İSTANBUL TECHNICAL UNIVERSITY ★ INSTITUTE OF SCIENCE AND TECHNOLOGY

CLASS BASED AVAILABILITY CONSIDERATIONS IN GMPLS NETWORKS

M.Sc. Thesis by
Adnan SANCAK

Department : Computer Engineering

Programme : Computer Engineering

JUNE 2010

İSTANBUL TECHNICAL UNIVERSITY ★ INSTITUTE OF SCIENCE AND TECHNOLOGY

CLASS BASED AVAILABILITY CONSIDERATIONS IN GMPLS NETWORKS

M.Sc. Thesis by
Adnan SANCAK
(504071501)

Date of submission : 07 May 2010
Date of defence examination: 07 June 2010

Supervisor (Chairman) : Prof. Dr. Sema OKTUĞ (ITU)
Members of the Examining Committee : Prof. Dr. Osman PALAMUTÇUOĞULLARI (ITU)
Assis. Prof. Dr. Ayşegül Gençata YAYIMLI (ITU)

JUNE 2010

İSTANBUL TEKNİK ÜNİVERSİTESİ ★ FEN BİLİMLERİ ENSTİTÜSÜ

GMPLS AGLARINDA SINIF BAZLI SÜRDÜRÜLEBİLİRLİK DEGERLENDİRMELERİ

YÜKSEK LİSANS TEZİ
Adnan SANCAK
(504071501)

Tezin Enstitüye Verildiği Tarih :	**07 Mayis 2010**
Tezin Savunulduğu Tarih :	**07 Haziran 2010**

Tez Danışmanı :	**Prof. Dr. Sema OKTUĞ (İTÜ)**
Diğer Jüri Üyeleri :	**Prof. Dr. Osman PALAMUTÇUOĞULLARI (İTÜ)** **Yrd. Doç. Dr. Ayşegül Gençata YAYIMLI (İTÜ)**

HAZİRAN 2010

FOREWORD

I would like to thank my supervisor Prof. Sema Oktuğ for her helpful comments, suggestions, improvements, and corrections to my master thesis.

I would also like to thank Dr. Burak Kantarcı for his support, supervision and for spending his precious time to evaluate my thesis across the sea in Canada.

I would like to thank Arcelik A.Ş. IT Department members in Sütlüce especially to my manager Zafer Kaya, my dear colleagues Murat Gökalp, Sibel Öktem, Hatice Ergör and all other IT Department members for their patience and support during my masters education.

The last but not least, I would like to express my deep appreciation for my family for their endless support.

This work is supported by TUBITAK (The Scientific and Technological Research Council of Turkey).

May 2010

Adnan SANCAK

Computer Engineer

TABLE OF CONTENTS

ABBREVIATIONS

BP	**:** Backup Path
CWS	**:** Computation While Switching
DPP	**:** Dedicated Path Protection
FAR	**:** Failure-Aware Routing
FDR	**:** Failure-Driver Routing
FIR	**:** Failure-Independent Routing
GMPLS	**:** Generalized Multi Protocol Label Switching
GSRO	**:** Gateway Specification Routing Object
ILP	**:** Integer Linear Programming
ISP	**:** Internet Service Provider
LDP	**:** Label Distribution Protocol
LP	**:** Linear Programming
LSP	**:** Light Switched Path
MPLS	**:** Multi Protocol Label Switching
MTBF	**:** Mean Time between Failures
MTTF	**:** Mean Time to Failure
MTTR	**:** Mean Time to Repair
OSPF	**:** Open Shortest Path First
OTN	**:** Optical Transport Network
PCE	**:** Path Computing Element
PLI	**:** Physical Layer Impairment
QoS	**:** Quality of Service
RSVP-TE	**:** Resource Reservation Protocol - Traffic Engineering
RWA	**:** Routing and Wavelength Assignment
SCA	**:** Spare Capacity Allocation
SLA	**:** Service Level Agreement
SPP	**:** Shared Path Protection
SSR	**:** Successive Survivable Routing
SRLG	**:** Shared Risk List Group
WP	**:** Working Path

LIST OF TABLES

LIST OF FIGURES

Page

CLASS BASED AVAILABILITY CONSIDERATIONS IN GMPLS NETWORKS

SUMMARY

Extended use of MPLS technology in transport networks which improves routing performance introduced some more sophisticated requirements like Advanced Network Management, Quality of Service (QoS) and Resource Optimization. Generalized Multiprotocol Label Switching (GMPLS) architecture mostly meet these requirements however, connection and network availability needs to be considered. In this thesis, we propose a new survivable connection provisioning scheme based on Spare Capacity Allocation (SCA) to maximize resource utilization while guaranteeing availability requirement defined in Service Level Agreement (SLA). We also present two additional class-based heuristic methods, namely Least Reliable Path (LRP) and Exchange Method (EM) in order to minimize blocking probability of incoming connection requests. We compare the performance of the optimization-based model and the proposed heuristics by simulation. The simulation results show that the LRP method leads to the least blocking probability while the SCA-based connection provisioning and the EM demonstrates the same blocking probability level. Furthermore, it is also shown that the heuristics do not introduce additional resource overbuild to the network when compared to the SCA-based model for different load levels.

GMPLS AĞLARINDA SINIF BAZLI SÜRDÜRÜLEBİLİRLİK DEĞERLENDİRMELERİ

ÖZET

Yönlendirme performansını iyileştiren MPLS teknolojisinin ulaştırma ağlarında giderek artan kullanımı beraberinde detaylı ağ yönetimi, Servis Kalitesi (SK) ve Kaynak Kullanım Optimizasyonu gibi daha ileri seviye isteklerin oluşmasına yol açtı. Generalized Multiprotocol Label Switching (GMPLS) mimarisi çoğunlukla bu istekleri karşılarken, ağ ve bağlantı sürdürülebilirliği halen hesaba katılmak zorundadır. Bu çalışmada, Yedek Kaynak Ataması (YKA) algoritmasına dayanan, kaynakların verimli kullanımını ve Servis Kalite Anlaşmlarında (SKA) belirlenen sürdürülebilirlik seviyesini garanti eden yeni bir bağlantı oluşturma şeması tasarlanmıştır. Ayrıca, bağlantı rededilme olasılığını düşürmek için En Az Yeterli Yol (EAYY) ve Değiştirme Metodu (DM) isminde iki adet sınıf bazlı sezgisel yöntem önerilmiştir. Önerilen optimizasyon tabanlı model ve sezgisel yöntemlerin performansları karşılaştırılmıştır. Simulasyon sonuçları göstermiştir ki EAYY yöntemi en düşük bağlantı rededilme olasılığını sağlamaktayken YKA tabanlı bağlantı oluşturma yönetim ve DM yöntemi birbirine benzer bağlantı rededilme değerleri üretmişlerdir. Ayrıca, sezgisel yöntemlerin YKA tabanlı model ile çeşitle ağ trafik seviyelerinde karşılaştırıldıklarında fazladan kaynak kullanımına yol açmadıkları da gösterilmiştir.

