANISM FOR LONG DURATION SHARED MESH PROTECTED CONNECTIONS

6.1 INTRODUCTION

Survivable mesh optical WDM networks play a crucial role on serving recent tremendous growth in the Internet traffic demand. The increasing demand on QoS-based traffic which carries a high volume of high-priority traffic requires new traffic engineering strategies, provisioning algorithms, and protection schemes to be developed. The new strategies typically take the SLA-aware algorithms into account to maintain a satisfactory level of QoS for the requested connection with regard to the parameters requested in the SLA. Connection availability is one of the most important QoS parameters specified in an SLA between customers and service providers over survivable WDM mesh networks. In addition to connection availability, connection holding time is another connection request characteristic which can play an important role in developing priority-aware algorithms for preserving high-priority requests [25] [26] [27] [28] [29].

The contribution presented in this chapter follows three main characteristics: i) Proposing a new time-aware TE path constraint considering holding time of connections in addition to the availability, ii) Introducing a novel provisioning algorithm considering the proposed metric, and iii) Applying a high volume of high-priority dynamic traffic with long duration to the introduced mechanism as the new simulation environment.

As the first part of the contribution in this chapter, a TE path constraint based on the combination of the connection availability, the connection holding-time, and the maximum path availability (MPA) of the request is introduced. The proposed provisioning algorithm presented in this chapter, as the second part of the contribution, benefits from the new path metric to better serve high-priority connection requests. To achieve this goal, it is assumed that the period during which a connection is valid,

holding-time, is known *a priori*. As discussed in [54] and [55], based on SLA contracts or bandwidth-leasing markets between network operators and customers, it is reasonable to assume that the connection holding time can be known in advance when the algorithm is serving dynamic traffic.

The second part of this chapter introduces a novel provisioning mechanism by which some of those high-priority connection requests which were blocked in other SLA-aware algorithms or protection schemes are accommodated. The study focuses on a specific type of traffic which is of dynamic type and mainly high-priority class with long duration. The majority of existing algorithms either takes a small portion of the traffic as being high priority into account, or considers short connection holding times. The proposed provisioning mechanism is a dynamic provisioning algorithm including a time-aware buffering mechanism which works on the basis of the new path constraint presented in this chapter. The provisioning mechanism proposed in this chapter employs three algorithms: i) An algorithm to calculate the maximum path availability discussed in Chapter 5 in detail, ii) An algorithm to find the matrix of time-aware maximum path availability of each connection, and iii) An algorithm by which the potentially blocked connections are buffered and served based on the connections' holding times. The potentially blocked connections are those connections which are blocked by other existing mechanisms. The study compares the performance of the proposed algorithm to either standard or other existing SLA-based or priority-aware algorithms.

The chapter is organized as follows: Section 6.2 identifies the motivations and objectives behind this chapter's contributions. Section 6.3 introduces a new time-aware traffic engineering path constraint. Section 6.4 presents a provisioning algorithm to improve the network performance. Section 0 talks about the simulation environments and the performance analysis of the proposed algorithm. Section 6.6 summarizes the chapter.

6.2 MOTIVATIONS AND OBJECTIVES

The previous studies in Chapter 4 and Chapter 5 have focused on static/dynamic traffic. The holding time of a connection is an important SLA parameter (as availability is) and can have considerable effect on the process of serving the connections. Although the algorithms proposed in Chapters 4 and 5 have considered two important parameters affecting the path calculation process, the priority level and the availability of connections, they never considered the connection holding time as an effective factor in path calculation process. That is, they never discussed what would happen if a high portion of the traffic is Gold traffic and the high-priority traffic occupies the resources for a long time. This is the motivation to propose a new path attribute which is able to provide a time-aware picture of the network resources together with a mechanism which can take advantage of the proposed path attribute to serve high-priority requests. This is also the motivation to introduce a new flow of traffic considering high priority and long duration as two important SLA-based characteristics of the traffic. The need for a mechanism which can benefit from the SLA-based TE path constraint to better serve the high-priority traffic is the motivation for introducing an algorithm by which some of those high-priority connection requests with long durations, which were blocked in other SLA-aware algorithms or protection schemes, are accommodated.

6.3 NOVEL TE PATH ATTRIBUTE: TIME-AWARE MAXIMUM PATH AVAILABILITY (TMPA)

The algorithms discussed in Chapter 5, such as the SMPA, and DMPA, considered two important characteristics of connections and networks to best serve requests based on the requested SLA parameters: the level of priority of connection requests, and availability of resources offered by service providers. However, as mentioned above, the holding time of a connection can play an important role in serving high-priority classes of traffic. If a routing mechanism knows when the best time is to serve requests, it may be able to minimize the number of blocked connections and maximize the amount of resource utilization. In some cases, in which the duration of a connection (holding time) is fairly

long, the resources will be occupied for a long time. Therefore, serving the other connections may rely on preemption of the established connections. Consequently, knowing the release time of such requests will help service providers to schedule the available resources for upcoming requests. The release time is the period of time before which a connection is established, served, and eventually disconnected, and is calculated as the summation of the holding time and arrival time of a connection. Combining time characteristics of connections with other connections' and networks' characteristics gives path calculation centers a much better picture of resource availability in a timed manner. Employing such a mechanism will enable service providers to know when certain resources will become available, and when certain requests can proceed for further processing. This is the motivation to add another characteristic of a connection request, holding time, in the optimal path calculation process [25]-[29].

To have a time-aware picture of the network resources from a service provider point of view, the information regarding the time characteristic of the connections needs to be propagated throughout the network. However, service providers will still need to disseminate the information about the maximum resource availability that they can offer (such as MPA discussed in Chapter 5) to give customers an opportunity to choose the best provider in a multi-homed network. To facilitate this possibility, a novel time-aware TE path constraint is presented in this chapter which can be disseminated all over the network. The proposed path attribute gives service providers (or customers) the chance to know the future time for further processing of those connections for which enough resources are not available at the current time.

In this chapter, an algorithm is proposed by which a novel TE path metric, TMPA, is calculated, and can be advertised in an autonomous system through an SLA negotiation mechanism (introduced in Chapter 3) for any pair of source and destination in a CRM matrix. The proposed TE path constraint helps customers to manage their requests, specifically high-priority requests, based on the network offered status in a timed manner.

Definition: Established connection request matrix (ECM)

The $ECM_{(s,d)}$ is a matrix in which the first column of the matrix contains a list of established connections ($C_{j(s,d)}$), between a specific pair of source (s_p) and destination (d_q), path including Gold and Silver requests, and the second column is the associated release time ($T_{j(s,d)}$) of each connection $C_{j(s,d)}$. r is the number of established connections per s-d pair at the time of the calculation of $T_{r(s,d)}$.

$$\forall j \in \{1,2,\dots,r\} \qquad ECM_{(s_p,d_q)} = \begin{bmatrix} C_{1(s_p,d_q)} & T_{1(s_p,d_q)} \\ C_{2(s_p,d_q)} & T_{2(s_p,d_q)} \\ \vdots & \vdots \\ \vdots & \vdots \\ \vdots & \vdots \\ C_{j(s_p,d_q)} & T_{j(s_p,d_q)} \end{bmatrix}$$

Definition: Shared risk established connection matrix (SECM)

The $SECM_{(s,d)}$ is a matrix in which the first column of the matrix contains the set of previously established connections affecting the links traveling between a pair of source and destination path, and the second column is the associated release time of each connection. k is the number of established connections affecting a path of the s-d pair. To determine what connections affect a path of a specific s-d pair, the SRLG of each link forming the s-d path are considered. L_i is the i^{th} link forming the path C_i and G is the group number to which the SRLG belongs. The following algorithm defines the SECM matrix.

Building SECM matrix

FOR all links forming $C_i \in$ ECM

DO

There is at least an SRLG group, G, to which L_i belongs so that

IF G > 1 THEN

Find those connections whose links may share the same group number with C_i

Concatenate the connection found in the above step together with their associated release time into ECM matrix {to build SECM matrix}

$$\exists [C_k \;\; T_k] \; in \; ECM \;\; AND \; C_k \in G: \;\; SECM = ECM \,\big|\, [C_k \;\; T_k] \;\; \{concatination\}$$

$$\forall k \in \{1,2,\dots,t\} \qquad SECM_{(s_p,d_q)} = \begin{bmatrix} C_{1(s_p,d_q)} & T_{1(s_p,d_q)} \\ C_{2(s_p,d_q)} & T_{2(s_p,d_q)} \\ \vdots & \vdots \\ \vdots & \vdots \\ \vdots & \vdots \\ C_{k(s_p,d_q)} & T_{k(s_p,d_q)} \end{bmatrix}$$

END

RETURN matrix $SECM_{(s,d)}$

An SRLG is defined as the set of links sharing a common risk (such as a common physical resource such as a fiber link or a fiber cable). The SRLG properties has been summarized in [10] and [56].

Definition: TMPA matrix

The TMPA matrix is a matrix ($TMPA_{mxm}$) in which m is the number of nodes in the network. The way by which each element of this matrix is calculated is shown below. Each element of the $TMPA_{mxm}$ matrix, the $TMPA_{(s,d)}$, is a kx2 matrix by itself in which k is the number of established connections affecting the links traveling between a pair of source and destination. The $TMPA_{(s,d)}$ matrix contains MPA of all established pairs of connections affecting s-d pair together with their associated offered times. In other words, T_j shows the time at which the MPA value of $MPA^{C_j}_{(s,d)}$ can be offered to the connection $C_{j(s,d)}$. The matrix of $TMPA_{(s,d)}$ can be written as below in which p and q are node numbers among m nodes in the network.

$In \; the \; matrix \; SECM$:

$\forall \; C_{j(s,d)} \in \{SECM_{(j,1)}\} \;\; AND \; \forall \; j \epsilon \{1,2,\dots,k\} : \;\; \exists \; p \;\&\; q \in \{1,2,\dots,m\}$:

$$TMPA_{(s_p,d_q)} = \begin{bmatrix} MPA^{C_0}_{(s_p,d_q)} & T_0 \\ MPA^{C_1}_{(s_p,d_q)} & T_1 \\ \vdots & \vdots \\ \vdots & \vdots \\ MPA^{C_j}_{(s_p,d_q)} & T_j \end{bmatrix}$$

The top TMPA matrix element, $\mathrm{MPA}^{C_0}_{(s_p,d_q)}$, is the MPA value offered when the current connection $C_0(s, d, A_{r0}, p, t_{0arrival}, t_{0holding})$ is released at T_0. Therefore, a general TMPA matrix element $\mathrm{MPA}^{C_j}_{(s_p,d_q)}$ will show the potential MPA value offered for the given pair of source and destination while the links forming the primary and backup paths of associated connections, C_j, from the 1st to the j^{th} row of the SECM matrix are released. During the period of ($T_{k-1} - T_k$), the MPA that a service provider may offer with regard to the release of associated connections would be $\mathrm{MPA}^{C_{k-1}}$ as shown in Figure 6.1.

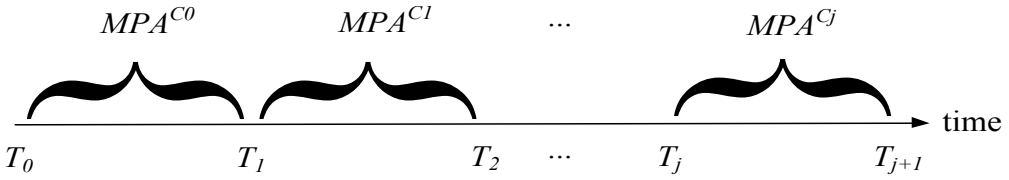


Figure 6.1 Potential MPA values after releasing associated connections

The TMPA matrix of all source and destination pairs for a network of *m* nodes is shown as below and is calculated in the TMPA module.

$$\forall\, p, q \in \{1,2,\dots,m\}: \qquad TMPA_{mxm} = \begin{cases} \left[TMPA_{(s_p,d_q)}\right] & p \neq q \\ 0 & p = q \end{cases}$$

To find the connections affecting the previously established connections between a specific pair of source and destination, the concept of SRLG of the links is used to help the algorithm to find the connections whose links may affect any pair of *s*-*d*. SRLG plays an important role in many path computation techniques including *k*-shortest path [57], [58], and [59]. Although SRLG propagation through signaling protocols such as RSVP-TE is not yet ratified [60], SRLG can be propagated along with routing information using OSPF-TE extensions in GMPLS networks [10]. Therefore, the information is already available to the algorithm and does not need to be propagated again.

6.4 ADAPTIVE PROVISIONING SLA-AWARE (APSA) MECHANISM

The mechanism proposed in this chapter takes advantage of the novel time-aware path constraint to establish, buffer, or block certain type of traffic. The buffered requests can be processed at a certain time when their SLA requirements are met and satisfy the maximum offered available resources. The contribution presented in this chapter proposes a provisioning algorithm which serves requests of certain level of priority in a time-aware manner. To avoid keeping a connection waiting for an extremely long time, some conditions and constraints for the buffering time will be applied, and will be discussed in the following sections of this chapter.

The proposed mechanism contains five main modules:

i) MPA module: responsible for offering the maximum available resources
ii) TMPA module: responsible for scheduling the maximum available resources at certain times
iii) Buffering module: responsible for buffering those requests for which enough resources are not available for a certain amount of time
iv) RWA module: responsible for finding optimal primary-backup pair of paths and assigning the wavelengths to those paths
v) Wavelength and graph update module: responsible for updating resource matrices

The following sections discuss the APSA algorithm and the associated modules. Figure 6.2 shows the modules involved in the APSA algorithm and how they interact. As discussed in previous chapters, connection requests are considered in the form of the CRM matrix and are served one by one. The request is applied to TMPA and MPA modules to be served either as an original request or as a buffered request for further processing. The TMPA algorithm uses the SECM matrix as an input and interacts with the MPA algorithm for the calculation of the proposed path attribute. Then the buffering high-priority connection (BHC) module is applied by which CRM is updated with a modified arrival time for the connection request.

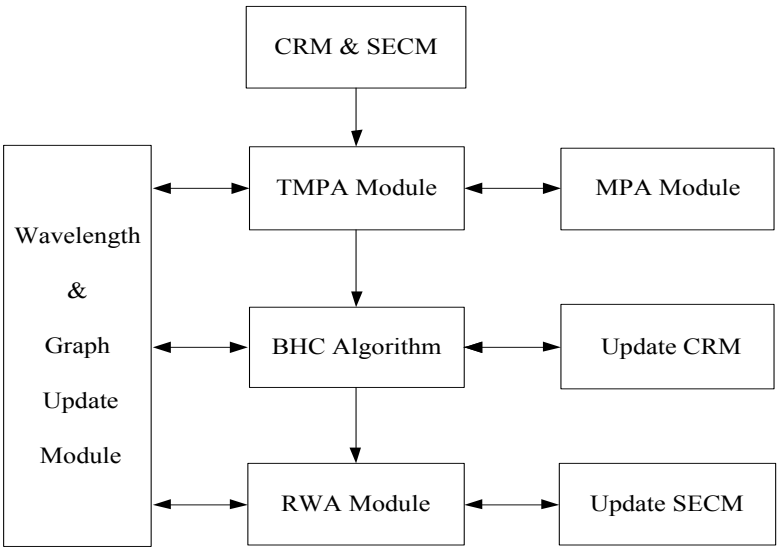


Figure 6.2 The APSA algorithm modules interaction

6.4.1 The APSA mechanism structure

The elaborated diagram on how the APSA algorithm works is shown in Figure 6.3. After each request is processed, the graph topology and wavelength usage matrices are updated. Each high-priority request is established, blocked, or buffered for further processing. The low-priority traffic is handled by routing and wavelength assignment module with no further processing. The n^{th} connection request is in form C_n *(s, d,* A_r*, p,* $T_{arrival}$*)* with the requested parameters: source, *s*, destination, *d*, availability, A_r, the priority level, *p*, and the arrival time, $T_{arrival}$, respectively.

Algorithm 6.1 shows the pseudo code for the APSA algorithm block diagram shown in Figure 6.3. When a new high-priority connection is requested, the APSA algorithm calculates the MPA matrix by running Algorithm 5.1 to find out whether the Gold request meets the best offer made by the service provider. If it does, the APSA algorithm applies the RWA module to the request. If the Gold connection requirements are not met, the APSA algorithm runs Algorithm 6.3 to modify the request and buffer the connection through the TMPA and BHC modules. When a Gold request has been buffered, the APSA algorithm employs the BHC module using Algorithm 6.4 to serve the high-priority

request. Since the APSA algorithm has been designed to better serve high-priority requests, it does not apply any further processing to low-priority requests other than the regular RWA module.

6.4.2 Modified APSA mechanism structure

The modified APSA algorithm uses the weighted maximum path availability concept presented in the DMPA algorithm in Chapter 5 rather than the MPA only. The request is first applied to the provisioning module of the DMPA algorithm. If the provisioning module of the DMPA algorithm can satisfy the ongoing connection SLA requirement, the request is served and not sent to other modules for further process. However, if the provisioning module of the DMPA algorithm facing a high-priority request has no choice other than blocking the request, the modified APSA algorithm sends the request to the TMPA and BHC modules for further processing. Algorithm 6.2 introduces the modified APSA algorithm. Figure 6.4 shows the block diagram of the modified APSA algorithm.