1. INTRODUCTION

The increasing use of *Multi Protocol Label Switching (MPLS)* technology in transport networks exposed new challenges to satisfy sophisticated needs [1]. One of these complex problems is to minimize resource cost of the network while meeting availability requirements. Nowadays, 100 Mbit links are assigned to customers for home usage only. It is also important to carry out requests from different classes and maintaining *Quality of Service (QoS)* agreements. By centralizing network management and separating data and control flow, *Generalized Multiprotocol Label Switching (GMPLS)* architecture is very suitable to accomplish such complex tasks. *Internet Service Providers (ISPs)* can now handle connection requests according to their *Service Level Agreements (SLAs)* which hold information about availability requirements of the connection among other things. However, considering failures which happen simultaneously in real world, availability or reliability schemes should take the Backup Resource Allocation Problem into account and also prioritize connections according their SLAs while recovering them.

There are two main protection techniques in *Optical Transport Networks (OTN)* and GMPLS Networks. One of them is restoration, which requires reserving backup resources in case failures occur [2]. *Dedicated Path Protection (DPP)* is 1:1 method, where there is one dedicated Protection Path for the Working Path. Since DPP results into a lot of resource consumption, a more efficient way to protect main Path is *Shared Path Protection (SPP).* In this schema, while the impact of failures to connections is taken account, backup paths are shared to minimize residual capacity. The connections are grouped according to their failure dependencies namely *Shared Risk List Groups (SRLG).* Considering the sharing scenario, it is important to make assumptions related to what proportion of bandwidth of working path should be restored or which paths should have priority when restoration happens.

Another protection technique called P-Cycle is proposed by W. D Grover [3]. This technique is based on creating a spanning cycle in network topology and thus creating a two-way protection for every. While the links on the cycle (Cycle Span) have one protection path on the cycle, the links that are not on the cycle (Straddling Links) will have two protection paths.

One of the realistic proposals about limiting backup resource is called partial restoration [4]. In this method, every single connection has a protection level θ, which shows the proportion of bandwidth to be restored when a fatal failure happens. If the θ value is 100%, then it becomes the old SPP schema. When $\theta < 1$, since not all of the connections could be saved, source end drops the connection. It is important to state that protecting a path is very costly, thus, partial restoration is very suitable for the network topologies with limited bandwidth.

Almost every study for Backup Resource Utilization in Transport Networks covers the network-planning process and simulation & numeric results are given for planning part. In most of the researches regarding availability in OTNs or GMPLS Networks, maximum double-link failures are considered. We know that the probability value drops dramatically considering scenarios with more than two link failures [5]. However, there are still researches targeting multiple link situations.

In this thesis, we will propose a new path protection scheme that automates currently used network infrastructure in order to minimize backup resource usage using *Spare Capacity Allocation (SCA)* method with an Availability guarantee acknowledged by SLA of the connections. We also define two additional heuristic methods to reduce Blocking Probability of incoming connection requests according to their SLA classes. The thesis continues as follows:

- Chapter 2 clarifies basic concepts about Availability in high capacity computer networks.
- Chapter 3 gives detailed information about Availability on GMPLS Networks and mentions previous work on that topic.
- Chapter 4 presents basic concepts and mathematical information about proposed connection allocation mechanism. The essential concepts about SCA and the detailed information about additional heuristics are also given in this chapter.

- Chapter 5 shows the implementation of simulation environmenton which proposed algorithms are tested. The numerical and simulation results are also presented in this chapter.
- Finally, the thesis is concluded in Chapter 6.

2. BASIC AVAILABILITY CONCEPTS IN HIGH CAPACITY NETWORKS

The reliability of complicated systems can be calculated using reliability theory [6] by assigning a failure rate to every functional block of the whole system. In high capacity computer networks, the basic system is characterized as an end-to-end connection, where in OTNs it becomes an end-to-end optical connection. The failure rate of an optical connection can be defined as a function of time namely z*(t).*

According to reliability theory, the reliability of a system is described as

$$R(t) = \Pr\{T > t\} = \int_{t}^{\infty} f(x) \cdot dx \qquad \textbf{(2.1)}$$

where *f(x)* is the probability density function and *t* is the system functionality duration starting from zero [4]. Solving this equation for continuous systems with a constant failure rate z*(t)* = λ we get the equation (2.2):

$$R(t) = e^{-\lambda x} \qquad \textbf{(2.2)}$$

As a result, the *Mean Time to Failure (MTTF)* of the system becomes simply 1/λ [7]. The mean time spent in a system in order to correct a failure is defined as *Mean Time to Repair (MTTR)*. The *Mean Time between Failures (MTBF)* is calculated by equation (2.3):

$$MTBF = MTTF + MTTR \qquad \textbf{(2.3)}$$

Moreover, applying these calculations to the system, namely an optical connection in our case, we can calculate the availability of the system by equation (2.4):

$$A = \frac{MTTF}{MTTF + MTTR} = \frac{MTTF}{MTBF} \qquad \textbf{(2.4)}$$

Since an end-to-end optical connection consists of multiple links or multiple wavelengths, the availability of an optical connection can be defined as in equation (2.5):

$$A_c = \prod_{\forall\, l_i \in c} A_{l_i} \tag{2.5}$$

where l_i is a network link on which connection c operates.

There are several protection mechanisms used in optical networks in order to achieve high availability. The most widely known and used techniques are listed below.

2.1 Dedicated Path Protection (DPP)

In DPP, the path of connection starting from source node to destination node, named *Working Path (WP),* is protected with a link-disjoint path to the WP, named *Backup Path (BP).* This method is also described as “1:1” or “1+1” in literature, showing that same amount of resources are dedicated and allocated to BP protect the WP. Thus, this method is considered to a very expensive way to protect an OTN connection, because the network resources are used inefficiently.