Algorithm 6.1 APSA algorithm

Input: CRM matrix
Output: Optimal P-B pair of paths, Updated CRM

1. $n \leftarrow 1$
2. WHILE n is smaller than the number of the rows in CRM matrix AND the connection type is Establish {$n \leq$ size (CRM_{rows}) AND CRM (n,8) = Establish}

   DO Steps 3-7

   3. Serve the n^{th} connection request
   4. Call Algorithm 5.1 {to calculate $MPA_{(s,d)}$}
   5. IF $MPA_{(s,d)}=0$ THEN

      Block the connection AND Go to Step 7

      ELSEIF $A_{rCn} \leq MPA_{(s,d)}$

      Call Algorithm 5.4 {Routing module}

      Call Algorithm 5.5 {Wavelength assignment and graph update module}

      Remove C_n from CRM

      ELSEIF p=Gold AND $A_{rCn} > MPA_{(s,d)}$

      Call Algorithm 6.3 {to calculate $TMPA_{(s,d)}$}

      IF $TMPA_{(s,d)} = 0$

      Block the connection AND Go to Step 7

      ELSE

      Call Algorithm 6.4 {to serve and buffer the connection}

      ELSE

      Block the connection AND Go to Step 7
   6. RETURN Optimal P-B pair of paths
   7. $n \leftarrow n+1$
8. END

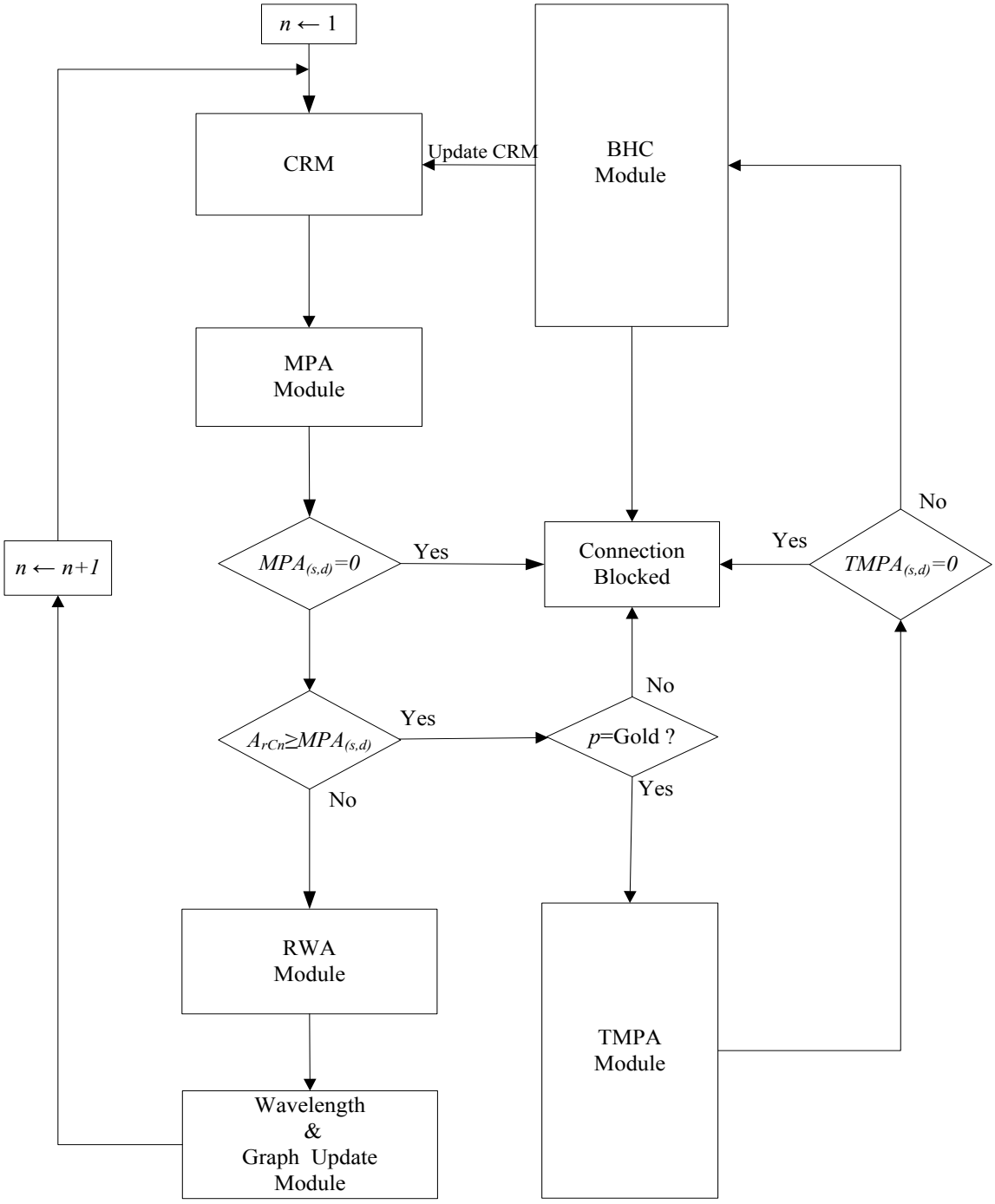


Figure 6.3 The APSA Algorithm building blocks

Algorithm 6.2 Modified APSA algorithm

Input: CRM matrix
Output: Optimal P-B pair of paths

1. $n \leftarrow 1$
2. WHILE n is smaller than the number of the rows in CRM matrix AND the connection type is Establish {$n \leq$ size (CRM_{rows}) AND CRM (n,8) = Establish}

   DO Steps 3-10

   3. Serve n^{th} connection request
   4. Call Algorithm 5.1 {to calculate MPA}
   5. IF $MPA_{(s,d)} = 0$ THEN

      Block the connection C_n AND Go to Step 10
   6. IF $A_{rCn} \geq MPA_{(s,d)}$ THEN

      IF $WMPA_{(s,d)} \geq 1$ THEN

      $A_{rCn} \leftarrow MPA_{(s,d)}$ AND Go to Step 7

      ELSEIF p=Gold AND $A_{rCn} > MPA_{(s,d)}$ THEN

      Call Algorithm 6.3 {to calculate $TMPA_{(s,d)}$} AND

      IF $TMPA_{(s,d)} = 0$

      Block the connection AND Go to Step 10

      ELSE

      Call Algorithm 6.4 {to serve and buffer the connection}

      ELSE

      Block the connection AND Go to Step 10
   7. Call Algorithm 5.4 {Routing module}
   8. Call Algorithm 5.5 {Wavelength assignment and graph update module}
   9. RETURN Optimal P-B pair of paths
   10. $n \leftarrow n+1$

11. END

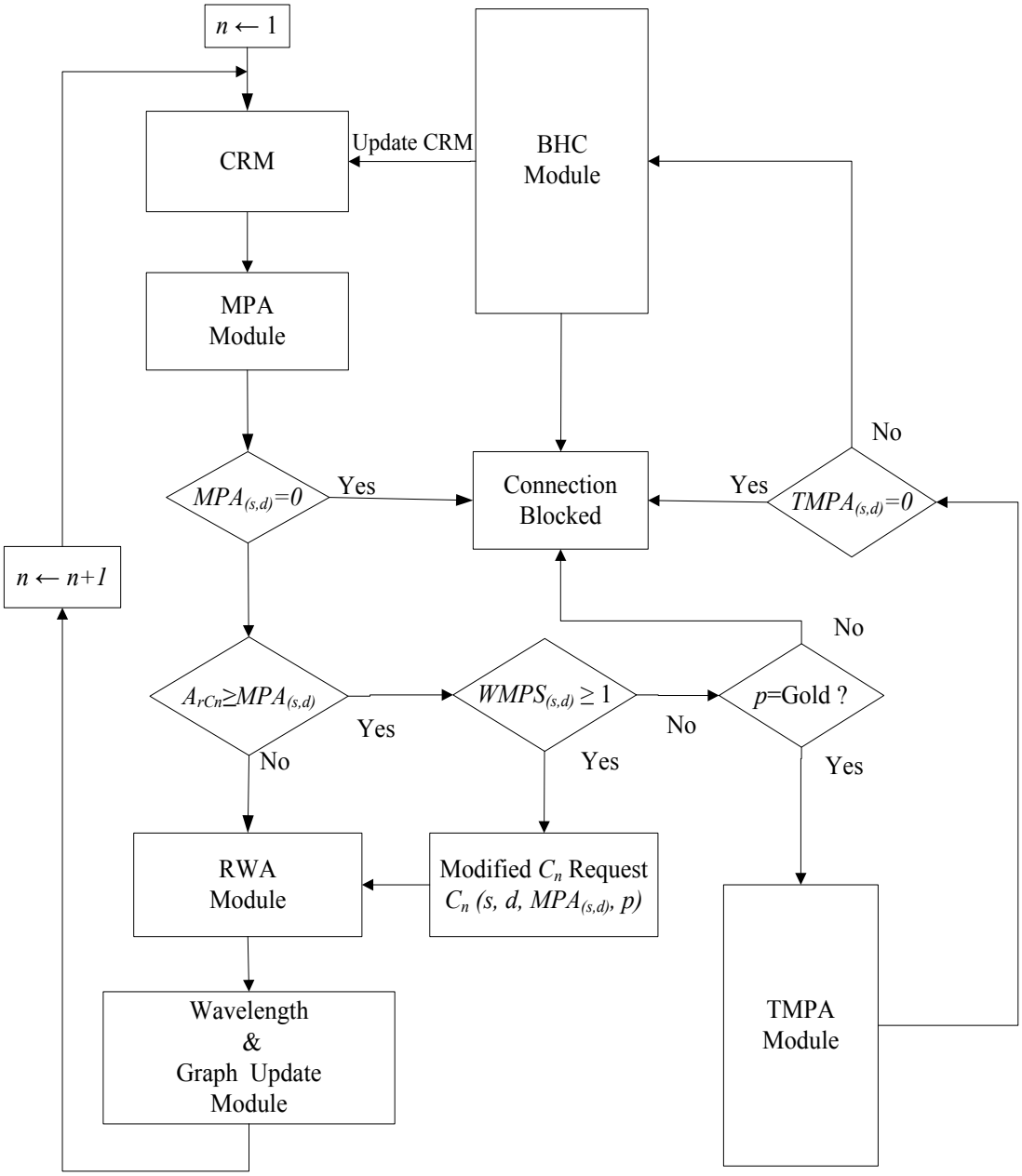


Figure 6.4 The modified APSA algorithm building blocks

6.4.3 The TMPA module

Algorithm 6.3 shows how the TMPA matrix is calculated in the TMPA module. The TMPA matrix contains the MPA values offered to all pairs of source and destination and their associated release times. Algorithm 6.3 calculates the $MPA_{m \times m}$ matrix for a network topology of m nodes. $MPA_{(s,d)}$ calculated in Algorithm 5.1 is the maximum offered path availability for a certain source-destination pair in the n^{th} connection request, and has been discussed in detail in Chapter 5. It is assumed that there is an automatic mechanism for SLA parameter negotiation between service providers and customers to propagate MPA information all over the network. The protocols used for dynamic SLA negotiation have been discussed in Chapter 3 in detail. If the $MPA_{(s,d)}$ is calculated after the release time of the connections associated with a specific pair of source and destination, the TMPA values can be propagated around the network. This is done in the same way that MPA information is disseminated over intra/inter-domain of a network involving multiple autonomous systems. TMPA information can be, and is, assumed to be propagated over the control plane of the network. To avoid buffering a request for an extremely long time, the TMPA algorithm is assumed to be applied to each connection request just once. If an already buffered request cannot be accommodated, it is not sent to the TMPA module for further processing and is simply blocked.

Algorithm 6.3 TMPA algorithm

Input: CRM, $C_0(s, d, A_{r0}, p, T_{0arrival}, T_{0holding})$, m as the number of nodes in the network

Output: $TMPA_{(s,d)}$ matrix

1. $k \leftarrow 1$, $u \leftarrow 1$, $v \leftarrow 1$
2. FOR all the values of $u \leq m$ AND $v \leq m$

   DO Steps 3-17 {to build the matrix $TMPA_{mxm}$}

   3. IF $u = v$ THEN

      $TMPA_{(s_u,d_v)} \leftarrow 0$ AND

      Go to step 17

   4. Build the ECM matrix of associated (s_u,d_v) pair (see the definition of the ECM_{rx2})

5. IF $r \leq 1$ THEN

   Block the request C_0 AND Go to step 17

6. FOR all connections in ECM matrix AND all links forming connection C_i

   DO

   There is at least an SRLG group, G, to which L_i belongs so that

   IF G > 1 THEN

   Find those connections whose links may share the same group number with C_i AND

   Concatenate the connection found in the above step together with their associated release time into ECM matrix {to build SECM matrix}

   $$\exists [C_k \;\; T_k] \; in \; ECM \;\; AND \; C_k \in G: \;\; SECM = ECM \,\big|\, [C_k \;\; T_k]$$

7. Sort the columns of SECM based on ascending order of the release times $\{T_j s\}$
8. FOR all values of k: $k \leq t$

   DO Steps 9-15 {to build $TMPA_{(s,d)}$ array}

   9. Save current wavelength, graph, and link availability matrices in new matrices
   10. Release connections $C_{1(s,d)}$ to $C_{k(s,d)}$ from the $SECM_{(s,d)}$ matrix {associated primary and backup paths of the 1^{st} to k^{th} connections (rows) of the $SECM_{(s,d)}$ matrix}
   11. Update new wavelength, graph, and link availability matrices
   12. Call Algorithm 5.1 {to calculate the MPA associated to k^{th} release: $MPA^{k}_{(s,d)}$}
   13. Calculate the k^{th} row of the TMPA matrix (see the definition of the TMPA matrix)
   14. RETURN the array $TMPA_{(s,d)}$
   15. $k \leftarrow k+1$

16. END

17. $u \leftarrow u+1$, $v \leftarrow v+1$
18. END
19. RETURN matrix $TMPA_{mxm}$

6.4.4 The BHC module

Algorithm 6.4 defines the steps involved in the BHC module. It is assumed that the n^{th} connection request arriving at t_n is a Gold request whose requirements have not been met and will potentially be blocked by the RWA module if no further processing is applied to it. The algorithm looks for the minimum amount of buffering time in the TMPA matrix at which the connection requirements are met. That is, the algorithm will investigate how long the request should be buffered to have a better chance of being established. The circumstances under which the buffered request is established are discussed in Algorithm 6.4.

If the requested availability of the Gold connection is higher than the $MPA_{(s,d)}$, the BHC module checks the TMPA matrix row by row to find which row has a smallest release time and can satisfy the connection requirements. When the BHC module finds the TMPA matrix's row which meets the connection requirements, if it satisfies the threshold time boundaries applied by the control plane of the network, it modifies the request's arrival time and inserts it in the CRM matrix as a connection request with a new arrival time and updates this matrix.

If it is assumed that the k^{th} row of the TMPA matrix is selected as the best offered MPA value for a specific pair of source and destination, T_k will be the earliest time after which the potentially blocked connection can be served. However, if the value of T_k is too long, it buffers the connection for extremely long time and may not let the request be served. As a result, some constraints should be considered for the T_k parameter, mainly lower and upper bounds. The release time of the first and the earliest connection should be considered as the lower bound. This makes the algorithm sure that the releasing process has started. The higher bound has been approximated using Equations 6.1 to 6.5.

As shown in Figure 6.5, N_{Tk} is the number of high-priority connections requested before T_k. To make sure that there are enough resources after T_k for the n^{th} connection, it is assumed that the number of newly established connections should be the same as the number of released ones. Although the equal number of established and released connections is not necessarily mapped into an equal number of utilized resources, the

result of the average number of wavelengths per connections in NSFNet network, presented in previous chapters, shows that the assumption is a good estimate.

The threshold buffering period of the queued connection is writen as T_{th}. As observed in Figure 6.5, if the number of high-priority requests before t_n is considered as N_{HP}, it can be assumed that on average every t_n/N_{HP} unit of time a Gold connection is requested.

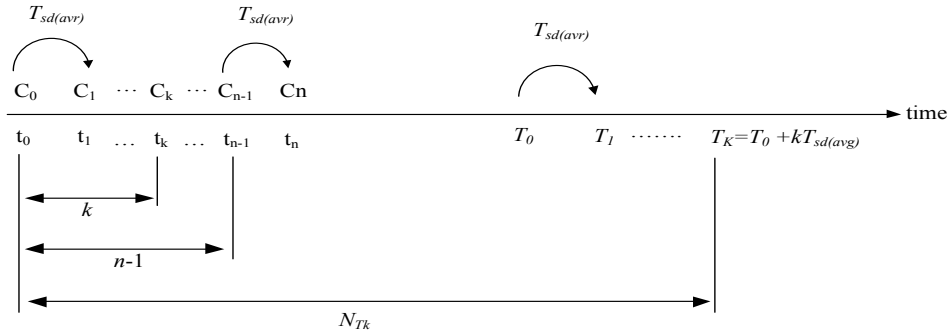


Figure 6.5 Average arrival interval of the next possible Gold request after establishing C_k

The higher and the lower bound of the buffering time are calculated as follows, where t_0 is the time at which the connection C_0 is being processed, T_0 is the time at which the connection C_0 is released, T_{th} is the maximum amount of time during which the request will be queued, N_{HP} is the number of the established high-priority connections between either *s-d* or *d-s* pairs by t_n, N_{sd} is the total number of the requests between either *s-d* or *d-s* pairs by t_n, v is an integer, ξ shows the percentage of high-priority requests, and $T_{sd(avr)}$ is the average arrival period of connections after which a high-priority request between *s-d* or *d-s* pairs may show up.

$$N_{T_k} - (n-1) \leq k \qquad \text{THEN} \qquad N_{T_k} \leq n + k - 1 \tag{6.1}$$

$$N_{T_k} = \frac{T_k}{T_{sd(avr)}} \qquad \text{THEN} \qquad T_k \leq (n + k - 1) \times T_{sd(avr)} \tag{6.2}$$

$$\text{THEN} \quad T_0 \leq T_k \leq (n + k - 1) \times T_{sd(avr)} \tag{6.3}$$

Assuming $\begin{cases} \nu = n + k - 1 \\ T_{sd(avr)} = \dfrac{t_n}{N_{HP}} \\ N_{HP} = \xi \times N_{sd} \end{cases} \quad 0 < \xi \leq 1$

THEN $T_{thmax} = \dfrac{\nu * T_0}{\xi * N_{sd}}$ 6.4

Assuming $k < n$, $\begin{cases} \nu_{min} = n \\ \nu_{max} = 2 \times n \end{cases}$ THEN $T_0 < T_{th} < 2T_0$ 6.5

6.4.5 The RWA and updates modules

To have a fair comparison between the existing (SSPP, SPA, SLA-aware) and the proposed (APSA) mechanisms, the RWA and wavelength update modules used in this part of the thesis are the same as discussed in detail in Chapter 5. The RWA module consists of a routing module and a wavelength assignment and graph matrices update module. The request to which RWA and updates modules are applied is a modified connection either by employing the WMPA parameter or by using the TMPA module. The only change in this module is that if the request is of connection release type, in addition to the graph and wavelength matrices, the TMPA matrix is also updated.

Algorithm 6.4 BHC module

Input: $ECM_{(s,d)}$, Original request $\{C_j(s, d, A_r, p, T_{arrival})\}$, $TMPA_{(s,d)}(mxm)$, m as number of nodes in the network

Output: Modified Request $\{C'_j(s, d, A_r, p, T'_{arrival})\}$

1. FOR all values of k smaller than m $\{\forall k \in \{1,\ldots,m\}\}$

   DO

   Check the TMPA matrix, find the smallest k^{th} row of the TMPA matrix such that it satisfies: $A_{rCj} \leq MPA^{k}_{(s,d)}$

2. END

3. IF $T_k < T_{th}$ THEN

   $T'_{arrival} \leftarrow T_k + \varepsilon$ AND

Update the CRM matrix with the modified connection request $\{C'_j(s, d, A_r, T'_{arrival})\}$

ELSE

Block the request C_j AND Terminate the subroutine

4. FOR all values of MPA in TMPA matrix $\{\forall MPA^k_{(s,d)} \in TMPA_{mxm}\}$

DO

IF $A_{rCj} > MPA^k_{(s,d)}$ THEN

Block the request $C_{j(s,d)}$ AND Terminate the subroutine

4. END
5. RETURN the Modified Request $\{C'_j(s, d, A_r, p, T'_{arrival})\}$

6.5 PERFORMANCE EVALUATION

To evaluate the network performance, dynamic traffic has been selected for performance analysis, and the ASR, the BP, the AWPC, and the resource overbuild (RO) of the modified APSA mechanism are compared with other existing algorithms. The RO computes the ratio of the sum of wavelength links for established backup paths to the sum of wavelength links for established primary paths. The performance of the modified APSA algorithm is compared with the schemes in which there are either no automatic SLA negotiations like SSPP [11] and [12], or SLA-aware algorithms such as SPA presented in Chapter 4 and the algorithm presented in [23], called in this thesis the SLA-aware algorithm. Some results of this part of the thesis are also available in [61] as one of the published contributions of this thesis.