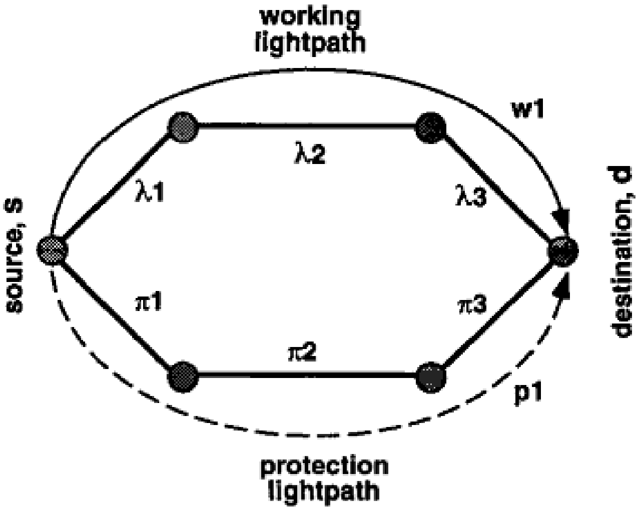


Figure 2.1 : The 1:1 dedicated path protection [2]

The figure 2.1 [2] shows an example of dedicated path protection where *w1* is the WP of connection from source *s* to destination *d* using links *λ1*, *λ2*, and *λ3*. The BP of the connection is *p1*, which consists of the links *π1*, *π2*, and *π3*. In this case, the availability of this connection can be calculated with equation (2.6):

$$A_c = A_{w1} + A_{p1} - A_{w1} \cdot A_{p1} \tag{2.6}$$

The dedicated path protection technique can also be applied to a group of connections. This scenario is called “1:N” protection, stating that N connections are protected by a single BP. It is also possible to protect a WP with multiple BPs. This scenario is named “M:1” protection, where M is the number of protection path. Another alternative is protecting multiple WPs with multiple BPs, which is called “M:N” protection. These three dedicated protection techniques are illustrated in figure 2.2 [2]:

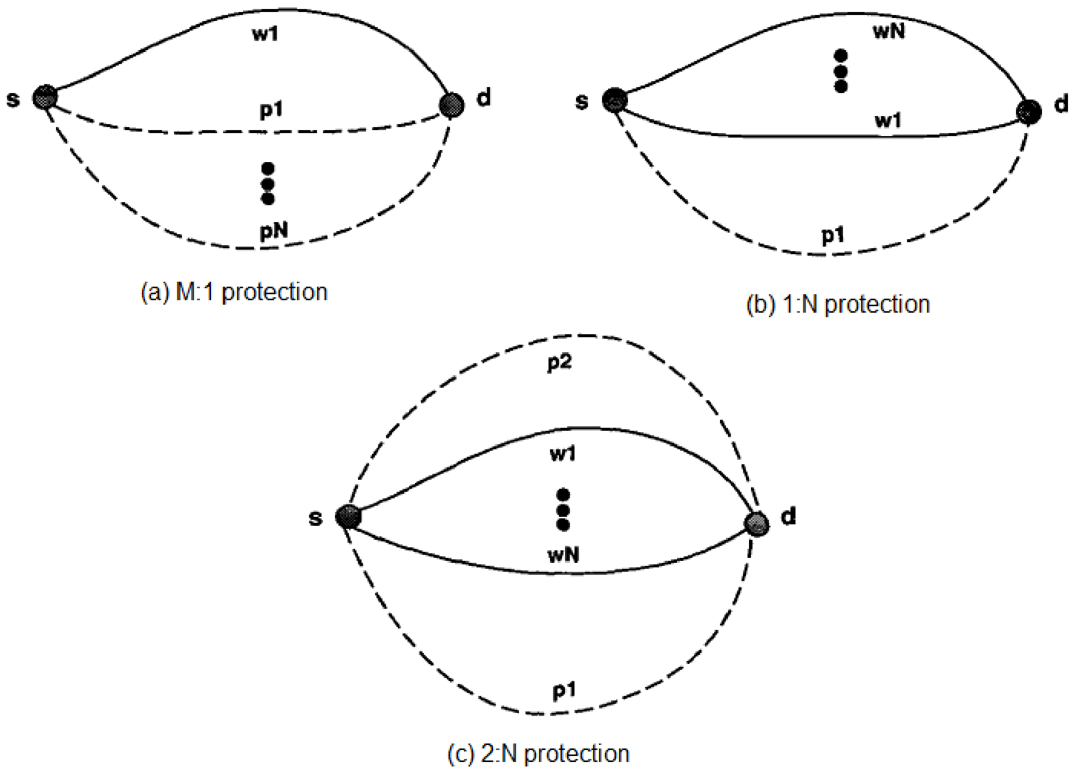


Figure 2.2 : Various dedicated path protection schemas [2]

2.2 Shared Path Protection (SPP)

To reduce the redundant resource usage in DPP, a more useful protection technique is presented where the backup resources are being shared among all connections [2]. In this technique, every connection receives an “1:1” dedicated protection. However, the connections with link-disjoint WPs share same BPs to decrease backup resource redundancy in networks. The figure 2.3 shows a SPP example of two connections. The availability of this whole system can be evaluated with equation (2.7):

$$A_s = A_{w1}A_{w2} + A_{w1}(1-A_{w2})A_{p2} + (1-A_{w1})A_{w2}A_{p1} \tag{2.7}$$

Here the availability of the system (A_s) is a sum of three possible states that makes the whole system available. The first state is where the connections with WPs *w1* and *w2* are available. In second state the connection with *w1* is available, but the connection with *w2* works on its BP *p2* as WP is failed. The third state is the exact opposite of second state, where connection with *w2* operates successfly whereas the connection having *w1* runs on its BP *p1* as its WP is failed. Note that, if WPs of both connections fail then the system becomes unavailable since they share the same backup resource on link *π5* and one of the connections becomes completely dead.