6.5.1 Simulation environment

The modified APSA algorithm has been evaluated based on the simulation environment discussed in Section 3.5.3.1. The changes applied to the injected traffic are as follows: Connection availability requests are uniformly distributed between two classes of traffic: Gold class with the availability of 0.9999, and Silver class with the availability of 0.999. To simulate an environment with a large number of high-priority requests, the percentage

of high-priority requests is considered a constant value of ξ=50% for analyzing the effect of connection duration on network performance discussed in Section 6.5.2, and variable values ranging from ξ=10% to 80% for analyzing the effect of changes in the number of high-priority requests discussed in Section 6.5.3. The connection arrival process is a Poisson process with constant arrival rate of β=40 connections per unit of time. The holding time of the connections follows an exponential distribution with a mean value ranging from μ=50 to 500 units of time. Despite the simulation environments in Chapters 3 to 5 in which μ was constant and β changed, in this chapter β is considered constant and μ changes. Based on the definition of offered load in A.1 and A.2, the performance evaluation in this chapter is based on the variable holding time (μ) of the connections, so that, the offered load ranges from $2x10^3$ to $20x10^3$ Erlangs. This helps to show the effect of the time variation on the evaluation process. For the sake of simplicity and to better show the effect of the algorithm on serving high-priority connections, it is assumed that T_{th} takes its maximum value.

6.5.2 Simulation results: the effect of connections' duration variations

As the first step of the performance evaluation, the effect of the holding time variation on network performance is studied. Figure 6.6 compares blocking probability of the APSA mechanism with the SSPP [11] and [12], SLA-aware [23], and SPA (see Chapter 4) algorithms. As shown in Figure 6.6, the APSA mechanism has better BP performance while the other existing algorithms have almost the same blocking rates for connections with long durations. To simulate a high risk network (see Chapter 2), the links' availabilities are considered low enough ranging from 0.99 to 0.9995 [22]. This makes the blocking probability of the mechanism high. The graphs in Figure 6.6 have an error ranging $\mp 1x10^{-3}$-$1.5x10^{-3}$. For the offered load of $12x10^3$ Erlangs, the 95% confidence interval of BP for the APSA mechanism is [0.969 0.971] which translates to a 0.1% relative error.

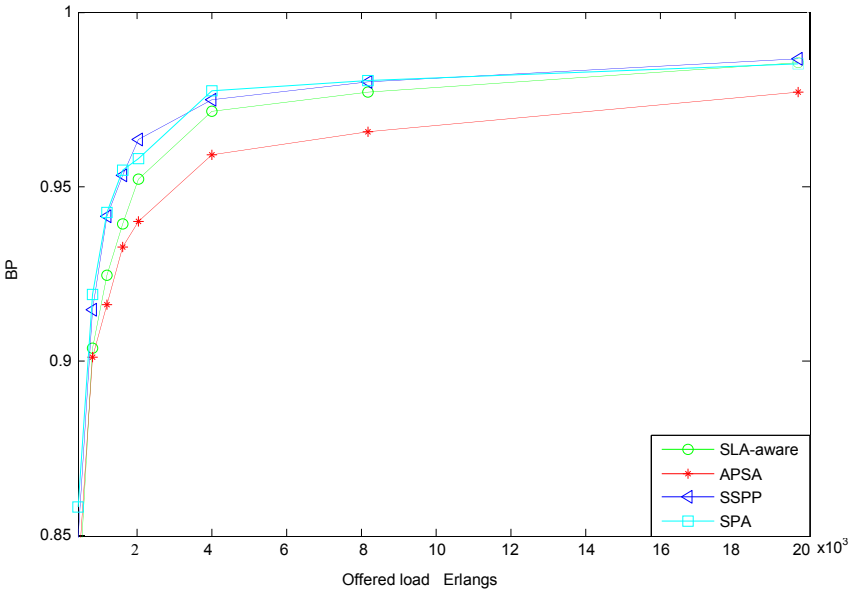


Figure 6.6 The effect of connections duration variation on blocking probability

Figure 6.7 shows the effect of connections duration variations on the AWPC. As shown in Figure 6.7, the APSA mechanism presents almost 13% decrease in the AWPC in comparison to the other algorithms. The graphs in Figure 6.7 have an error ranging from ∓ 0.24 to ∓ 0.5 wavelengths.

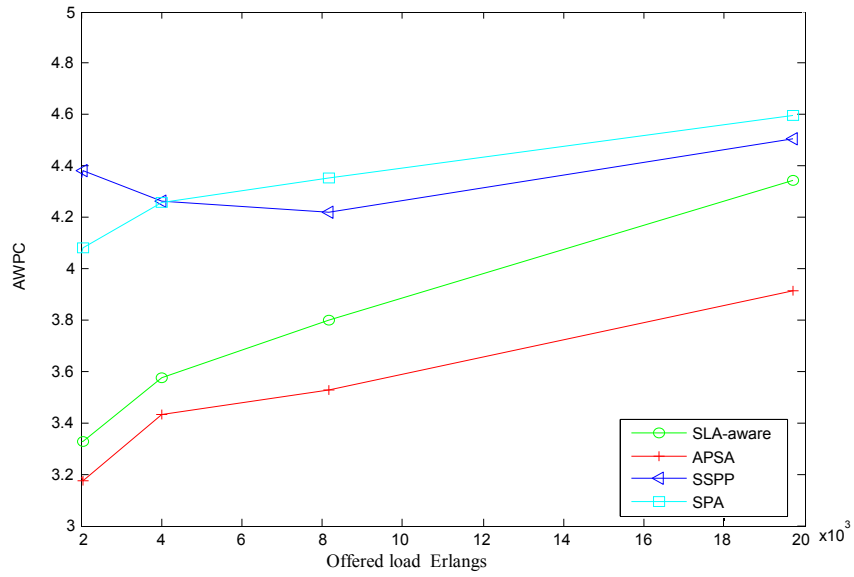


Figure 6.7 The effect of connections duration variation on average number of the allocated wavelengths per connection

Figure 6.8 shows the effects of connection duration on resource overbuild compared to other algorithms. While the SLA-aware and SPA algorithms have worse resource overbuild performance than the SSPP for long duration connections, the APSA mechanism shows almost 20% decrease in RO as observed in Figure 6.8. Based on the resource overbuild definition presented earlier in this chapter, it shows the APSA mechanism selects the backup paths more optimally and efficiently compared to other protection schemes. The graphs in Figure 6.8 have an error ranging around $\mp 4 \times 10^{-4}$ - 8×10^{-4}. For the offered load of 12×10^{3} Erlangs, the 95% confidence interval of the RO for the APSA mechanism is [0.0094 0.0106] which translates to a 6.3% relative error.

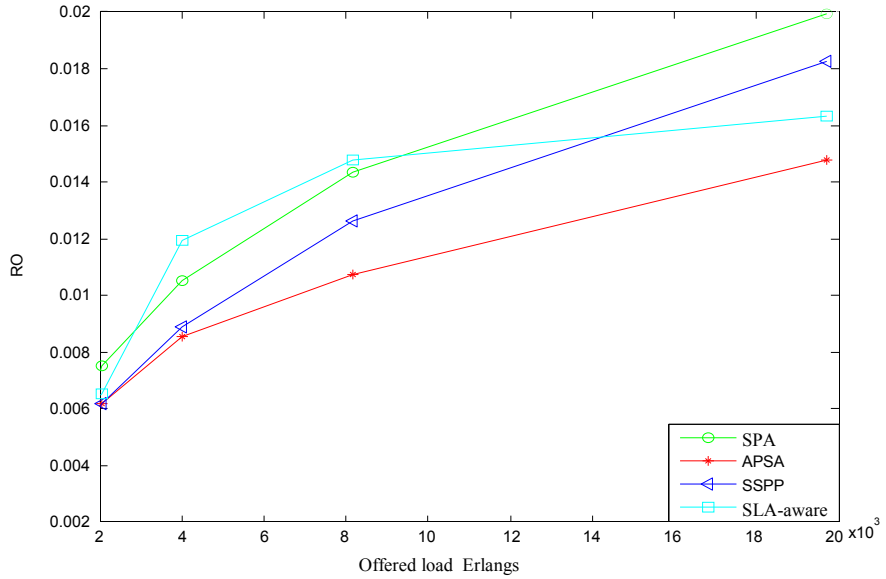


Figure 6.8 The effect of connections duration variation on resource overbuild, compared to other algorithms

Figures 6.9 to 6.11 show the effect of connection duration variation on the ASR in the APSA mechanism compared to the other algorithms. As observed in Figure 6.9, the APSA algorithm improves the ASR for Gold requests (ASR-gold) by 2.5% on average. In addition, the improvement in Gold requests does not degrade the ASR of Silver (ASR-silver) requests as it is shown in Figure 6.10, so that the APSA mechanism either has the same or higher ASR for Silver class of traffic than the other algorithms.

That is, to accommodate high-priority traffic, the proposed APSA algorithm does not reduce service to other classes of traffic. As in Figure 6.11, the ASR of all types of traffic (ASR-total) shows an improvement of almost 2% on average for APSA algorithm compared to other algorithms. The graphs in Figure 6.11 have an error ranging from ∓0.08% to ∓0.2%. For the offered load of $12x10^3$ Erlangs, the 95% confidence interval of ASR for the APSA mechanism is [2.9% 3.1%] which translates to a 3.6% relative error.

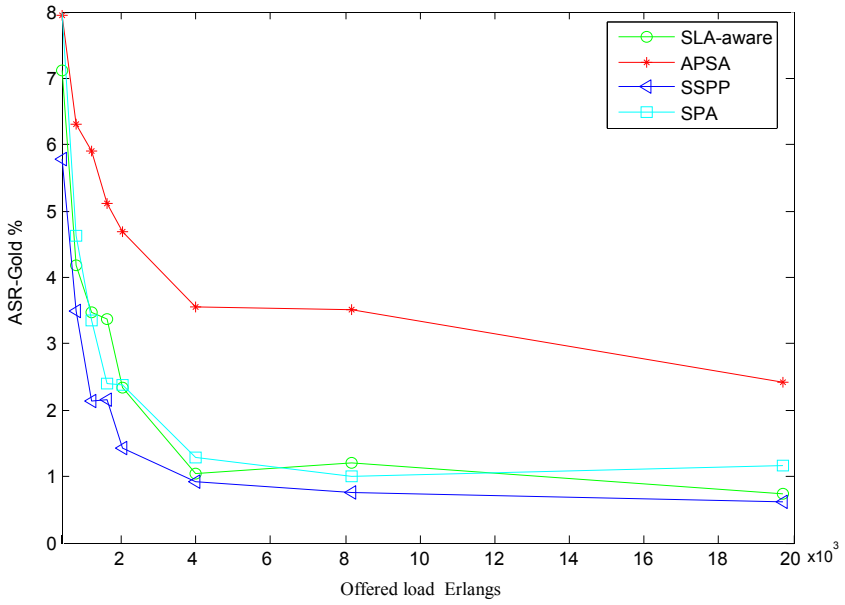


Figure 6.9 The APSA availability satisfaction rate for Gold requests compared to other algorithms

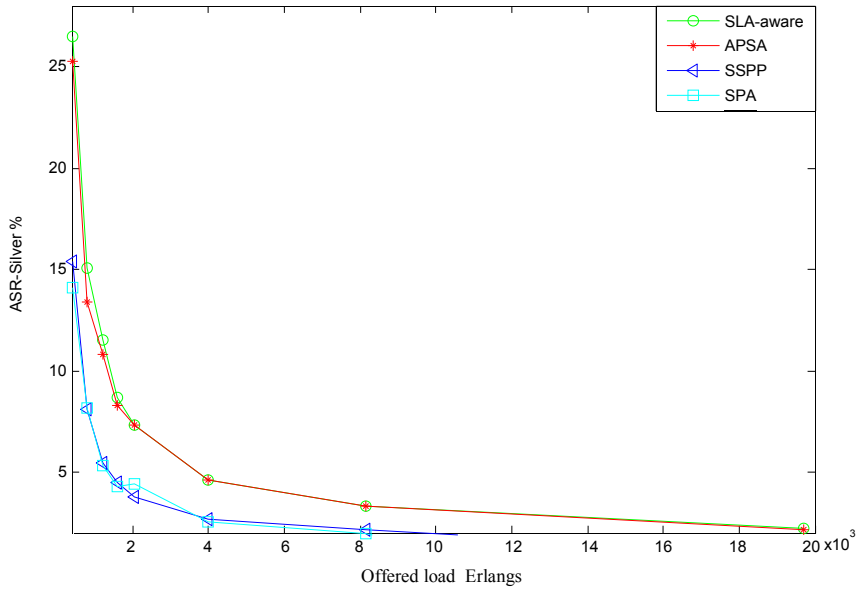


Figure 6.10 The APSA availability satisfaction rate for Silver requests compared to other algorithms

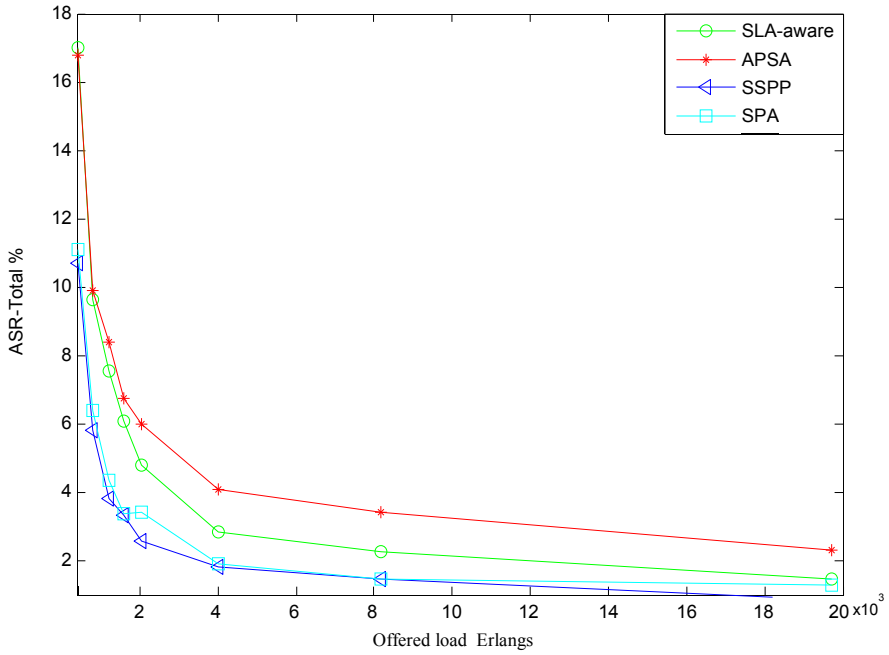


Figure 6.11 The APSA availability satisfaction rate for all traffic types, compared to other algorithms

6.5.3 Simulation results: the effect of changes in the number of high-priority connections

As the second step of the performance evaluation, the effect of changes in the number of high-priority requests on network performance is studied. This section studies how the proposed APSA mechanism behaves when the percentage of Gold requests increases from 10% to 80%. As Figure 6.12 shows, the APSA algorithm has an average increase of 9.1% in the RO for ξ ranging from 10% to 80% while the SLA-aware algorithm has an average growth of 17.2% which is almost twice that of the APSA algorithm. In addition, Figure 6.12 shows for longer connection durations, the APSA algorithm behaves better since the curves for different values of ξ in the APSA algorithm converge to the lower RO. The graphs in Figure 6.12 have an error ranging around $\mp 4\text{x}10^{-4}$-$8\text{x}10^{-4}$.

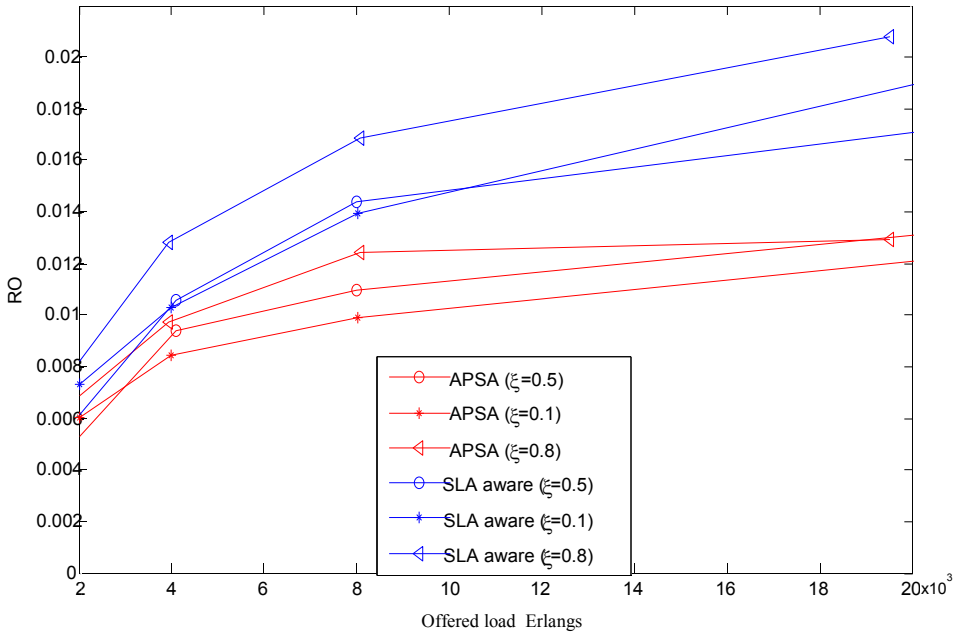


Figure 6.12 The effect of changes in the number of high-priority requests on resource overbuild of the APSA mechanism compared to other algorithms

The blocking probability of high-priority requests, BP-gold, has been considered as the number of the blocked Gold requests over the total number of the Gold requests. Figure 6.13 shows that as ξ increases, BP-gold of the APSA and SLA-aware algorithms decreases since both are priority-aware algorithms. However, the APSA mechanism

better accommodates high-priority requests as ξ increases from 10% to 80%, and decreases blocking probability by 3.5% on average while SLA-aware algorithm only drops it 1.6% on average. That is, the other algorithm improves the blocking rate of high-priority requests less than the APSA when the number of such requests increases. The graphs in Figure 6.13 have an error ranging from $\mp 7 \times 10^{-4}$ to $\mp 2 \times 10^{-3}$. For the offered load of 12×10^{3} Erlangs, the 95% confidence interval of BP for the APSA mechanism is [0.0928 0.932] which translates to a 0.2% relative error.