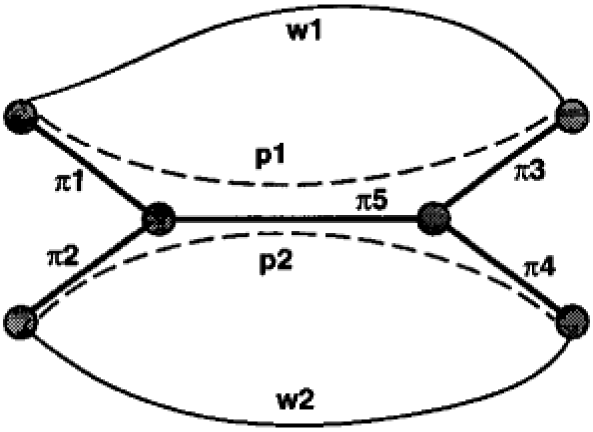


Figure 2.3 : Shared path protection schema for two connection [2]

2.3 Segmented Path Protection

In Segmented Path Protection technique, the main idea is protecting parts of WP with different BPs instead of protection whole WP with one BP [8]. The WP is separated into smaller paths called primary segments and a protection path is assigned to every primary segment of the connection. The figure 2.4 shows an example of end-to-end segmented path protection.

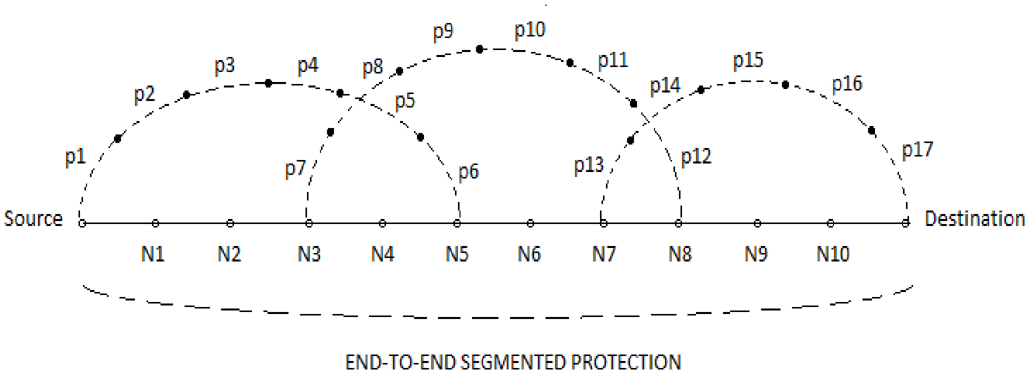


Figure 2.4 : End-to-End Segmented Path Protection.

Here the WP of the connection starts from source, uses nodes *N1-N10* and reaches to the destination. The connection is divided into three primary segments which are (*Source – N5*), (*N3-N8*) and (*N7-Destination*). These three primary segments are protected by three protection paths which are (*p1-p6*), (*p7-p12*) and (*p13-p17*). In case of a failure in first primary segment, the connection would be routed to the first backup segment (*p1-p6*) and then continue with the operational part of the connection (*N5-Destination*). This examples points to one advantage of segmented path protection as the BP does not have to be exactly link-disjoint with WP in order to achieve end-to-end protection in segmented path protection.

2.4 P-Cycle Protection

P-Cycle protection is a cycle-based path protection schema proposed to achieve ring-like restoration speed while optimizing spare capacity assignment [9]. A p-cycle, short for “pre-configured cycle”, creates a complete cycle in network topology. The links within this cycle are called cycle-spans whereas the other links on the topology are called straddling links. When there is link failure on the network, the failure is corrected within the cycle. Looking at the example at figure 2.5 [3], we see a connection established from A to C using links A-B and B-C. The p-cycle of the network consist of the links A-B, B-C, C-D, D-E, and E-A. When one of these links of the connection fails, for example the link B-C, the failure is corrected by the links that complete the cycle in opposite direction.