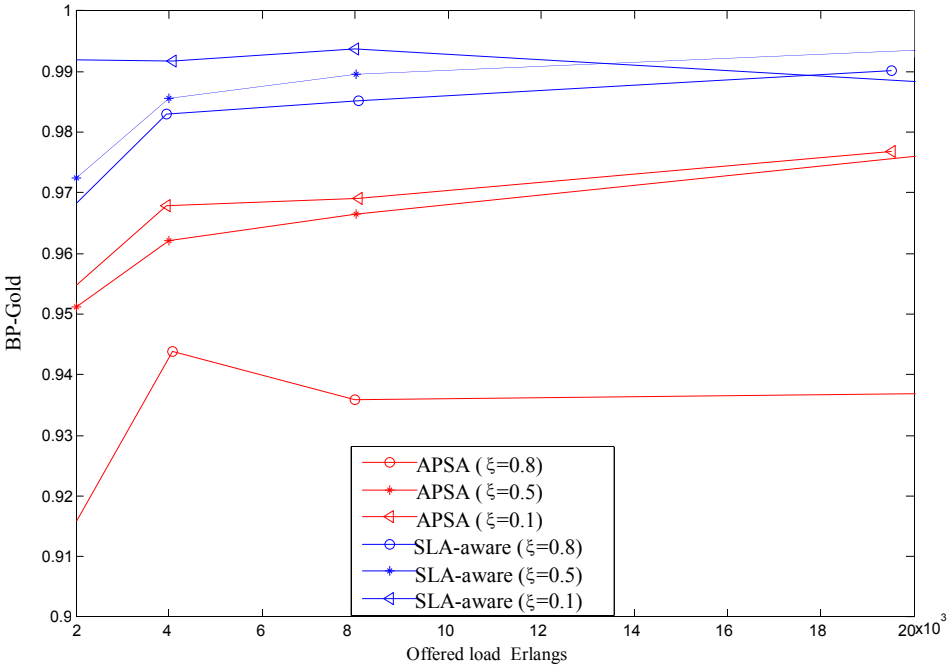


Figure 6.13 The effect of changes in the number of high-priority requests on blocking probability of the APSA mechanism compared to other algorithms

Likewise in Figure 6.14, the APSA algorithm better accommodates high-priority requests as it increases the ASR of Gold requests with long connection duration, ASR-gold, by almost 4% when the percentage of high-priority requests, ξ, varies from 10% to 80%. However, the SLA-aware algorithm cannot accommodate Gold requests with long duration connections, when ξ varies from 10% to 80%. The figure also shows ASR-gold performance degrades when the connections duration becomes longer.

The effect of changes in the number of high-priority requests and holding time on standard shared mesh protection scheme is shown in Figure 6.15. As it is expected and verified through the graphs in Figure 6.15, the SSPP protection scheme has no understanding of the class of traffic it receives and treats all the requests the same. This is the reason why the blocking rate, resource rebuild, and availability satisfaction rate for different values of ξ is almost the same. In addition to the number of Gold requests, Figure 6.15 shows that the SSPP highly degrades network performance of the requests of long durations with increasing blocking rate and resource overbuild, and decreasing availability satisfaction ratio.

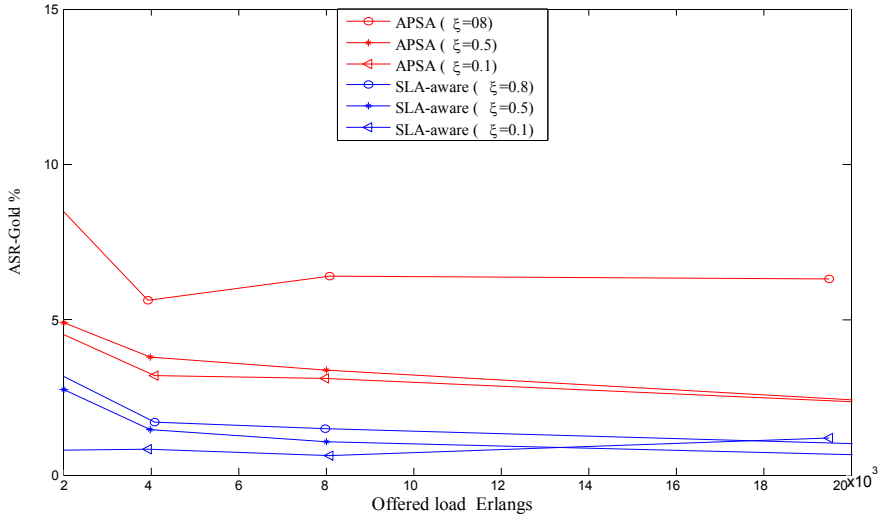


Figure 6.14 The effect of changes in the number of high-priority requests on availability satisfaction rate of the APSA mechanism compared to the SLA-aware algorithm

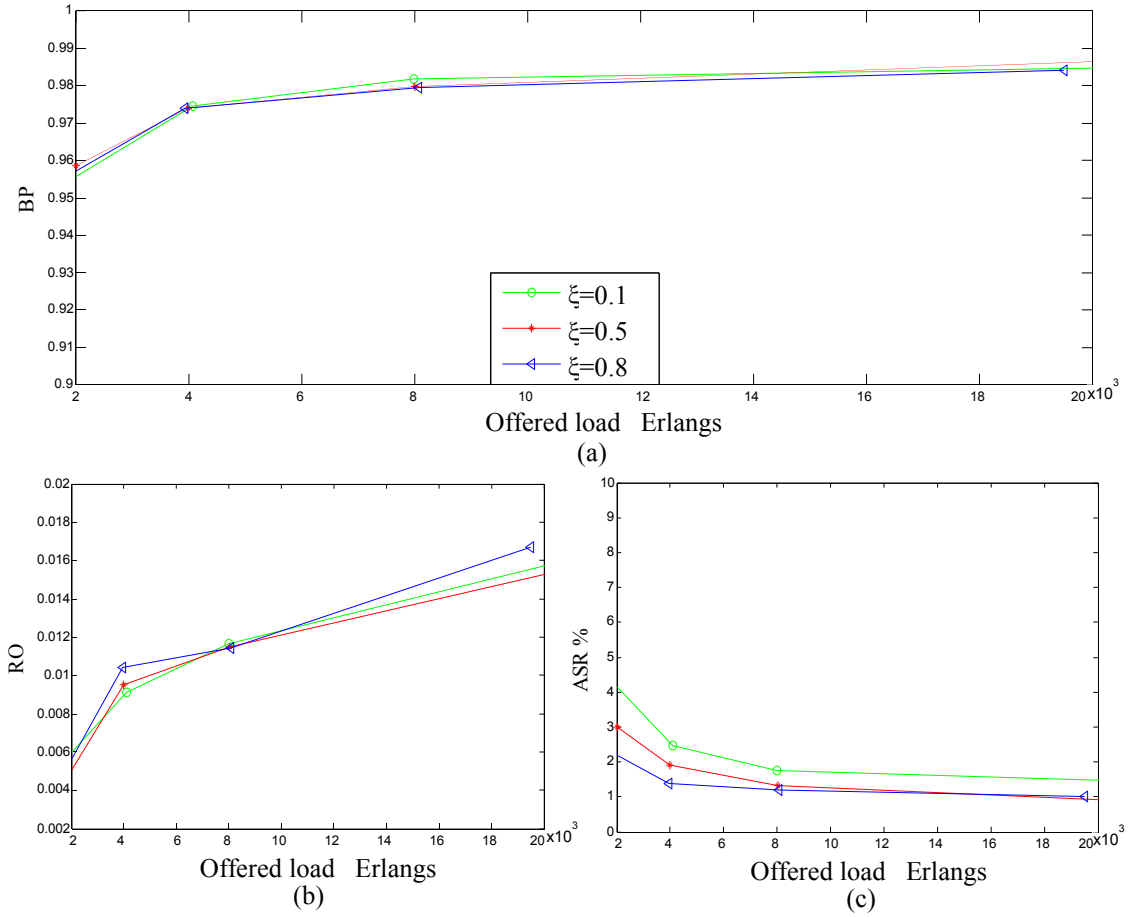


Figure 6.15 The effect of changes in the number of high-priority requests on SSPP scheme performance for (a) blocking probability (b) resource overbuild (c) availability satisfaction rate

6.6 SUMMARY

In this chapter, an adaptive provisioning SLA-aware algorithm has been introduced over shared mesh survivable WDM networks. The proposed mechanism consists of two parts, a novel provisioning algorithm which buffers and further processes the potentially blocked high-priority connection requests, and a new time-aware path constraint which takes advantage of availability and holding-time as two crucial SLA connection parameters.

The APSA mechanism has been developed to overcome the shortcomings of other existing algorithms to better serve a large number of high-priority connection requests

with fairly long durations. To achieve this goal, a novel traffic engineering path constraint, TMPA, has been introduced. The TMPA path constraint benefits from two important SLA connection parameters, requested availability and holding time. The TMPA metric helps the APSA algorithm to buffer the potentially blocked high-priority requests and to serve them in a future time rather than blocking them. The mechanism has also considered a means of controlling the buffering duration.

The simulation results show the network performance improvement of the proposed APSA algorithm when the number of high-priority requests increases. They also show how the APSA mechanism better accommodates high-priority connections with dramatically long holding time.

CHAPTER 7 HISTORY-AWARE SLA-BASED MECHANISM OVER SHARED-MESH WDM NETWORKS

7.1 INTRODUCTION

One of the concerns from a service provider's point of view is to keep the costs of the services they offer as low as possible. To achieve this goal, service providers should meet the customer requirements based on the requests considered in an SLA contract, otherwise they may be penalized for the period of time during which the SLA has been violated. The service provider's responsibility is to provide services which comply with SLAs in the least expensive manner. In fact, service providers follow two goals at the same time: satisfying requested services with the least SLA violations. In this chapter, a routing mechanism is proposed by which the primary and backup paths are selected in a way that the SLA violation and the revenue of the company are considered as two important factors for choosing the paths.

For the networks in which the links are reliable enough to satisfy the connection requests, the down time (DT) of the connections usually may not exceed the allowable down time (ADT) considered in the SLA. In this case, service providers can satisfy the SLA content while they are exploiting the surplus (unused) portion of the ADT of the connections to serve future requests. That is, a mechanism may recognize the connections whose SLA requirements are satisfied even if they are terminated before their requested holding times have expired. In networks with the large number of connection requests, this mechanism may save required period of time for those requests which are potentially blocked by other schemes. For the networks in which the links are of high risk but the connection requests have long durations, the same condition mentioned above may happen.

The contributions presented in this chapter are in two parts. In the first part, a routing algorithm is discussed which benefits from a new cost function for the path calculation. The path selection policy in the introduced routing mechanism in this chapter is based on the possible and allowable down time of the paths. In the second part, a mechanism is

presented to either avoid the SLA violation or at least minimize it by proposing a new path attribute. The proposed path attribute in this chapter flags established paths by SLA violation factor, and creates a history of paths and their degree of riskiness. The main goal of the mechanism proposed in this chapter is to bring higher revenue to ISPs. Since the proposed mechanism keeps track of a specific attribute of the paths as the paths history, it has been called in this thesis history-aware mechanism. The simulation results of both parts are compared to conventional algorithms [11], [12] and existing related mechanisms [62], [23] in terms of the revenue that a service provider can earn. First, some aspects of the mechanism will be justified using an analytical model.

The chapter is organized as follows: Section 7.2 identifies the motivations and objectives behind this chapter's contributions. Section 7.3 investigates an analytical model to pave the way for discussing the proposed mechanism. In Section 7.4, a new path attribute is presented. Section 7.5 presents a new path-cost function. Section 7.6 proposes a routing algorithm which benefits from the new path attribute and cost function introduced in the previous sections. Section 7.7 investigates the performance of the proposed mechanism through simulations and compares it to other existing algorithms. Section 7.8 summarizes the discussion.

7.2 MOTIVATIONS AND OBJECTIVES

In the proposed work presented in previous chapters, algorithms and mechanisms to satisfy the SLA requirements were proposed. However, no consideration was given to what would happen if the SLA was violated. This is a motivation for introducing a new mechanism that considers SLA violations as a factor and tries not to violate it or to minimize such violations. To achieve this goal, the mechanism needs a tool to relate the routing algorithm to SLA violations. A new risk-aware path attribute, which flags paths based on their degree of riskiness, is introduced for this purpose. The degree of riskiness is determined by approximating the probability of SLA violation.

The cost function of optimal path calculation reported in earlier chapters was based on the path availability and number of assigned wavelengths. With the definition of the new path attribute based on the SLA violation, a new path-cost function is introduced which combines the previously proposed cost functions with the newly defined path attribute to decrease the probability of SLA violation. This is the motivation for introducing a new cost function which is based on the number of assigned wavelengths, path failure arrival rate, and the path attribute.

7.3 AN ANALYTICAL MODEL INVESTIGATION

To explain the effect of the routing algorithm presented as the first part of the contribution, an analytical model is presented. The topology shown in Figure 7.1 includes two paths from a source to a destination with different path availabilities, A_ps. It is assumed that the requested availability in the SLA is A_r=0.985 and two paths are the legitimate candidates, i.e., they meet the availability requirements in the SLA. Clearly, the one with the minimum cost from the service provider's point of view should be selected.

As shown in Figure 7.1, the links forming the paths have the same mean time to repairs (MTTR) and different failure arrival rates, λ_j. The relationship between MTTR, failure arrival rate, and availability is discussed later in Equations 7.1 and 7.3. Based on the real-world statistics published by Bellcore, link MTTR and link mean time between failures (MTBF) are the longest times among other types of MTTR and MTBF, such as equipment MTTR, transmitter and receiver failure rate [63]. Based on this fact, only link MTTR and MTBF are considered in this thesis. The distribution of the MTBF for links forming the path 1234 is considered to be a Uniform Distribution of U[1000, 4000] hours [31] and for the path 154 is considered to be U[4000,10000] hours [31]. MTTR of the links is considered constant for all paths for a fair comparison and is 12 hours for both paths.

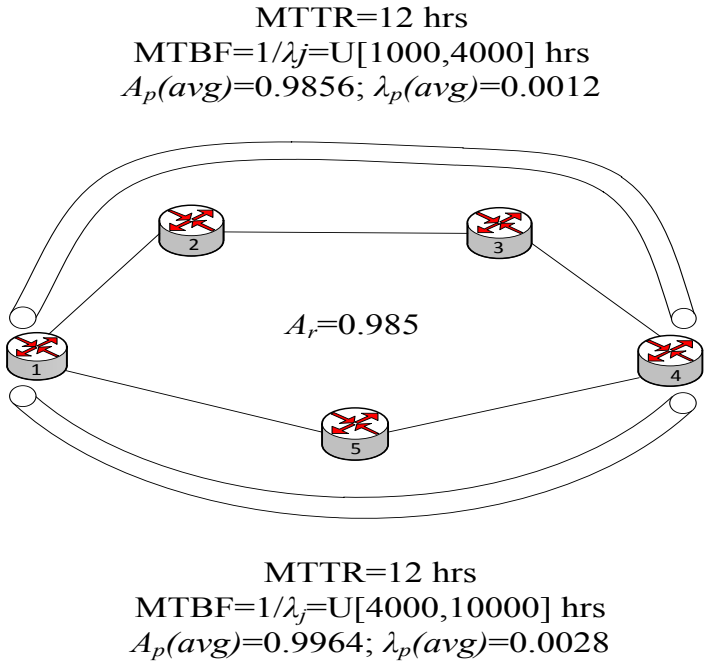


Figure 7.1 An analytical model of optimal path selection process based on the path failure arrival rate

To see how the different paths are selected by different algorithms, a couple of scenarios over which the different mechanisms choose their paths are considered. If the problem is examined only from the availability perspective, path 1234 should be selected since this path requires lower availability based on Equation 7.1 presented in [64].

$$A_j = \frac{MTBF}{MTBF + MTTR} \tag{7.1}$$

However, if the number of wavelengths used on the selected path is considered, assuming both paths meet the availability requirement, the cost of the path 154 is less than the path 1234 based on the algorithm used in [62]. The cost function used in this part of the discussion is presented as Equation 7.2 and is adopted from [23], in which MTBF is representative of the failure arrival rate of a link, MTTR is the mean time to repair, and A_j is the link availability. This minimal cost from an ISP's point of view chooses the best path among a set of all legitimate paths, where $\alpha \leq 1$ is a constant that defines a weighting between resource utilization and link availability. H_p is the hop count of the chosen path

which is equal to the total number of wavelengths occupied by path P. Assuming α=0.8 [23], path 154 is selected as the minimal costly path.

$$f_{cost} = (1 - \alpha)H_p + \alpha A_p \quad 7.2$$

However, since the availability is usually close to one and the parameter α is also selected close to one [23], the cost function in Equation 7.2 considers more the hop count than the availability. Equation 7.4 is presented to resolve this shortcoming of Equation 7.2.

As discussed in detail in [65], considering the definition of the link availability in Equation 7.1, the failure arrival rate of a link can be calculated as in Equation 7.3 where A_j is the availability of the link j, λ_j represents the failure arrival rate of the link, and $MTTR_j$ is the mean time to repair of the link j.

$$\lambda_j = \frac{1 - A_j}{A_j * MTTR_j} \quad 7.3$$

However, in this chapter, a new definition of the optimal path cost function applicable to the path selection is defined in Equation 7.4, so that the cost of the path will be proportional to ω/λ where ω is the total number of wavelengths used to form the path and λ is the failure arrival rate for the selected path. With this new definition of the path cost, path 1234 will be selected since it has the higher failure arrival rate and consequently is less expensive for the service provider to allocate. In general, among several paths which meet the requested SLA requirements, the path with the lowest number of the assigned wavelength (ω) and highest failure arrival rate (λ) can be counted as the lowest path cost for a service provider. Assuming a fixed value for the mean time to repair and considering Equation 7.3, the higher link failure arrival rate translates to the lower link availability, and lower link availability translates to lower path availability, and consequently it translates to the lower cost to service providers. However, a more precise cost function will be introduced later in Section 7.5 which also considers the SLA violation risk as a factor in the optimal path selection.

$$f_{cost} \propto \frac{\sum_{i \in P} w_i}{\lambda_p} \quad 7.4$$

7.4 NOVEL RISK-AWARE PATH ATTRIBUTE

Before entering the discussion of introducing a new path attribute which considers the risk of SLA violation as a criterion, a couple of definitions which may help to give a better understanding of the proposed path attribute are presented below. The definition of the SLA violation risk, the way it is calculated, and the related assumptions have been discussed in Chapter 2. Assuming a constant value for MTTR, SLA violation risk can be written as Equation 7.5.

$$\text{SLA violation risk} = P_r(RADT < MTTR) \quad 7.5$$

in which the residual allowable down time (RADT) [30] for any link is calculated by the following formula where ADT is allowable down time of a link, the CDT is the cumulative down time, ANF is allowable number of failures, and the CNF is the cumulative number of failures.

$$\text{RADT} = \text{ADT} - \text{CDT} = \text{MTTR} \times (\text{ANF} - \text{CNF})$$

The number of failures is assumed to be uniformly distributed among all connections for simulation purposes. Since DT≠0, the residual holding time (RHT) is required to be monitored to calculate the residual allowable down time.