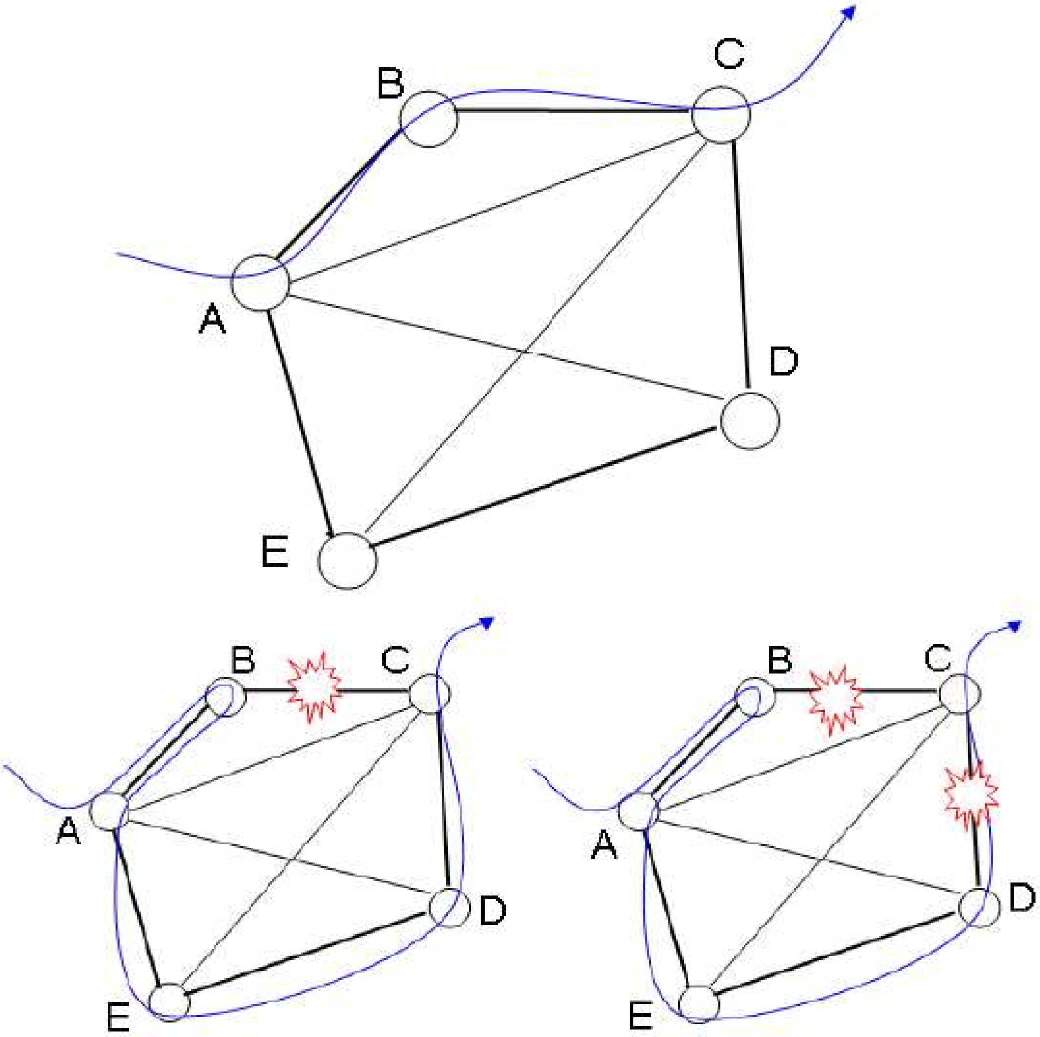


Figure 2.5 : P-Cycle Protection Example [3]

We should note that in p-cycle protection, the connections using cycle-span links endure only single-link failures because on a second failure, the cycle cannot be completed. However, a connection on straddling links is protected against dual link failures. For example, a failure for the connection from E to C using link E-C can be corrected using cycle-span links E-A, A-B, and B-C or using the other cycle-span links E-D and D-C.

3. AVAILABILITY AND GMPLS

3.1 Classification of previous work on Availability in GMPLS Networks

Most of the proposals on availability schemas in GMPLS networks are built on top of the previous approaches for OTNs. GMPLS employs the *Label Distribution Protocol (LDP)* which includes improvements of *Open Shortest Path First (OSPF)* protocol and some advanced implementations of *Resource Reservation Protocol - Traffic Engineering (RSVP-TE)* extensions [10]. Supplying decent, reliable and practical information about nodes, links and connections on the network is very important in order to provide accurate and meaningful results in path allocation problems. Therefore, there are many proposals for LDP implementations in GMPLS networks.

Another vital issue on GMPLS networks is Backup Capacity Allocation Problem. There are many fast and reliable methods proposed to minimize resources while guaranteeing availability. Considering the real life scenarios, allocating minimal redundant resources is the first goal for the ISPs.

The other important topics about availability on GMPLS networks are Dynamic Routing and Inter-Domain Path Protection Schemes.

3.2 Label Distribution Protocol Enhancements in GMPLS Networks

Majority of the OSPF and RSVP proposals use GMPLS signaling in OTNs to improve routing or control channel messaging. Considering our prioritized approach, it is very crucial to declare efficient and availability-aware extensions of LDP in order to have a promising QoS support in the network.

In [11], the authors propose a new protocol improving OSPF in order to reduce bandwidth usage in control messaging. Another objective of this article is to create a reliable messaging protocol by not only distributing link state information but also dispatching wavelength availability information to be used in path allocation process. It is shown that control messaging overhead decreases 3 to 7 times compared to conventional OSPF. Proposed messaging protocol also performs better than period or threshold based protocols when the blocking probability of incoming requests is concerned.

There are also OSPF modifications that focus on improving node activities in GMPLS plane. As a striking example of this [12], the authors add node architecture constraints to their OSPF extension in order to solve inner-node problems when creating new light-paths. By decreasing number of attempts to establish a *Light Switched Path (LSP)* between nodes that are connected through a lot hops, better results are obtained in terms of blocking probability.

Another work [13] aims to make the *Routing and Wavelength Assignment (RWA)* algorithms more efficient by adding special parameters in OSPF messages. Results from the testbed scenarios show that more reasonable and accurate routing is achieved.

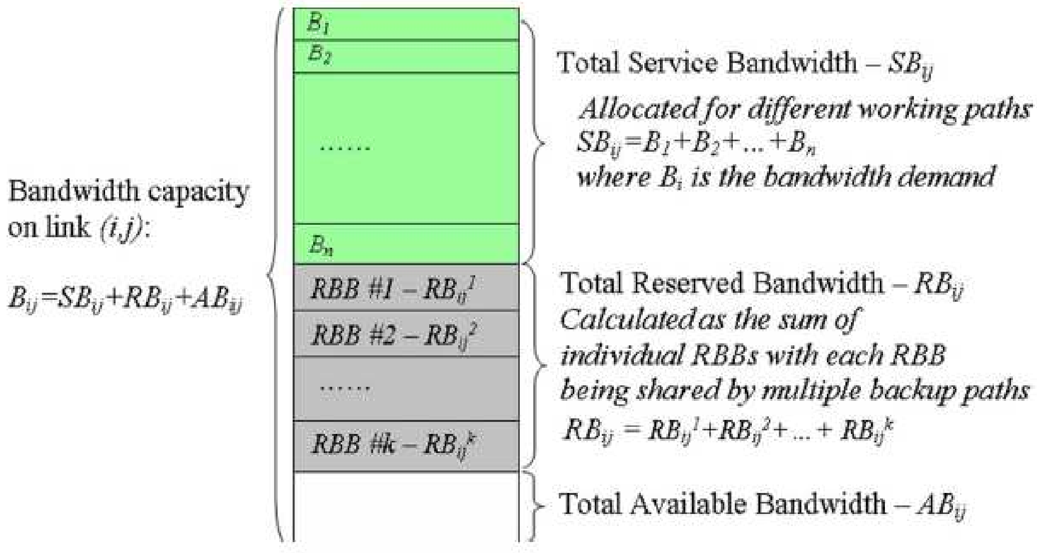
Lastly, there is a traffic extension proposal for OSPF to carry shared mesh restoration in GMPLS networks [14]. Since GMPLS control plane is flexible and powerful enough to transfer connection information in desired granularity, the authors propose to use sharing degree information of BPs so that shared path restoration could be possible. Although there are no reliable methods to transmit routing information in order to minimize control messagging overhead, the proposal showed that shared mesh restoration is possible to implement in GMPLS networks but not available to be used in near future.

3.3 Backup Resource Allocation Problem in GMPLS Networks

Another important topic concerning availability in GMPLS Networks is Spare Capacity Allocation Problem. Protecting every path (connection, light path, etc.) increases redundancy in networks. Therefore, establishing the balance between protection level and resource consumption becomes an important challenge. There are two main perspectives of this problem. The first one focuses on design case of the OTNs. In this case, nodes of the network topology are defined and links are assumed to have unlimited bandwidth. Taking account all possible connection requests, resources are allocated while being constrained by the availability requirements. Afterwards, *Linear Programming (LP)* or *Integer Linear Programming (ILP)* based heuristic algorithms compute the best backup path decisions. As a result, a network topology with optimal resource allocation is calculated. The scope of the second case is the network topologies with limited resources. In this case, connections are requested dynamically and then heuristic algorithms compute best backup path candidates with minimum resource consumption. Unlike the first case, the availability constraints of the connections are more decisive since if there is no extra capacity, connection requests are declined, which results in higher blocking probability.

A recent paper [4], about Spare Capacity Allocation problem suggests Partial Restoration Mechanism. In this method, it is assumed that working paths are constructed from smaller light paths, lambdas … etc. and when a failure occurs, it is possible to restore a proportion of actual bandwidth. Every connection request has an attribute called Protection Level θ, which defines the proportion of the bandwidth to restore. By this way, it is assumed that availability impairment should reduce when multiple link failures occur. A new algorithm called Spare Capacity Reconfiguration is proposed to reorganize backup path resources in every network event occurrence like connection request or topology change.

Another proposal on this area is suggests allocating backup resources as bandwidth blocks [15]. In this work, it is implied that sharing backup resources among similar bandwidth-level groups using SRLG principle would utilize resource consumption. It is also important to state that this method is scalable for large networks and needs minimum change over existing protocols.



B_1
B_2
……
B_n
RBB #1 – RB_{ij}^1
RBB #2 – RB_{ij}^2
……
RBB #k – RB_{ij}^k
Bandwidth capacity on link (i,j):
$B_{ij}=SB_{ij}+RB_{ij}+AB_{ij}$
Total Service Bandwidth – SB_{ij}
Allocated for different working paths
$SB_{ij}=B_1+B_2+...+B_n$
where B_i is the bandwidth demand
Total Reserved Bandwidth – RB_{ij}
Calculated as the sum of individual RBBs with each RBB being shared by multiple backup paths
$RB_{ij} = RB_{ij}^1+RB_{ij}^2+ ... + RB_{ij}^k$
Total Available Bandwidth – AB_{ij}

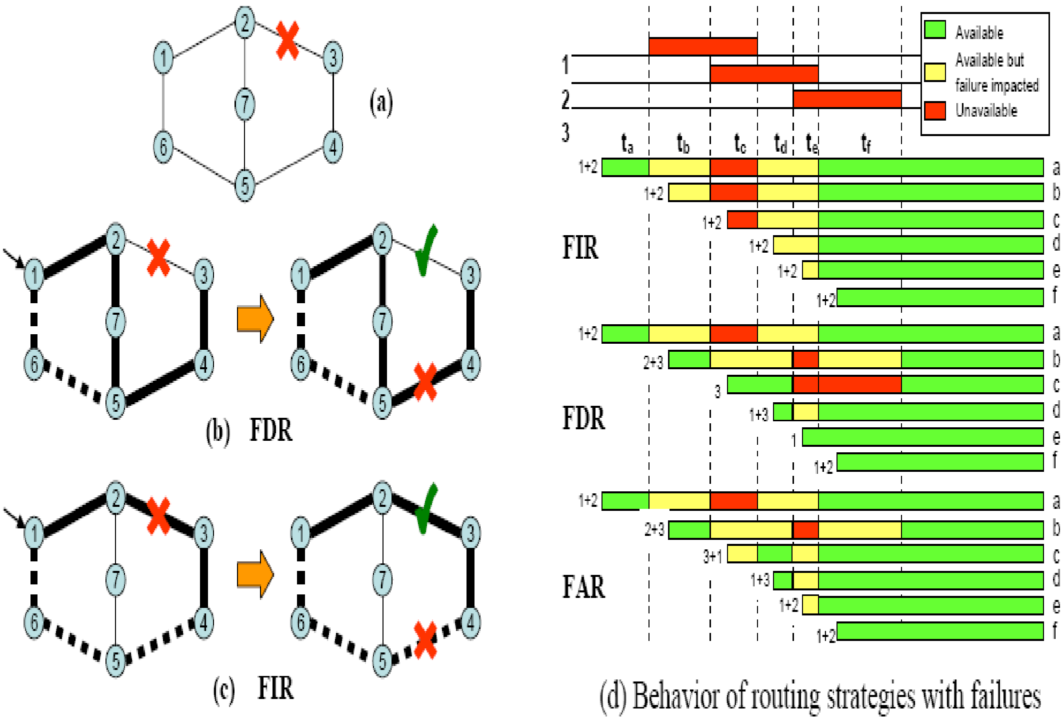
Figure 3.1 : Illustration of Reserved Bandwidth Block Structure in [15]

The figure 3.1 shows the proposed bandwidth block structure where the green area is the primary service bandwidth share, the gray area is backup bandwidth share and the white area is unallocated bandwidth. The backup bandwidth share is partitioned according to the connection request bandwidth requirements and SRLGs are grouped with similar bandwidth requiring connections.

Lastly, using the idea of partial restoration, authors propose a dynamic routing framework structure in GMPLS Networks [16]. An ILP computation mechanism is declared to find the best working and backup path groups while using a cost function to decrease backup path redundancy and meeting availability requirements. It is shown that better blocking probability and low redundancy could be achieved when the proposed connection schema is used.

3.4 Dynamic Routing

The other topic that should be investigated is Dynamic Routing in GMPLS Networks. Dynamic Routing is pointing to special algorithms to update routing information in topology in order to find best working and backup path pairs. As a good example of this, the authors propose a new heuristic named *Failure-Driven Routing (FDR)* by combining advantages of *Failure-Aware routing (FAR)* and *Failure-Independent Routing (FIR)* approaches to achieve better results [17]. The performance of three routing algorithms is given below in figure 3.2 handling three sequential link failures. We could see that failure-driven approach produces better availability in multi-failure scenarios.



(d) Behavior of routing strategies with failures

Figure 3.2 : The performance of FDR, FIR & FAR in [17]

Another work on this area discusses the possibility to carry *Physical Layer Impairment (PLI)* and availability information of wavelength using OSPF and RSVP traffic extensions [18]. It is shown that extending OSPF and RSVP to carry desired information to create impairment aware signalling architecture is possible. It is also shown that the performance output in terms of blocking probability becomes more vital in case a trade-off situation with control messaging overhead.