Definition: Committed service time (CST)

The committed service time (CST) is defined as the period of time during which an ISP is committed to provide the service to the customer avoiding any SLA violation based on the SLA contract. CST is defined below based on ADT and holding time (HT).

$$CST = HT - ADT$$

Definition: Satisfied committed service time requirement

The CST requirements are met when the ISP serves the customer's requests while avoiding SLA violations. If the ISP cannot fulfill this commitment, it will be penalized for the period of outage. Since, in general, the down time of failures could take different values, the larger value of DT (DT > RADT) translates to having SLA violation, and having SLA violation results in less possibility of CST satisfaction.

Definition: Path risk factor (PRF)

The PRF is defined as an SLA violation criterion by which a currently established path of certain class of service is evaluated as not risky, low risk, risky, or high risk. It shows how risky a path can be and how it can affect the future path computation process. The PRF is considered as a path attribute for each traffic level separately which creates an updated history of paths' specific virtue for all paths of the same source-destination pair.

The risk tolerance of a path is calculated based on two criteria:

1) The amount of time left for the allowable down time of the path
2) Whether or not any SLA violation occurs during the committed service time

PRF provides a path history for the algorithm by which the algorithm has a history of the network status based on how risky the paths of a specific source and destination pair are.

Definition: Established connection matrix including PRF property (PECM)

The matrix of currently established connections has already defined in Chapter 6. Path risk factorized established connection matrix (PECM) is a database of the currently established paths from a specific source-destination pair (s_p, d_q) which carries the PRF attribute of each request in each level of priority separately. The following matrix presentation shows a sample of this matrix calculated for Gold requests.

For all connections in the ECM: $$PECM^{Gold}_{(s_p,d_q)} = \begin{bmatrix} C_{1(s_p,d_q)} & PRF_{1(s_p,d_q)} \\ C_{2(s_p,d_q)} & PRF_{2(s_p,d_q)} \\ \vdots & \vdots \\ \vdots & \vdots \\ \vdots & \vdots \\ C_{j(s_p,d_q)} & PRF_{j(s_p,d_q)} \end{bmatrix}$$

As the first part of the contribution in this chapter, a unique path attribute is presented by which every decision making node has a picture of the network in terms of SLA violation risk of the possible candidate paths of certain level of priority for a certain source and destination pair. The SLA violation risk has been introduced in Equation 7.5. An approximation of Equation 7.5, by which having SLA violation is estimated, is used in PRF definition in Equation 7.6. The proposed path metric can be disseminated using the dynamic SLA negotiation proposed in Chapter 3 as an attribute of the prospective selected paths. The definition of the PRF metric is shown in Equation 7.6.

$$PRF = \begin{cases} 0 & \text{Path: not risky} & \text{IF } RADT > MTTR \text{ \& CST requirement are satisfied} \\ 1 & \text{Path: low risk} & \text{IF } RADT > MTTR \text{ \& CST requirement are not satisfied} \\ 2 & \text{Path: risky} & \text{IF } RADT < MTTR \text{ \& CST requirement are satisfied} \\ 3 & \text{Path: high risky} & \text{IF } RADT < MTTR \text{ \& CST requirement are not satisfied} \end{cases} \quad 7.6$$

7.5 NEW PATH COST FUNCTION

As the second part of the contribution presented in this chapter, the failure arrival rate is considered as a new link cost function for the path calculation. Since it is assumed that the MTTR is fixed and the link failure arrivals are independent, the failure arrival process will be additive. The overall failure arrival rate of a path, λ_p, can be defined as Equation 7.7 where λ_j is the failure arrival rates of the links forming the path P. The reasons why the failure arrival process can be additive over the above conditions has been discussed in [31] and [66].

$$\lambda_{\mathrm{p}} = \sum_{j \in \mathrm{P}} \lambda_j \qquad 7.7$$

To find the optimal path among a set of paths, a new optimal cost function is defined in Equation 7.8. This cost function is based on the proposed path attribute (PRF) and thus a path (P) with the minimum cost to the ISP can be found.

$$f_{cost} = \varepsilon \times \frac{\sum_{i \in P} w_i}{\sum_{i \in P} \lambda_i} + (1 - \varepsilon) \times PRF \qquad 7.8$$

where ε is a constant scaling factor that balances between the cost of the path in terms of number of assigned wavelengths, failure arrival rate, and the PRF. P is a set of legitimate paths. PRF is a path attribute and has been defined earlier. Regarding the above optimal cost function, the most optimal cost to an ISP will be earned when the following conditions are all met:

1) The number of assigned wavelengths is minimized (minimum hop count)
2) The value of the failure arrival rate is maximized (to save most reliable paths)
3) The value of the PRF is minimized (minimum SLA violations)

7.6 HISTORY-AWARE SLA-BASED SHARED PATH PROTECTION MECHANISM (HASP)

The HASP mechanism consists of two main modules, the RWA module and the release module. The block diagram of the HASP mechanism is shown in Figure 7.2 presenting the contents of each module separately. The HASP mechanism first modifies the cost of the links of the residual graph [32] using the failure arrival rates of the links as the link cost function. It takes the requests from the CRM matrix in a way that has no knowledge of the upcoming request. The CRM is a matrix of all connection requests through which the requests are served one by one. In this stage, a set of legitimate primary paths are calculated. The legitimate paths are the paths which fulfill the SLA requirements. The proposed algorithm then identifies whether a certain request needs a backup path based on the customer's request as well as the ISP's network capacity. To do so, it compares the

possible down time (PDT) of the previously calculated primary paths to allowable down time. Algorithm 7.1 presents the steps involved in the HASP mechanism including the routing and release modules. The steps 2 to 10 are the routing module operation and step 12 refers to the release module. The PDT is the period of down time of a connection request applied and calculated by the ISP based on the available network capacity. However, the ADT is the period of down time of a connection requested by the customer based on the SLA. The general definition of both is presented in Equation 7.9. For the PDT calculation, it is assumed that $A=A_p$ and for the ADT calculation $A=A_r$, where A_p and A_r are availability assigned by the ISP and requested by the customer respectively. For both cases, it is assumed that $T=\mathrm{HT_c}$, the holding time of the connection C.

$$(1-A)\times T=\begin{cases} ADT_c & \mathrm{A}=A_r \\ PDT_c & \mathrm{A}=A_p \end{cases} \tag{7.9}$$

In the case of having a backup path, A_p and A_r will be calculated through Equation 7.10 presented in [23] where A_{PB} is the joint availability of a primary-backup pair, a_{ij} is the availability of the path from i to j, B and P are a set of paths for backup and primary path pairs respectively.

$$A_{PB}=\prod_{(i,j)\in P} a_{ij}+\prod_{(i,j)\in B} a_{ij}-\prod_{(i,j)\in B\cup P} a_{ij} \tag{7.10}$$

After finding a set of primary paths or a pair of primary-backup paths, the algorithm selects the optimal path with the minimum cost to the ISP using Equation 7.8. The HASP algorithm calls the release module to terminate those connections whose CST requirements are met. The release module steps are explained in Algorithm 7.2.

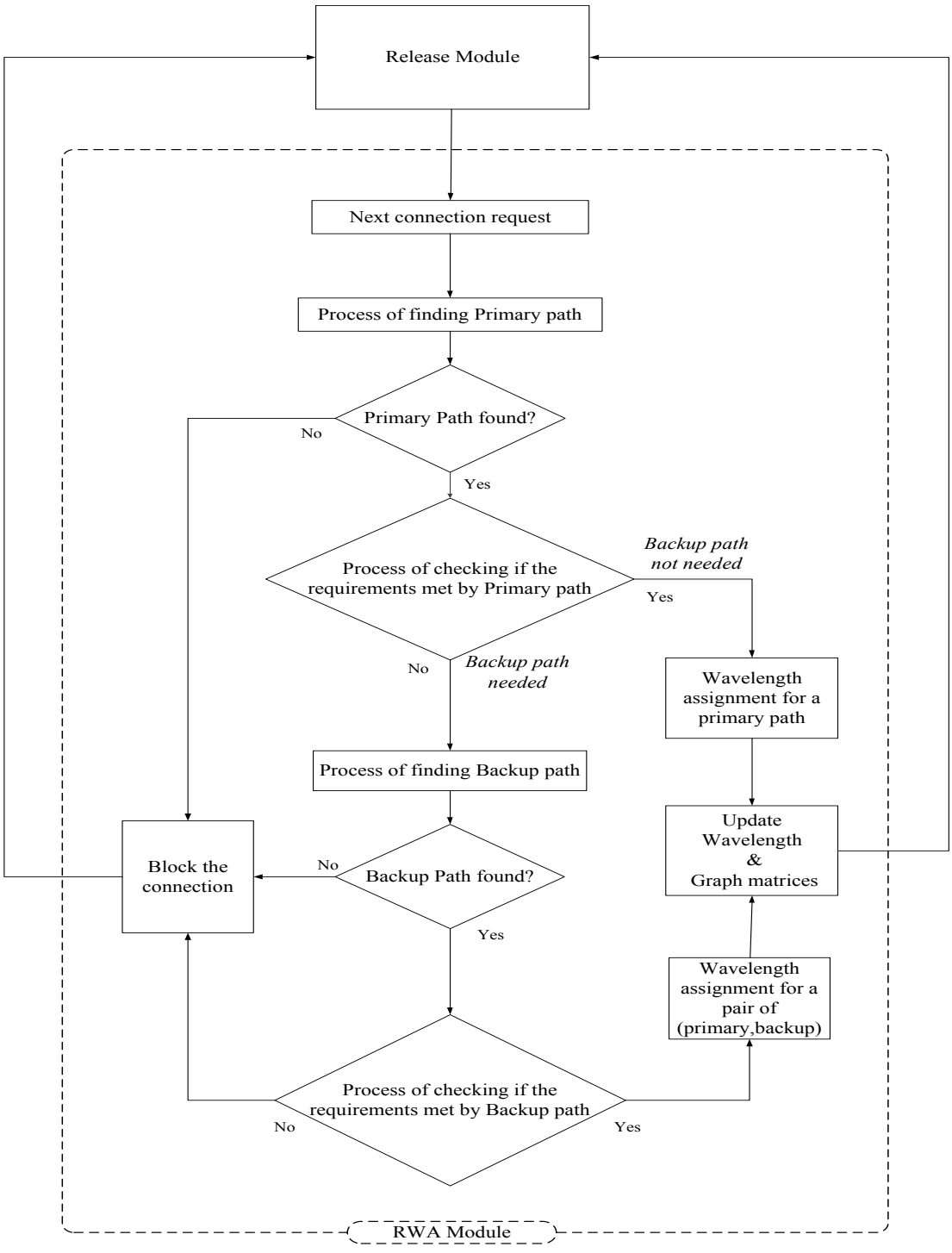


Figure 7.2 Block diagram of the proposed HASP mechanism

Algorithm 7.1 HASP Algorithm

Input: CRM, ECM, PECM matrices
Output: Optimal pair of P-B paths, Updated graph status

1. $n \leftarrow 1$
2. Serve n^{th} connection request
3. Modify the cost of the links of the residual graph using Equation 7.7
4. Apply *k-shortest path* algorithm to calculate a set of k possible primary paths for a given source-destination pair using the pre-calculated cost function in Step 3
5. IF the primary path not found THEN
   Block the connection
6. IF $PDT_{Cn} < ADT_{Cn}$ {No backup path needed}
   Find all possible primary paths and their PRFs from the PECM matrix AND
   Find the primary path with the lowest cost using Equation 7.8 AND
   Assign wavelengths for the primary path using the FF technique AND
   Update wavelength and graph matrix AND
   $n \leftarrow n+1$
   ELSE {backup path needed}
   Apply *Dijkstra* algorithm {to calculate backup paths for all possible primary paths}
7. IF the backup path not found THEN
   Block the connection
   ELSE
   Find all possible pairs of primary-backup paths using Equations 7.9 and 7.10 satisfying condition on Step 6
8. IF the pair of path not found THEN
   Block the connection
   ELSE
   Find the pair of paths with the lowest cost through Equation 7.8 AND
   Assign wavelengths for the backup path using Algorithm 5.5 AND
   Updated wavelength and graph matrix
9. RETURN Optimal pair of P-B paths
10. $n \leftarrow n+1$

11. Call Algorithm 7.2 {Release module}
12. Go to step 1

In addition to releasing the satisfied CST connections, Algorithm 7.2 flags the connections belonging to the ECM matrix as not risky, low risk, risky, or high risk paths based on Equation 7.6. Regarding the minimal cost definition in Equation 7.8 and PRF definition in Equation 7.6, Algorithm 7.2 releases the network resources of eligible paths while avoiding SLA violations. As the last step of the HASP algorithm, the release module updates the PECM matrix and residual holding time matrix (RHTM) and returns to Algorithm 7.1. The RHTM matrix keeps track of the residual holding times of all established connections belonging to the ECM, and PECM keeps the previously established connections together with their most updated PRF values.

The main differences between the mechanism proposed in this chapter and the mechanisms introduced in the previous chapters are: i) Link cost function is based on failure arrival rate rather than the availability, ii) Path cost function for choosing the optimal primary-backup pair of paths is based on failure arrival rate, the number of assigned wavelengths, and the path risk factor introduced in this chapter, iii) The algorithm exploits the unused portion of the ADT to serve future high-priority requests which is the responsibility of the release module introduced in this chapter, and iv) The algorithm considers SLA violations as a criterion to bring more profit to service providers.

Algorithm 7.2 HASP Release Module

Input: ECM, PECM, and RHTM matrices

Output: Updated RHTM, Flagged ECM

1. FOR all currently established connections in ECM matric
   DO
   IF $RHT_{Ci} < RADT_{Ci}$ THEN
   $RHT_{Ci} \leftarrow 0$ AND
   Modify C_i parameters
   END

2. Release the resources forming C_i path
3. Update the wavelength and graph matrix
4. Update RHTM
5. Flag the paths in ECM based on the PRF criterion using Equation 7.6
6. Update PECM with the flagged path
7. RETURN the matrices RHTM, ECM, PECM

7.7 PERFORMANCE EVALUATION

To simulate a real world environment, dynamic traffic has been selected for the performance analysis. The simulation compares the ASR, BP, AWPC, and the revenue earned by the service provider of the proposed algorithm with other standard and existing related algorithms.

Definitions for the BP, AWPC, and ASR were presented in the earlier chapters. The ISP revenue calculation will be shown later as Equation 7.11 adopted from [30]. Some results of this part of the thesis are also available in [67] as one of the published contributions of this thesis.

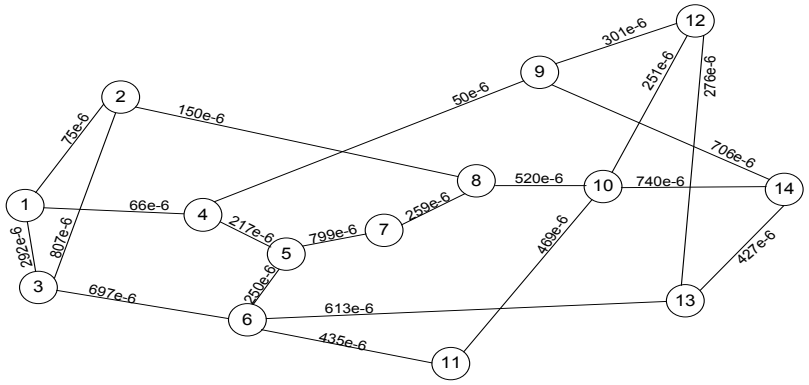


Figure 7.3 NSFNet network with high link failure arrival rates

7.7.1 Simulation environment

The HASP algorithm has been evaluated based on the simulation environment discussed in Section 3.5.3.1. Slight changes are applied as follows: The first part of the performance

evaluation in this chapter focuses on high risk networks. The definition of high risk networks are presented in Chapter 2. To simulate a network with high link failure arrival rate, the link availabilities are uniformly distributed between 0.99 and 0.9995. Based on Equation 7.3, this link availability distribution translates to uniformly distributed failure arrival rate between $40x10^{-6}$ and $840x10^{-6}$ connections per hour. The topology selected for this part of the simulation is NSFNet shown in Figure 7.3. Connection availability requests are uniformly distributed between two classes of traffic: Gold class with the availability of 0.9999, and Silver class with the availability of 0.999. For simulation purposes, ε, the scaling factor, has been considered 10^{-4} for high-risk networks, the value of k, for k-shortest path algorithm, has been set to 3, and the number of failures is assumed to be uniformly distributed among all connections.

7.7.2 Performance evaluation over high risk networks

In the first step of the first part of the evaluation, the performance of the routing and wavelength assignment module of the HASP mechanism is compared to the SSPP algorithm [11] and [12]. The performance of the HASP algorithm is also compared to the CSPP algorithm evaluated in Chapter 3 to show the superiority of the new routing algorithm in the first step. For this part of the simulation, the routing module performance is analyzed based on the offered load. The arrival process of connection requests is considered a Poisson process with arrival rate of β. The holding time of the connections follows an exponential distribution with a mean value of μ=1. For simulation purposes, β is ranging from 20 to 70 to simulate the offered load of 20 to 70 Erlangs.

Figure 7.4, Figure 7.5, and Figure 7.6 compare the BP, ASR, and AWPC of the HASP algorithm with the SSPP and CSPP schemes over the network shown in Figure 7.3. As Figure 7.4 shows, the proposed algorithm has 22.5% improvement in blocking probability, 11.5% lower assigned wavelength per connection, and about 11% higher availability satisfaction rate than comparable algorithms for the offered load of 40 Erlangs. Based on these measures, the conclusion is that the HASP algorithm is a proper choice for networks with high risk links. The graphs in Figure 7.4 and Figure 7.6 have an error ranging from $\mp 6x10^{-4}$ to $\mp 2.9x10^{-3}$ connections per hour. For the arrival rate of

β=40 in the HASP mechanism, the 95% confidence interval of the BP is [0.0585 0.0615] which translates to a 2.5% relative error, and the 95% confidence interval of the ASR is [94.8% 95.2%] which translates to a 0.15% relative error. The graphs in Figure 7.5 have an error ranging from $\mp$0.12 to $\mp$0.23 wavelengths.