3.5 Inter-Domain Availability in GMPLS Networks

The last special area concerning availability in GMPLS Networks is availability on multi-GMPLS domains. Up to this part of this thesis, all the papers considered a single GMPLS domain, but in real world there are multiple domains controlled by different ISPs. As a result, there are many connections requesting out-of-domain resources and destination points. The basic solution to this problem is to let specific controllers compute the path inside the domain and choose the best path according to cost comparison afterwards. In one of the example papers [19] of this issue, authors suggested a new method named *Computation While Switching (CWS).* In this method, paths inside domains are computed by *Path Computing Elements (PCE)* and rated with a decisive number to show their quality. The source of the connection chooses the best path and starts sending data, but search for a better path still continues and if a better result is found, the old path is switched to new one.

Another paper [20] proposes using *Gateway Specification Routing Objects (GSRO)* for multi-domain GMPLS network management. GSRO holds information about domain that it resides and the gateway information to neighbor domains and originally proposed for OTNs [21]. Every GSRO is responsible for sending information about its domain to the PCE of next domain when a multi-domain connection is going to be established. By carrying necessary information to PCE of next domain, ILP algorithms could be run in order to decide best path decisions inside the domain in terms of availability and resource consumption.

4. DEFINITIONS OF NEW SCHEME AND HEURISTIC METHODS

4.1 Definition of Proposed Scheme

In this thesis, we aimed to define an automated mechanism to allocate connection requests according to their classes with respect to the availability requirements and backup resource capacity. The Backup Resource Allocation is a very crucial process in servicing requests since the ISP's have to make sure that connections operate without problems in case a network failure occurs. On the other hand, every single assignment for backup resource is to decrease resources for new connection requests. That is why most ISP's tend to minimize residual capacity on their network. Our collection allocation mechanism takes account all the conditions stated above.

In our protection scheme [28], the connection requests can be dropped because of three conditions:

i.) Bandwidth Inefficiency: There are no available resources to allocate WP of the connection.

ii.) Availability Constraint: There is not any suitable path available to meet availability requirements specified by SLA.

iii.) Spare Capacity Constraint: There are no available backup resources on the network when incoming connection request is allocated.

We consider the network topology as *G (V, E),* where *V* is the set of nodes and *E* is the set of links. Each link *j* has a total bandwidth (or wavelength count) of B_j. B_j is represented as

$$B_j = Q_j + V_j + F_j \qquad \textbf{(4.2)}$$

where Q_j, V_j and F_j are working, spare and free capacity on link *j* respectively. Every connection request *c* has defined parameters as $< s_C, d_C, A_C, B_C, \theta_C >$, which are source, destination, availability requirement, bandwidth requirement and protection level respectively.

The WP of the connection, W_C, is calculated with *Successive Survivable Routing (SSR)* Algorithm suggested in [22]. First, the algorithm accepts the shortest path between s_C and d_C, which is calculated by running using Dijkstra Shortest Path Method, as WP. Then *k* more link-disjoint shortest paths are also calculated as BP candidates by excluding the links constructing WP. To choose best BP, the backup cost impact is calculated by multiplying failure-link incidence matrix *(U)* and failure matrix *(F)*. The result is called tabu-link vector *(T)* showing the links that could not be used in backup path. Then, cost is calculated for every backup path that has no tabu-link. The best candidate is chosen as P_C, BP of the connection *c*. The figure 4.1 shows a detailed structure of SSR Algorithm matrices.

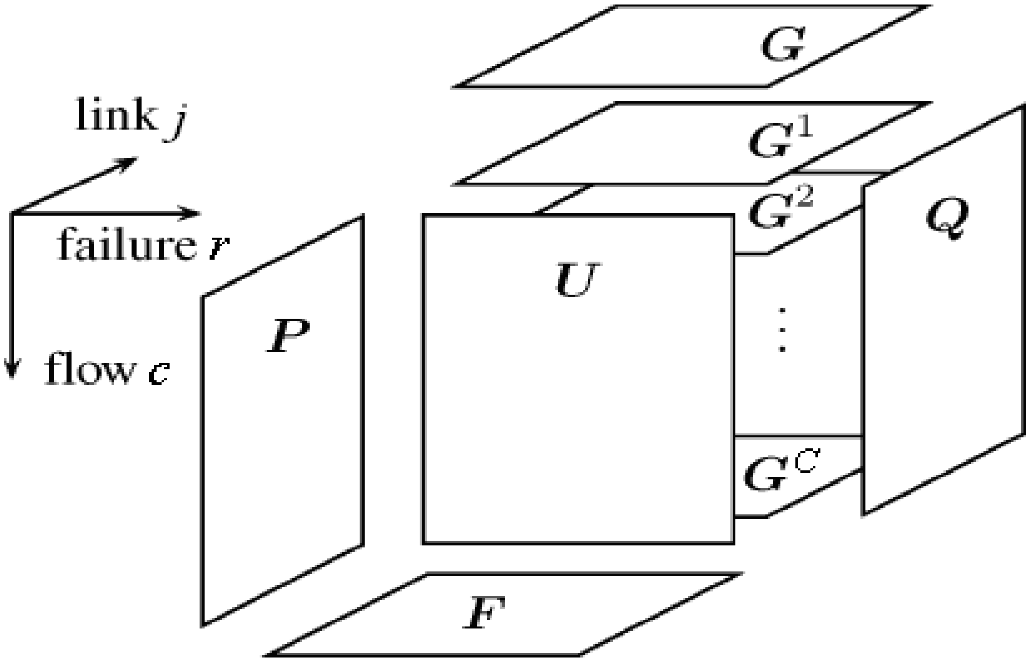


Figure 4.1 : SSR matrix structures in [22].

The set of single and dual link failure combinations is defined as *R* [23]. Every member of this set, π_r is showing the stationary probability of that failure. The set of single and dual failures is classified as described below.

1. R_c^{non} is the set of failures that will make the connection down *c* down in a non-restorable manner.

2. $R_c^{\overline{WP}}$ represents the set of failures that are not a member of R_c^{non} but takes the connection *c* down by affecting both W_C and P_C .

3. $R_c^{\overline{W}\,P}$ is the set of failures whose members hit W_C but does not affect P_C.