As the second step of the first part of the evaluation, the performance of the routing module of the proposed HASP mechanism is compared to the SLA-aware algorithm presented in [23] for the network shown in Figure 7.3. For this part of the simulation, the offered load is a function of the service time of connections. The connection arrival process is considered a Poisson process with constant arrival rate of β=40. To model the long connection holding time ranging from 3 months to 2 years, the holding time of the connections follows an exponential distribution with a mean value ranging from μ=90 to 720 Days. Connection availability requests are also uniformly distributed between two classes of traffic: Gold class with the availability of 0.9999, and Silver class with the availability of 0.999. Although the horizontal axis in Figures 7.7-7.9 and Figures 7.14-7.16 show connection duration ranging from 90 to 720 Days, it can easily translate to the offered load ranging from $3.6\text{x}10^3$ to $28.8\text{x}10^3$ Erlangs. The main reason that the horizontal axis is shown in terms of the duration rather than the load is to show the effect of the connection duration on network performance.

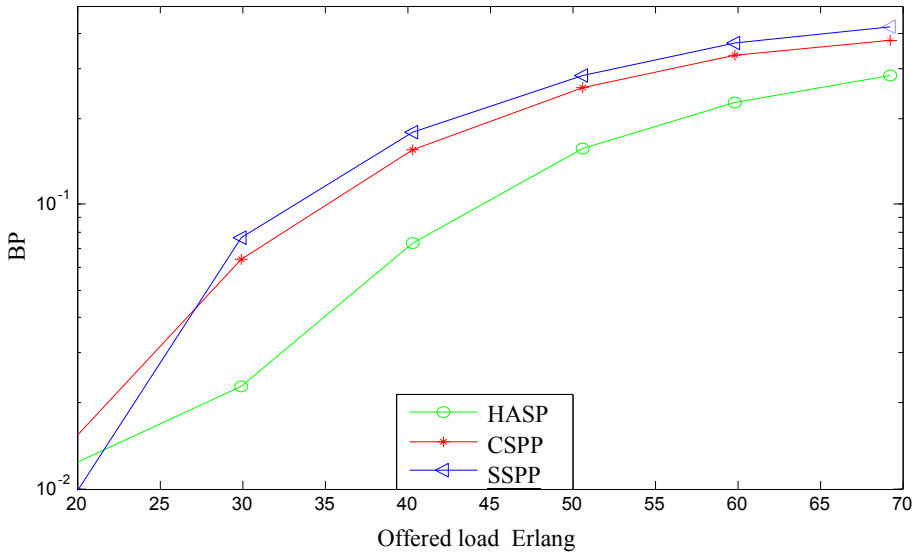


Figure 7.4 The BP performance analysis of the HASP algorithm compared to the standard algorithms over a network with high failure arrival rate

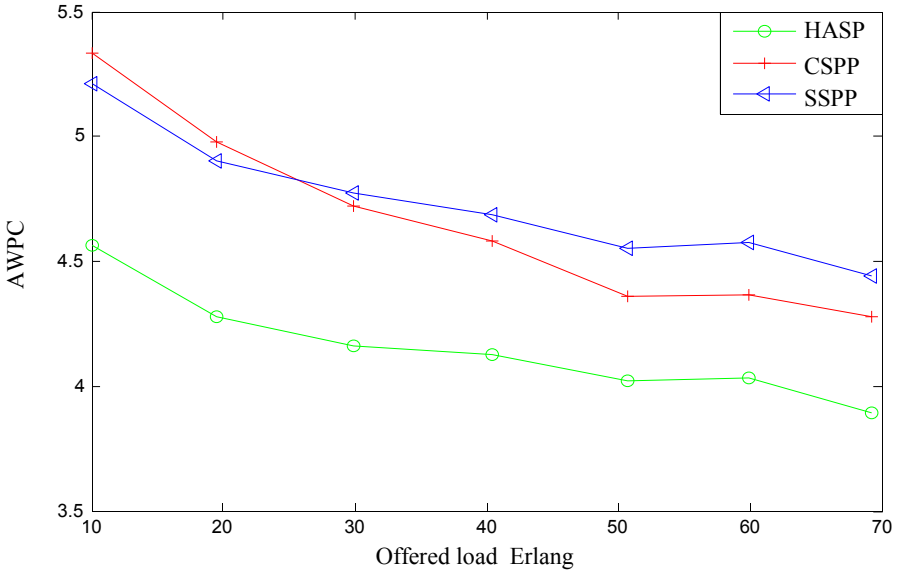


Figure 7.5 The AWPC performance analysis of the HASP algorithm compared to the standard algorithms over a network with high failure arrival rate

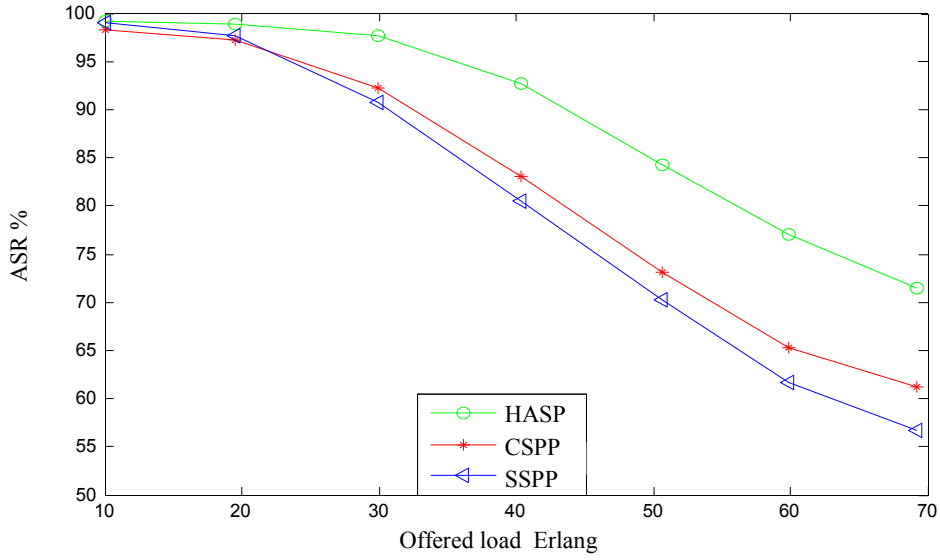


Figure 7.6 The ASR performance analysis of the HASP algorithm compared to the standard algorithms over a network with high failure arrival rate

As Figure 7.7, Figure 7.8, and Figure 7.9 show, for a connection time of 12 months, there are 5% lower assigned wavelength per connection, and about 3% higher availability satisfaction rate, and marginally better blocking probability than the SLA-aware

algorithm [23] over a network with high failure arrival rate. The graphs in Figure 7.7 and Figure 7.9 have an error ranging from $\mp 7x10^{-4}$ to $\mp 10^{-3}$.

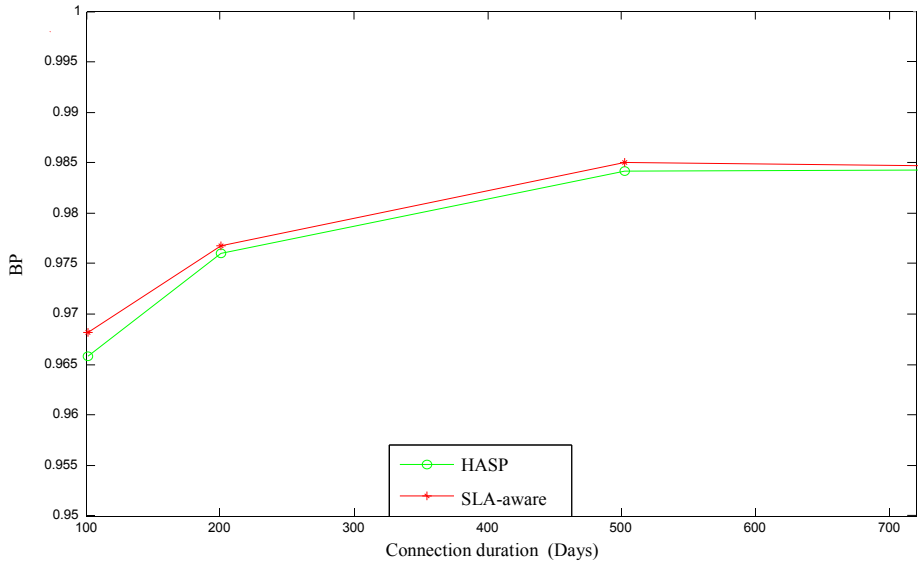


Figure 7.7 The BP performance analysis of the HASP algorithm compared to the SLA-aware algorithm over a network with high failure arrival rate

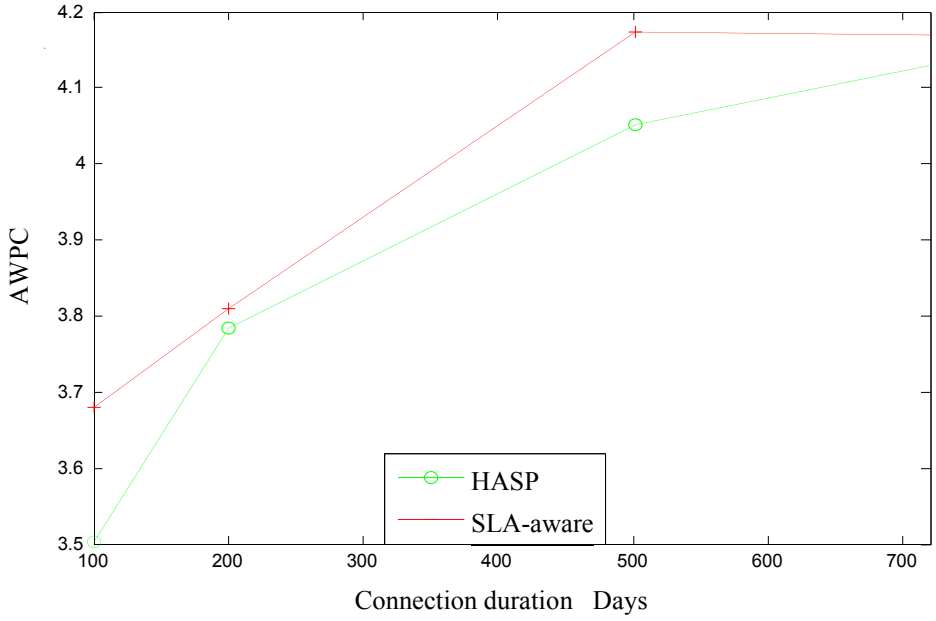


Figure 7.8 The AWPC performance analysis of the HASP algorithm compared to the SLA-aware algorithm over a network with high failure arrival rate

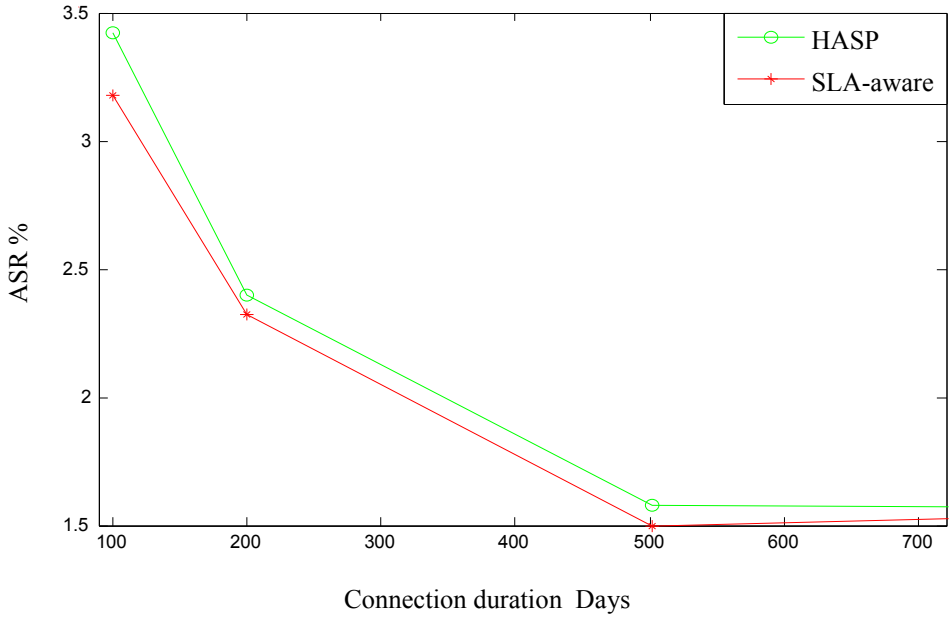


Figure 7.9 The ASR performance analysis of the HASP algorithm compared to the SLA-aware algorithm over a network with high failure arrival rate

7.7.3 Performance evaluation over low risk networks

The second part of the performance evaluation focuses on low risk network. The topology selected for this part of the simulation is NSFNet shown in Figure 7.10. To simulate a network with low link failure arrival rate, the link availabilities are uniformly distributed between 0.999 and 0.99999 [23]. Based on Equation 7.3, this link availability distribution translates to uniformly distributed failure arrival rate between 0.8×10^{-6} and 80×10^{-6} connections per hour. For simulation purposes, ε, the scaling factor, has been considered 10^{-5} for low-risk networks. The rest of the conditions considered in the first part of the simulation are maintained the same for the second part of the simulation.

Figure 7.11, Figure 7.12, and Figure 7.13 compare BP, AWPC, and ASR of the HASP algorithm respectively with the standard algorithms SSPP and CSPP over the network shown in Figure 7.10.

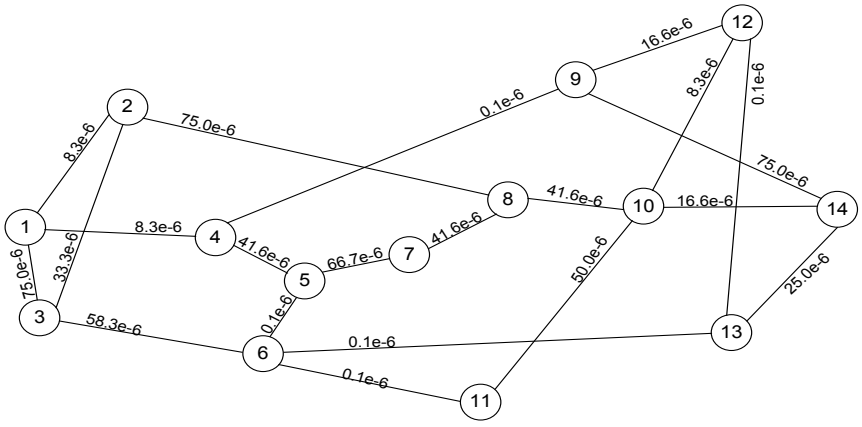


Figure 7.10 NSFNet network with realistic link failure arrival rates

As Figure 7.11 shows, the proposed HASP mechanism has more than 97% improvement on average in blocking probability compared to existing algorithms. The graphs in Figure 7.11 have an error ranging from $\mp 6 \times 10^{-5}$ to $\mp 3 \times 10^{-3}$.

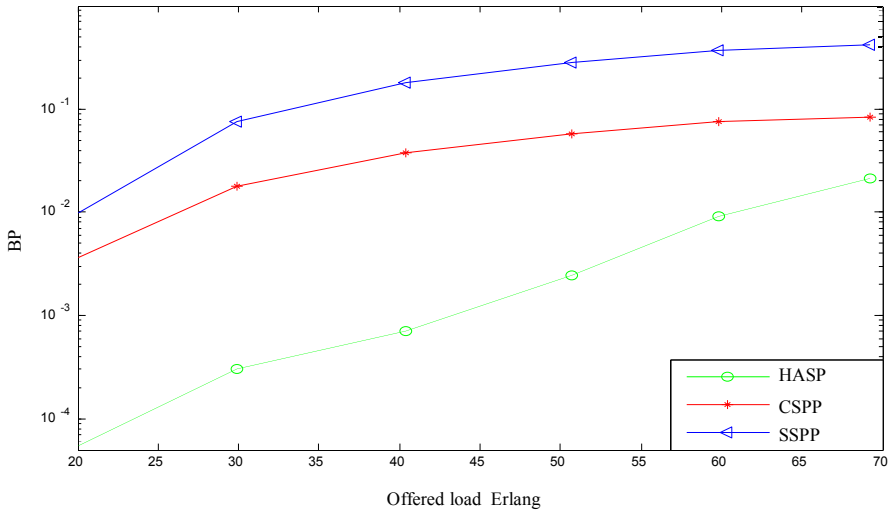


Figure 7.11 The BP performance analysis of the HASP algorithm compared to the standard algorithms over a network with normal failure arrival rate

Figure 7.12 demonstrates 27% lower assigned wavelength per connection on average compared to the other algorithms. Figure 7.13 shows a 15% higher availability satisfaction rate on average than the SSPP and 5% higher than the CSPP algorithms. The numerical comparisons have been computed for the offered load of 40 Erlangs. The graphs in Figure 7.12 have an error ranging from ∓ 0.12 to ∓ 0.20 wavelengths. Similarly in Figure 7.13, the graphs have an error ranging from $\mp 6 \times 10^{-4}$ to $\mp 2.9 \times 10^{-3}$. For the arrival rate of β=40 in the HASP mechanism, the 95% confidence interval of the HASP

mechanism's results in Figure 7.13 is [98.94% 99.06%] which translates to a 0.06% relative error.

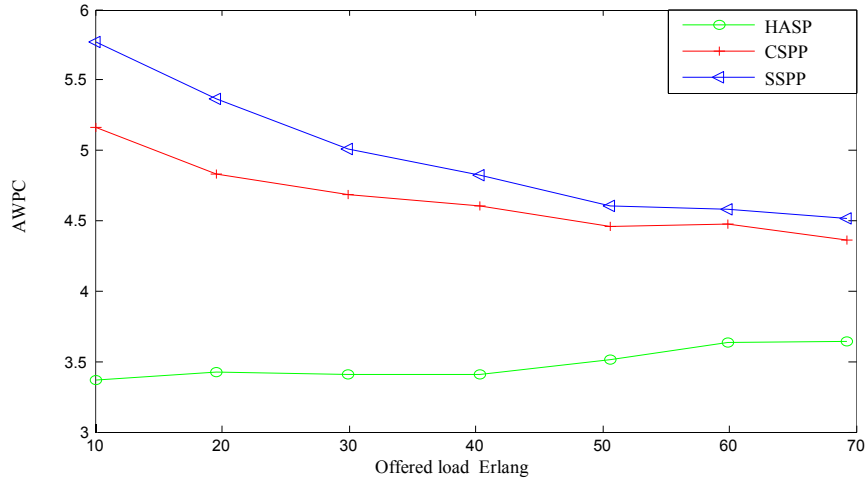


Figure 7.12 The AWPC performance analysis of the HASP algorithm compared to the standard algorithms over a network with normal failure arrival rate

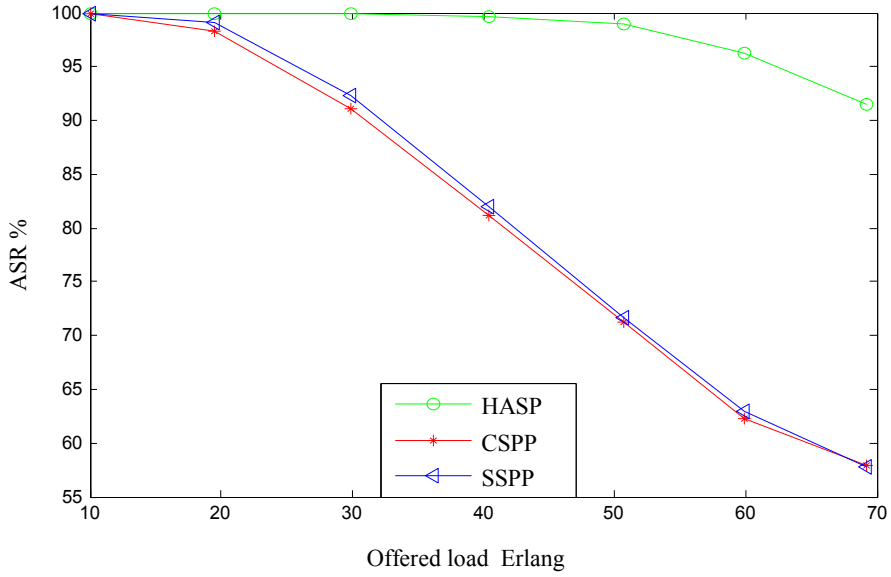


Figure 7.13 The ASR performance analysis of the HASP algorithm compared to the standard algorithms over a network with normal failure arrival rate

This part of the simulation verifies that the HASP algorithm is suitable for networks with low link failure rate. Clearly, since the SSPP algorithm does not consider the availability as a constraint in path calculation, we do not expect to see much difference in the BP and ASR in the second part of the evaluation compared to the first part.

7.7.4 Revenue analysis

The last step of the evaluation process of the HASP mechanism investigates how much more revenue the new mechanism brings to the ISP than the SSPP [11] and [12], and the existing SLA-aware [23] algorithms when a high risk network (see Chapter 2) is considered. The values for calculating revenue for different classes of traffic is based on the facts presented in [63] and the revenue is calculated based on the net revenue formula, Equation 7.11, presented in [63]. As mentioned in [63], the net revenue R for an ISP is defined for n connections in Equation 7.11, where C_i is the service fee charged per month by an ISP, T_i is the holding time in months for connection i, P_i is monthly penalty for an ISP when the SLA of connection i is violated, and n is total number of provisioned connections. As discussed in detail in [31], it is assumed that the failures follow a memory-less independent process, and the SLA violation rate is averaged over hundred thousands of trials. Therefore, SLA violation ratio which is calculated as a fraction of SLA violations over total trails is a good estimate of the SLA violation risk [31].

$$R = \begin{cases} \sum_{i=1}^{n} C_i \times T_i - \sum_{i=1}^{n} P_i \times T_i & \text{SLA violated} \\ \sum_{i=1}^{n} C_i \times T_i & \text{SLA not violated} \end{cases} \qquad 7.11$$

The values for C_i and P_i have been selected based on the description of service levels and the table providing the cost per month and penalty per month of various levels of the services in [63]. As discussed in [63], the cost and the penalty for Gold services are twice as much as the cost and the penalty for Silver services.

The revenue of an ISP relies on the amount of service time that the ISP provides to the customer. The cumulative service time of different classes of traffic has been demonstrated in Figure 7.14 in which the HASP mechanism has a longer cumulative offered service time for high-priority connections than the other algorithms. However, the difference in cumulative service time of the HASP for Silver requests compared to the other algorithms is marginal. Figure 7.14 (a) clearly shows that the HASP mechanism

spends more time serving high-priority requests than low priority ones. Consequently, the ISPs using the HASP mechanism can earn more money by simply serving more high-priority connection requests than those using the other algorithms. As shown in Figure 7.14 (b), the HASP mechanism does not degrade the service time of the low-priority requests.

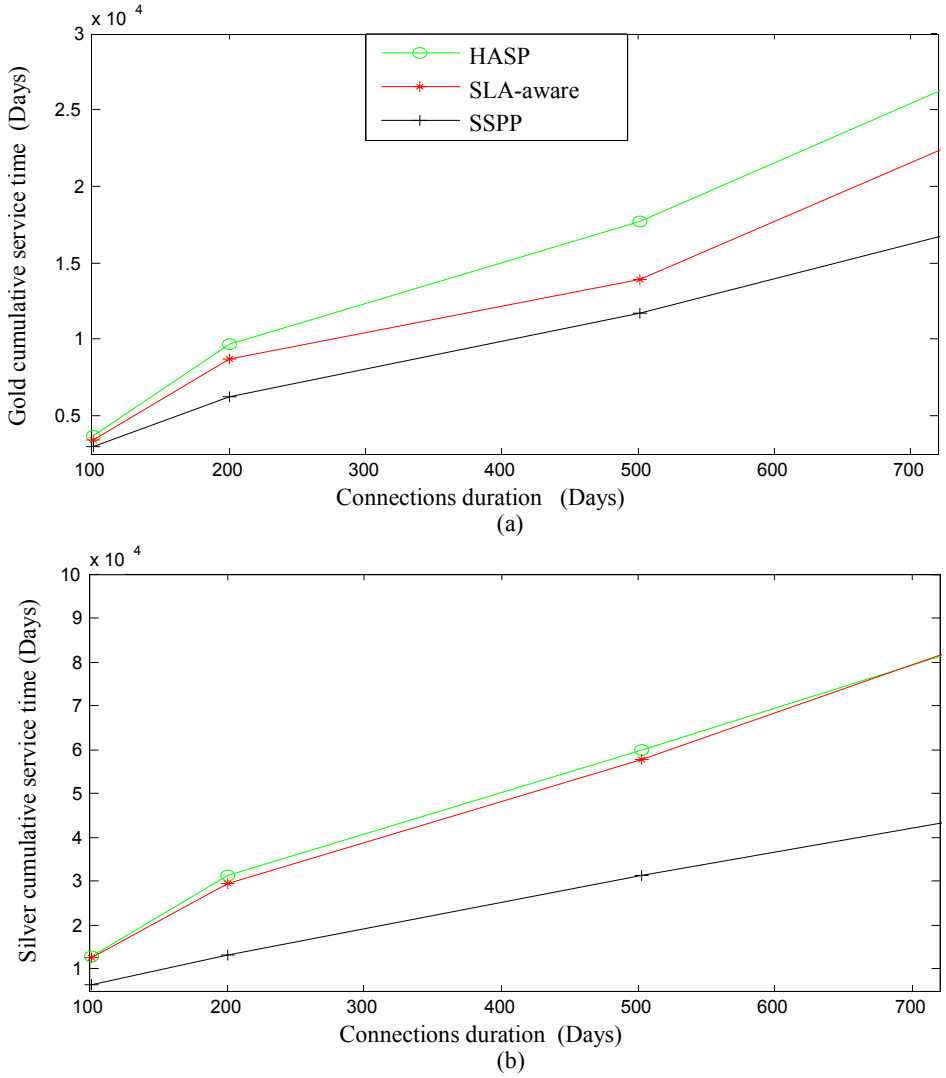


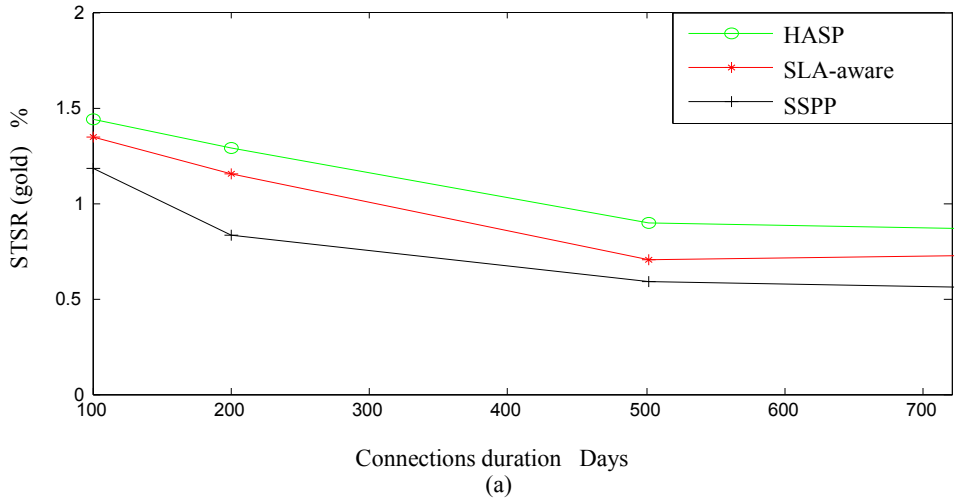
Figure 7.14 The cumulative service time evaluation for Gold and Silver connections over different mechanisms

Definition: Service time satisfaction ratio (STSR)

The STSR of each class of traffic denotes the percentage ratio of the cumulative service time offered by ISP to the total committed service time. The total committed service time includes all connections including blocked and established.

Since the blocking probability over large values of offered loads is low (as shown in Figure 7.7), the STSR values are expected to be low over large values of offered loads. Figure 7.15 shows 20% and 40% increase in service time satisfaction ratio of the HASP mechanism compared to the SLA-aware and SSPP algorithms, respectively. The graphs in Figure 7.15 have an error ranging $\mp 0.06\%$. For the connection duration of 400 Days, the 95% confidence interval of the HASP mechanism's results in Figure 7.15 is [0.94% 1.06%] which translates to a 6% relative error.

This part of the simulation was done on the network shown in Figure 7.3 to evaluate the providers' revenue over a risky network. As shown in Figure 7.16, the HASP algorithm brings 33% more revenue to the ISP than the standard scheme, SSPP algorithm [11] and [12], and about 10% more than the SLA-aware algorithm [23].



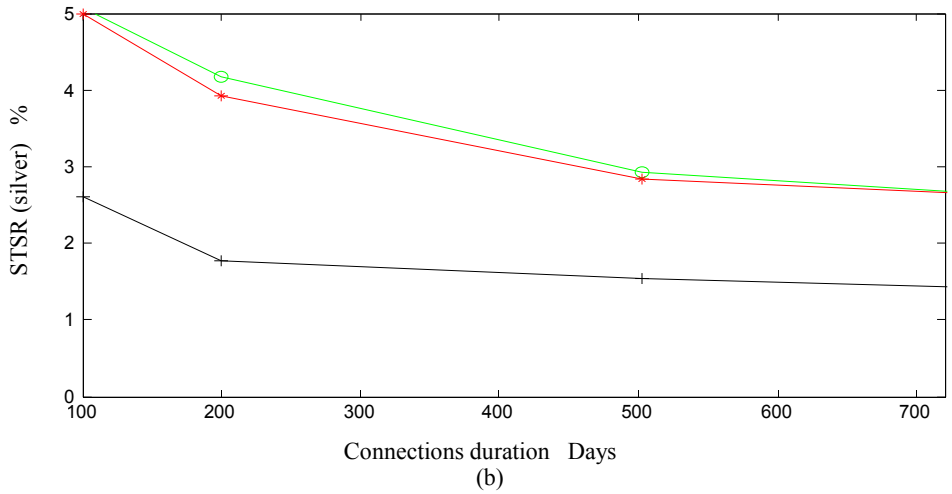


Figure 7.15 The service time satisfaction rate evaluation for Gold and Silver connections over different mechanisms

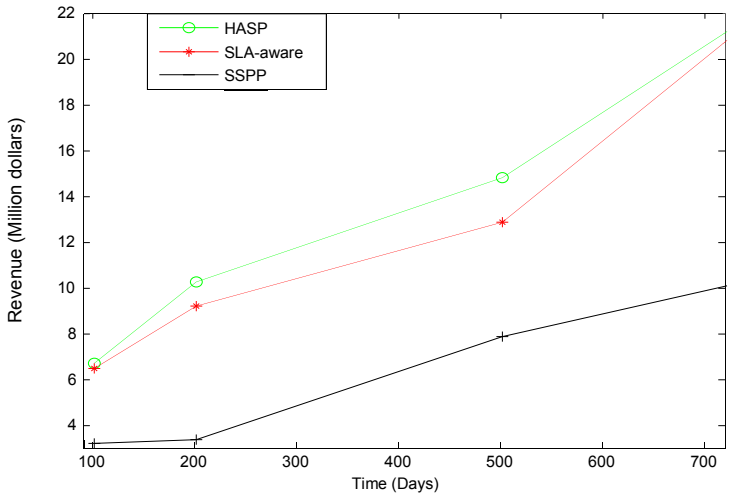


Figure 7.16 Revenue evaluation earned by an ISP over different mechanisms

7.8 SUMMARY

In this chapter a dynamic provisioning mechanism has been presented through which service providers can exploit the unused allowable down time of the connections to serve additional requests. The algorithm has benefited from two factors of a connection request: the holding time, and the failure arrival rate. The mechanism illustrated in this chapter has routed the requests in such a way that any SLA violation is either avoided or minimized. To achieve this goal, the already established paths were flagged with a novel path metric to indicate their risk tolerance of SLA violation. The proposed history-aware mechanism has incorporated a unique path attribute and a novel cost function into a routing algorithm. The cost function considers the number of wavelengths, the failure arrival rate of the connections, and an SLA violation risk as the main factors.

Two different simulation environments have been developed to evaluate the performance of the networks with high link failure arrival rate and low link failure arrival rate. Simulation results have verified that the proposed mechanism has better network performance over both simulation environments. The algorithm has also provided higher revenue for service providers compared to the standard and existing SLA-aware algorithms. It has been shown that the proposed mechanism satisfies the two main objectives of a service provider, higher revenue with minimized SLA violations.

CHAPTER 8 CONCLUSION AND FUTURE WORK

This chapter summarizes the contributions presented in previous chapters and presents future work topics related to the dissertation. The work presented in this thesis has looked for novel SLA based infrastructure and mechanisms, proper traffic engineering path/link attributes, and suitable algorithms for priority-aware shared mesh optical networks. The goal has been to have an infrastructure for negotiating desirable SLA parameters and path attributes to better serve high-priority connection requests over shared mesh WDM networks.

8.1 MAIN CONTRIBUTIONS

The first contribution proposed in Chapter 3 has presented a dynamic SLA negotiation mechanism for shared mesh optical networks. Both intra and inter domain communications have been considered to disseminate the proposed TE extensions using OSPF and BGP protocols. Link attributes as SLA parameters are negotiated via intra-domain mechanism, and any new proposed SLA-based TE path attributes can be advertised through inter-domain negotiation mechanism. The contribution has shown how SLA negotiation protocols together with the proposed TE metric can improve the performance of different protection schemes or algorithms. Since the proposed mechanism in this contribution disseminating link/path attributes can cause heavy control overheads in a dynamic environment, an alternative means of communication has been employed to reduce the overheads and resolve the possible scalability issues. The network performance has been evaluated from two different and important points of view: the control overhead reduction employing an existing method, and the performance improvement using the proposed mechanism. Performance analysis has shown that the proposed mechanism can be easily scalable using a path state advertisement concept. It has also verified that the proposed scheme has a better availability satisfaction ratio performance while it has never degraded the blocking probability. In addition, the

introduced mechanism has not applied more overhead in terms of the total number of allocated wavelengths than standard algorithms.

The second contribution presented in Chapter 4 has tested the mutual and bidirectional negotiating communications process between customers and service providers based on the SLA parameters. This contribution has employed a dynamic priority-aware provisioning mechanism by which customers and service providers can negotiate some vital SLA parameters before actually placing the order and establishing the requests. The proposed algorithm has looked for a remedy for high-priority requests that could not be accommodated as they have violated the initial availability offered by the network. A path constraint considering the initial status of the network in terms of the path availabilities was presented. This parameter has represented the maximum initial capacity of the network for accommodating upcoming connection requests. By employing the path constraint, the requests issued by customers which have been beyond the initial capacity of the network could be modified to comply with the network initial conditions.

The third contribution presented in Chapter 5 can be summarized in three parts. In the first part, a novel TE path metric has been introduced. An algorithm has been proposed to calculate and dynamically update the proposed path constraint. Two algorithms which have taken advantage of the proposed metric have been introduced in the second part of the contribution to improve the network performance for static and dynamic traffic. Employing the proposed path constraint, the proposed algorithms have improved the performance of high-priority connection requests by reducing the blocking probability, increasing availability satisfaction rate, better preserving high-priority connection requests, and reducing the average number of allocated wavelengths per connection.

The forth contribution presented in Chapter 6 has discussed an adaptive provisioning SLA-aware algorithm over shared mesh survivable WDM networks. The proposed mechanism has consisted of two parts: i) A novel provisioning algorithm to buffer and further process the potentially blocked high-priority connection requests, and ii) A new time-aware path constraint to benefit from availability and holding-time as two crucial SLA connection parameters. The proposed algorithm has been developed to better serve a

large number of high-priority connection requests with fairly long durations. To achieve this goal, a novel TE path constraint has been introduced. The proposed path constraint benefits from two important SLA connection parameters, requested availability and holding time. This metric has helped the provisioning algorithm to buffer the potentially blocked high-priority requests and serve them in a timed manner rather than blocking them. Simulation results have shown that the proposed mechanism has reduced the blocking probability of the high-priority requests, increased availability satisfaction rate, better accommodated high-priority connection requests, reduced the average number of allocated wavelengths per connection, and decreased resource overbuild compared to conventional and existing SLA-aware algorithms.

The last contribution of the thesis presented in Chapter 7 has introduced a dynamic provisioning mechanism through which service providers have exploited the unused allowable down time of the connections to serve additional requests. The algorithm has benefited from two factors of a connection request: the holding time, and the failure arrival rate. The mechanism illustrated in this contribution has routed the requests in a way that any SLA violation is either avoided or minimized. To achieve this goal, the already established paths were flagged with a novel path metric proposed there to show their risk tolerance to SLA violation. The proposed mechanism has kept track of a specific attribute of the paths as the paths history to refresh and update its history of the paths' attribute. The proposed mechanism has incorporated a unique path attribute and a novel cost function into a routing algorithm. A cost function has been defined which considers the lower cost factors such as the number of wavelengths and the failure arrival rate of the connections, and an SLA violation risk factor. Two different simulation environments were considered to evaluate the performance of the high risk and low risk networks with high link failure arrival rate and low link failure arrival rate respectively. Simulation results have verified that the proposed mechanism has better network performance over both simulation environments. The algorithm has also provided higher revenue for service providers compared to the standard and existing SLA-aware algorithms over high risk networks. Based on the simulation results, it has been shown

that this part of the research satisfies two main objectives of a service provider, higher revenue with minimal SLA violations.

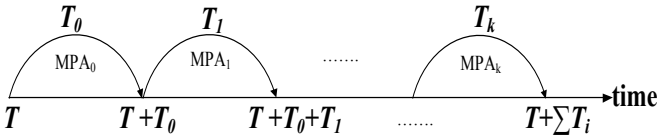
8.2 FUTURE WORK

A couple of issues which are left as future research possibilities are noted below.

Partial protection consideration:
By employing partial protection, the backup resource allocation can be better optimized. To achieve this goal, the level of protection can be considered for any established connection. Protection level of a connection is defined as the percentage of the working bandwidth to be restorable by the protection path of the connection once the working path is interrupted regardless of the location of the failure pattern [46]. In all simulation environments for all contributions, the level of protection has been considered 100%. That is, all the suggested values offered by the negotiating center are based on the fact that the level of the protection has been considered 100%. However, it can affect the performance of the network and sharing process if it varies, and it can be a possibility for future research. The level of protection has been defined in Chapter 2.

Guaranteed maximum path availability (GMPA) employment:
A number of path attributes including TMPA which is time-aware metric have been introduced in this dissertation. Another version of time-aware path attribute can be defined so that it introduces MPA together with the period of time during which the offered MPA is guaranteed by the service provider. Calling it guaranteed maximum path availability (GMPA), GMPA can be the best offer from the ISP which will be valid for a specific period of time, T. Service providers can run an auction and sell their resources for a certain and limited period of time.

$GMPA = [(MPA_{sd}, T_{sd})]$



Floating maximum path availability (FMPA) employment:

Throughout this dissertation, it has been assumed that the availability request of a connection is not changed during the connection holding time. However, sometimes customers prefer to change their SLA contract parameters without breaking the connections. It may happen regarding changes on the class of traffic that customers transfer. That is, a connection is established for a preliminary availability; over the holding time of the connection the availability request changes. That might help to release some backup paths or to choose other backup paths with different characteristics. In fact, the MPA of a specific source and destination pair can have different values, MPA^1 and MPA^2, for different period of time, T_1 and T_2, during the connection holding time.

$$FMPA_{sd} = [(MPA_{sd}^1, T_1, MPA_{sd}^2, T_2)]$$

Variable time to repair assumption:

In Chapter 7, it has been considered that the MTTR of the links belonging to an ISP could be a constant value. However, analyzing more realistic and complicated cases requires the algorithms to consider variable time to repair rather than a fixed value. Considering variable time to repair requires the SLA violation risk formulas to be changed in a way to support the addition of another variable. Prior to this change, the SLA violation risk probability is calculated based on the failure arrival rate.

BIBLIOGRAPHY

[1] A. Mellouk, Ed., *End to end quality of service engineering in next generation hetrogenous networks*.: John Wiley, 2009.

[2] H. El-Sayed, A. Mellouk, L. George, and S. Zeadally, "Quality of service models for heterogeneous networks: overview and challenges," *Annals of Telecommunications*, vol. 63, pp. 639-668, 2008.

[3] W. Zhou, L. Liu, and J. Song, "Challenges for End-to-End Quality of Service in Heterogeneous Networks," in *Computer Science and Information Engineering*, 2009, pp. 389 - 393.

[4] A. Farrel and I. Bryskin, *GMPLS architecture and applications*.: Morgan Kaufmann, 2006.

[5] S. Blake et al., "An Architecture for Differentiated Services," IETF, RFC 2475, 1998.

[6] D. Grossman, "New Terminology and Clarifications for Diffserv," IETF, RFC 3260, 2002.

[7] W. Fawaz, B. Daheb, O. Audouin, M. Du-Pond, and G. Pujolle, "Service level agreement and provisioning in optical networks," *IEEE Communications Magazine*, vol. 42, no. 1, pp. 36 - 43, 2004.

[8] D. Katz, K. Kompella, and D. Yeung, "Traffic Engineering (TE) Extensions to OSPF Version 2," IETF RFC 3630, 2003.

[9] L. Berger, I. Bryskin, A. Zinin, and R. Coltun, "The OSPF Opaque LSA Option," IETF, RFC 5250, 2008.

[10] K. Kompella and Y. Rekhter, "OSPF Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS)," IETF RFC 4203, 2005.

[11] J. Lang, B. Rajagopalan, and D. Papadimitriou, "GMPLS recovery functional specification," IETF RFC 4426, 2006.

[12] E. Mannie and D. Papadimitriou, "Recovery (Protection and Restoration)

Terminology for GMPLS," IETF RFC 4427, 2006.

[13] H. Ould-Brahim, D. Fedyk, and Y. Rekhter, "BGP Traffic Engineering Attribute," IETF RFC 5543, 2009.

[14] A. Manolova, S. Ruepp, J. Buron, and L. Dittmann, "On the Efficiency of BGP-TE Extensions for GMPLS Multi-Domain Routing," in *international conference on Optical Network Design and Modeling, ONDM*, 2009, pp. 1-6.

[15] Y. Yin and G. Kuo, "An Improved OSPF-TE in GMPLS-Based Optical Networks," in *Workshop on High Performance Switching and Routing*, 2005, pp. 241-245.

[16] X. Wang and H. Schulzrinne, "RNAP: a Resource Negotiation and Pricing Protocol," in *International Workshop Network and Optical System*, 1999, pp. 77-93.

[17] Tequila Consortium. (2001, Oct.) SrNP: Service Negotiation Protocol. [Online]. http://www.ist-tequila.org/deliverables

[18] T.M.T Nguyen, N. Boukhatem, Y.G. Doudane, and G. Pujolle, "COPS-SLS: a service level negotiation protocol for the Internet," *IEEE communication magazine*, vol. 40, no. 5, pp. 158 - 165, 2002.

[19] Ambient Networks Consortium, "Connecting Ambient Networks - Architecture and Protocol Design," WWI Ambient Networks, 2005.

[20] V. Sarangan and J.C. Chen, "Comparative Study of Protocols for Dynamic Service Negotiation in the Next-Generation Internet," *IEEE Communications Magazine*, vol. 44, no. 3, pp. 151-156, 2006.

[21] W. Fawaz, T. Sawah, and C. Rjeily, "Priority-aware optical shared protection: An offline evaluation study," *journal of computer applications*, vol. 32, pp. 1677-1684, 2009.

[22] W. Fawaz, K. Chen, and G. Pujolle, "Priority-enabled optical shared protection: An online efficiency evaluation study," *journal computer applications*, vol. 30, pp. 3690-3697, 2007.

[23] R. He, B. Lin, and L. Li, "Dynamic service-level-agreement aware shared-path

protection in WDM mesh networks," *journal of computer application*, vol. 30, pp. 429-444, 2007.

[24] R. Lin and L. Li, "A New Network Availability Algorithm for WDM Optical Networks," in *5th International Conference on Computer and Information Technology*, 2005, pp. 480 – 484.

[25] M. Tornatore, C. Ou, J. Zhang, A. Pattavina, and B. Mukherjee, "Efficient shared-path protection exploiting the knowledge of connection-holding time," in *Optical networks design and modeling*, 2005, pp. 65-72.

[26] M. Tornatore, D. Lucerna, L. Song, B. Mukherjee, and A. Pattavina, "Dynamic SLA Redefinition for Shared-Path-Protected Connections with Known Duration," in *National Fiber Optics Engineers*, 2008.

[27] L. Song, J. Zhang, and B. Mukherjee, "Dynamic provisioning with reliability guarantee and resource optimization for differentiated services in WDM mesh networks," in *Optical fiber communication conference*, vol. 3, 2005.

[28] M. Xia, C.U. Martel, L. Shi, M. Tornatore, and B. Mukherjee, "A Novel SLA for Time-Differentiated Resilience with Efficient Resource Sharing in WDM Networks," in *IEEE ICC*, 2010, pp. 1-5.

[29] X. Wei, L. Guo, X. Wang, Q. Song, and L. Li, "Availability guarantee in survivable WDM mesh networks: A time perspective," *Journal of information science*, vol. 178, no. 11, pp. 2406-2415, 2008.

[30] O. Gerstel and G. Sasaki, "Meeting SLAs by Design: a Protection Scheme with Memory," in *Conference on Optical Fiber Communication and the National Fiber Optic Engineers Conference, OFC/NFOEC*, 2007, pp. -13.

[31] M. Xia, M. Tornatore, C.U. Martel, and B. Mukherjee, "Risk-Aware Provisioning for Optical WDM Mesh Networks," *IEEE/ACM Transactions on Networking*, pp. 1-11, December 2010.

[32] J.H. Sarker and H.T. Mouftah, "Service reliability with enhanced failure recovery rate for multiple failures in survivable optical networks," in *24th Biennial Symposium on Communications*, 2008 , pp. 88-92.

[33] R. Clemente, M. Bartoli, M.C. Bossi, G. D'Orazio, and G. Cosmo, "Risk management in availability SLA," in *5th International Workshop on Design of Reliable Communication Networks, DRCN*, 2005, pp. 411-418.

[34] J. Zhang, K. Zhu, H. Zang, N. Matloff, and B. Mukherjee, "Availability-aware provisioning strategies for differentiated protection services in wavelength-convertible WDM mesh networks," *IEEE ACM transactions on networking*, vol. 15, no. 5, pp. 1177-1190, 2007.

[35] J. Zhang, K. Zhu, and B. Mukherjee, "A New Provisioning Framework to Provide Availability-Guaranteed Service in WDM Mesh Networks," in *IEEE International Conference on Communications*, 2003, pp. 1484–1488.

[36] S. Chen and K. Nahrstedt, "An Overview of Quality-of-Service Routing for the Next Generation High-Speed Networks: Problems and Solutions," *IEEE Network*, 1998.

[37] Z. Wang and J. Crowcroft, "Quality-of-service routing for supporting multimedia applications," *IEEE Journal on Selected Areas in Communications*, vol. 14, no. 7, pp. 1228 - 1234 , 1996.

[38] F.A. Kuipers and P.F.A. Van Mieghem, "Conditions That Impact the Complexity of QoS Routing," *IEEE/ACM TRANSACTIONS ON NETWORKING*, vol. 13, no. 4, pp. 717-730, 2005.

[39] H. Zang, J.P. Jue, and B. Mukherjee, "A Review of routing and wavelength assignment approaches for wavelength-routed optical WDM networks," in *Optical Networks*, 2000, pp. 47-60.

[40] Y. Sun, J. Gu, and D.H.K. Tsang, "Routing and Wavelength Assignment in All-Optical Networks with Multihop Connections," *International Journal of Electronics and Communications*, vol. 55, no. 1, pp. 10-17, 2001.

[41] A. Farrel and I. Bryskin, *GMPLS Architecture and Applications*.: Morgan Kaufmann, 2006.

[42] M. Chen, R. Zhang, and X. Duan, "OSPF Extensions in Support of Inter-Autonomous System (AS) MPLS and GMPLS Traffic Engineering," IETF RFC

5392, 2009.

[43] Y. Rekhter, T. Li, and S. Hares, "A Border Gateway Protocol 4 (BGP-4)," IETF RFC 4271, 2006.

[44] A. Nafarieh, B. Robertson, W. Phillips, and S. Sivakumar, "Dynamic SLA Negotiation Mechanism in Support of Priority-aware Algorithms in Shared Mesh Optical Networks," in *ICINC*, 2010.

[45] J. Segovia, E. Calle, and P. Vila, "Availability analysis of GMPLS connections based on physical network topology," in *ONDM*, 2008, pp. 1-6.

[46] Q. Guo, P. Ho, A. Haque, and H. Mouftah, "Availability-constrained shared backup path protection (SBPP) for GMPLS based spare capacity reprovisioning," in *IEEE International Conference on ICC07*, 2007.

[47] T.H. Cormen, C.E. Leiserson, R.L. Rivest, and C. Stein, *Introduction to Algorithms*, 3rd ed.: MIT Press, 2009.

[48] A. Nafarieh, W. Phillips, B. Robertson, and S.C. Sivakumar, "Statically Pre-provisioned Priority-aware Algorithm for Shared-Mesh Optical Networks," in *International Conference on Transparent Optical Networks, ICTON*, 2010, pp. 1-4.

[49] T.M.T Nguyen, N Boukhatem, Y.G Doudane, and G Pujolle, "A service level negotiation protocol for the internet," in *IEEE Comminication Magazine*, 2002, pp. 158-165.

[50] L Green, V Mirchandani, I Gergol, and D Verchere, "Design of a dynamic SLA negotiation protocol for grids," in *GridNets*, 2007.

[51] E.W Dijkstra, "A note on two problems in connection with graphs," *Numeriche Mathematik*, vol. 1, pp. 269-271, 1959.

[52] J. Yen, "Finding k shortest loopless paths in a network," *Management science*, vol. 17, pp. 712-716, 1971.

[53] A. Nafarieh, S. Sivakumar, W. Phillips, and B. Robertson, "Dynamically provisioned priority-aware algorithms in shared mesh optical networks," in *Int. ICST Conf. on Heterogeneous Networking for Quality, Reliability, Security and*

Robustness, QShine, 2010.

[54] M. Tornatore, C. Ou, J. Zhang, A. Pattavina, and B. Mukherjee, "PHOTO: an efficient shared-path protection strategy based on connection-holding-time awareness," *Journal of Lightwave Technology*, vol. 23, pp. 3138-3146, 2005.

[55] L. Song and B. Mukherjee, "New approaches for dynamic routing with availability guarantee for differentiated services in survivable mesh networks: the roles of primary-backup link sharing and multiple backup paths," in *GLOBECOM*, 2006, pp. 1-5.

[56] D. Papadimitriou et al., "Shared Risk Link Groups Inference and Processing," IETF, Internet Draft 02, 2003.

[57] E. Oki, N. Matsuura, K. Shiomoto, and N. Yamanaka, "A disjoint path selection scheme with shared risk link groups in GMPLS networks," *IEEE communication letters*, vol. 6, no. 9, pp. 406-408, 2002.

[58] E. Oki, N. Matsuura, K. Shiomoto, and N. Yamanaka, "A disjoint path selection scheme with SRLG in GMPLS networks," in *Workshop on High Performance Switching and Routing Merging Optical and IP Technologies.* , 2002, pp. 88-92.

[59] N. Yamanaka, K. Shiomoto, and E. Oki, *GMPLS technologies: broadband backbone networks and systems*.: CRC press, 2006.

[60] F. Zhang, D. Li, O.G Dios, and C. Margaria, "RSVP-TE Extensions for Configuration SRLG of an FA," IETF, Standards Track 03, 2011.

[61] A. Nafarieh, S.C. Sivakumar, Bill Robertson, and William Phillips, "Asaptive Sla-aware re-provisioning mechanism for long duration shared mesh protected connections," in *ICIIN*, 2011.

[62] L. Guo, H. Yu, and L. Li, "Joint routing-selection algorithm for a shared path with differentiated reliability in survivable wavelength-division-multiplexing mesh networks," *Optics Express*, vol. 12, no. 11, pp. 2327-2337, 2004.

[63] M. Xia, M. Batayneh, L. Song, C.U Martel, and B. Mukherjee, "SLA-Aware Provisioning for Revenue Maximization in Telecom Mesh Networks," in *GLOBECOM*, 2008, pp. 1-5.

[64] M. Xia, L. Song, M. Batayneh, and B. Mukherjee, "Event-Triggered Reprovisioning with Resource Preemption in WDM Mesh Networks: A Traffic Engineering Approach," in *Optical Fiber Communication Conference (OFC)*, 2008, pp. 1-3.

[65] N. Bouabdallah and B. Sericola, "Introducing a Relative Priority for the Shared-Protection Schemes ," *IEEE Transactions on Dependable and Secure Computing*, vol. 4, no. 3, pp. 205 - 215 , 2007.

[66] R. Bhandari, *Survivable networks:algorithms for diverse routing*.: Kluwer academic publishers, 1999.

[67] A. Nafarieh, S.C. Sivakumar, B. Robertson, and W. Phillips, "Memory-aware SLA-based mechanism for shared mesh WDM networks," in *International congress on ultra modern telecommunications and control systems*, 2011.

[68] R. Mandeville, "Benchmarking Terminology for LAN Switching Devices," IETF RFC 2285, 1998.

[69] P. Lenkiewicz, M. Hajduczenia, M.M. Freire, H.J.A. da Silva, and P.P. Monteiro, "Estimating Network Offered Load for Optical Burst," in *Networking*, vol. 3976, 2006, pp. 1062-1073.

[70] A. Leon Garcia and I. Widjaja, *Communication Networks Fundamental Concepts and Key Architectures*.: Mc Graw Hill, 2004.

[71] G. Fenton, "Mathematics for internetworking," Dalhousie University, Course Notes 2006.

[72] E. R. Dougherty, *probability and statistics for the engineering, computing, and physical sciences*.: Prentice Hall, 1990.

APPENDIX A DEFINITIONS

A.1 OFFERED LOAD

The network offered load is defined as the ratio between the total network traffic load and the network capacity, as indicated by the following equation in which L_i is the amount of traffic generated by a single user i (out of n) in a unit of time, and C_j is the capacity of a single link j (out of m) in the network [68].

$$L_{offered} = \frac{\sum_{i=1}^{n} L_i}{\sum_{j=1}^{m} C_j} \quad [68]$$

It should be noted that, according to this definition, the offered network load can be greater than 1, since users might generate more traffic than the maximum that the network structure can relay [69].

A.2 ERLANG

Erlang is used in telephony and network as a statistical measure of offered load or carried load on service providers. Erlang is a dimensionless unit to measure traffic intensity or as called in this thesis offered load. One Erlang is the offered load that would occupy a single trunk 100% of the time. Offered traffic (in Erlangs) is related to the traffic arrival rate, λ, and the average traffic-holding time, h, by the following equation provided that h and λ are expressed using the same units of time [70].

$$E = \lambda \times h$$

A.3 CONFIDENCE INTERVAL ON A PROPORTION

Considering a sample of n observations of a Bernoulli trial, the proportion of "success" in the sample is given by the following equation in which N_n is the number of successes in n trials. The estimator $\hat{p}$ is an estimate of the true probability of p [71].

$$\hat{p} = \frac{N_n}{n}$$

The standard deviation of the estimate is

$$\sigma_{\hat{p}} = \sqrt{\frac{p(1-p)}{n}}$$

If the n is considered large enough, the distribution of N_n can be approximated by a normal distribution. Therefore, the (1-α) confidence interval of the p is calculated by the following formula in which $Z_{\frac{\alpha}{2}} = 1.96$ for 95% confidence interval which has been considered in this thesis.

$$[L, U] = \hat{p} \mp Z_{\frac{\alpha}{2}}\sigma_{\hat{p}} = \hat{p} \mp Z_{\frac{\alpha}{2}}\sqrt{\frac{\hat{p}(1-\hat{p})}{n}} \qquad [71]$$

The thorough discussion in this regard has been provided through [72].