4. The last set of failures R_c^{WP} has no effect to the working or backup path of connection *c*.

Considering those sets, the availability of the connection impacted by failures *R* is calculated by:

$$A_c^R = 1 - \sum_{r \in R} \pi_r \tag{4.2}$$

The stationary probabilities are calculated by solving the Markov chain [24] showed in figure 4.2 using equations (4.3)-(4.5).

$$(\lambda_T - \lambda_i + \mu_i)\pi_i = \lambda_i \pi_0 + \sum_{j=1,\, j \neq i}^{E} \frac{\lambda_j + \mu_j}{\mu_i + \mu_j}\pi_i + \frac{\lambda_i + \mu_j}{\mu_i + \mu_j}\pi_j \tag{4.3}$$

$$\pi_0 + \sum_{i=1}^{E} \pi_i + \sum_{i=1}^{E} \sum_{j=1,\, j \neq i}^{E} \frac{\lambda_j}{\mu_i + \mu_j}\pi_i = 1 \tag{4.4}$$

$$\lambda_T = \sum_{i=1}^{E} \lambda_i ,\ \lambda_i = 1/MTTF_i ,\ \mu_i = 1/MTTR_i \tag{4.5}$$

where $MTTF_i$ and $MTTR_i$ shows the Mean Time to Fail and Repair values for each link respectively.

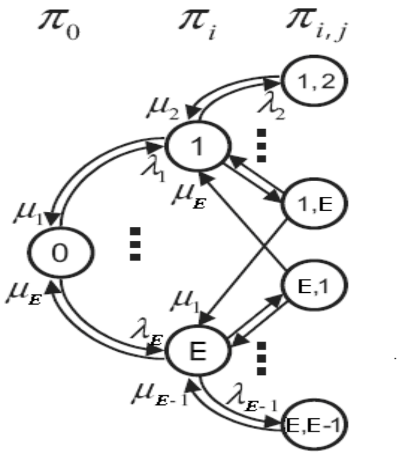


Figure 4.2 : Markov Chain for Failure Probabilities [24]

The spare capacity in each link is calculated Spare Capacity Allocation Method proposed here [4]. The spare capacity at each link is calculated by

$$Minimize\ : \sum_{\forall j \in E} v_j \tag{4.6}$$

$$1 \geq y_{j,r} \geq 0, \forall j \in E, \forall r \in R_c^{\overline{WP}} \tag{4.7}$$

$$y_{j,\{m\}} \geq 1 - \frac{v_j + \sum_{\forall k | \{m\} \in R_k^{\overline{WP}}, j \in P_k} b_k \cdot \theta_k \cdot q_k^{\{m\}}}{\sum_{\forall k | \{m\} \in R_k^{\overline{WP}}, j \in P_k} b_k \cdot \theta_k} \tag{4.8}$$

$$\forall j \in E, \forall \{m, n\} \in \dot{R}_k^{\overline{WP}}$$

$$y_{j,\{n,m\}} \geq 1 - \frac{v'_j + \sum_{\forall k | \{n\} \in R_k^{\overline{WP}}, j \in P_k} b_k \cdot \theta_k \cdot q_k^{\{n,m\}}}{\sum_{\forall k | \{n\} \in R_k^{\overline{WP}}, j \in P_k} b_k \cdot \theta_k} \tag{4.9}$$

$$\forall j \in E, \forall \{n, m\} \in \ddot{R}_k^{\overline{WP}}$$

$$v'_j = v_j - s_{j,\{n\}} \tag{4.10}$$

$$s_{j,r} = \sum_{\forall k | r \in R_k^{\overline{WP}}, j \in P_k} b_k \cdot \theta_k \cdot \left(1 - q_k^r\right) \tag{4.11}$$

$$1 \geq q_c^r \geq y_{j,r}, \forall j \in P_c, c \in C, \forall r \in R_c^{\overline{WP}} \tag{4.12}$$

$$\begin{aligned} u_c &= u_c^{non} + u_c^{\overline{WP}} + \dot{u}_c^{\overline{WP}} + \ddot{u}_c^{\overline{WP}} \\ u_c &= \sum_{\forall r \in R_c^{non}} \pi_r + \sum_{\forall r \in R_c^{\overline{WP}}} \pi_r \\ &+ \sum_{\forall m \in W_c} \left(\left(1 - \theta_c\right) + q_c^{\{m\}}\right) \cdot \sum_{\forall n | \{m, n\} \in \dot{R}_c^{\overline{WP}}} \pi_{\{m,n\}} \\ &+ \sum_{\forall \{n, m\} \in \ddot{R}_c^{\overline{WP}}} \left(\left(1 - \theta_c\right) + q_c^{\{n,m\}} \cdot \theta_c\right) \cdot \pi_{\{n,m\}} \\ &\forall c \in C \end{aligned} \tag{4.13}$$

$$u_c \leq u_c^{SLA}, \forall c \in C \tag{4.14}$$

The goal of this SCA model [4] is to minimize Spare Capacity v_j on each link *j*. A transition variable $y_{j,r}$ is defined to calculate the non-restorable partition of link *j* due to the failure *r*. Equation (4.8) guarantees that there is enough spare capacity to be allocated on the link *j* in case a single link failure *{m}* occurs. If there is a double failure *{n, m}* on the network, first the failure *{n}* is recovered. v_j' shows the rest of the spare capacity left on link *j* and equations (4.9) and (4.10) assures that there is enough spare capacity to recover all the dual link failures. $s_{j,r}$ is the amount of residual bandwidth needed to recover the connections having link *j* on their WP when a failure *r* occurs. The unavailability value of a connection *c* is calculated by equation (4.13) and lastly, equation (4.14) applies SLA availability constraint for each connection on the network.

Using the models described above, the connection allocation algorithm is visualized in figure 4.3. As initiation, the stationary failure probabilities calculated using equation set (4.3) – (4.5). If a connection request event occurs, the bandwidth and availability conditions are checked to decide whether or not to allocate incoming connection request. If the conditions are secured, then according to the value of Network Event Counter (N_C) Spare Capacity Allocation Algorithm is run (by including WP capacity of the incoming request) to get Spare Capacity values for each link *j*. If there is enough f_j on each link to allocate new calculated v_j's, incoming request is accepted and the N_C is reset [28].

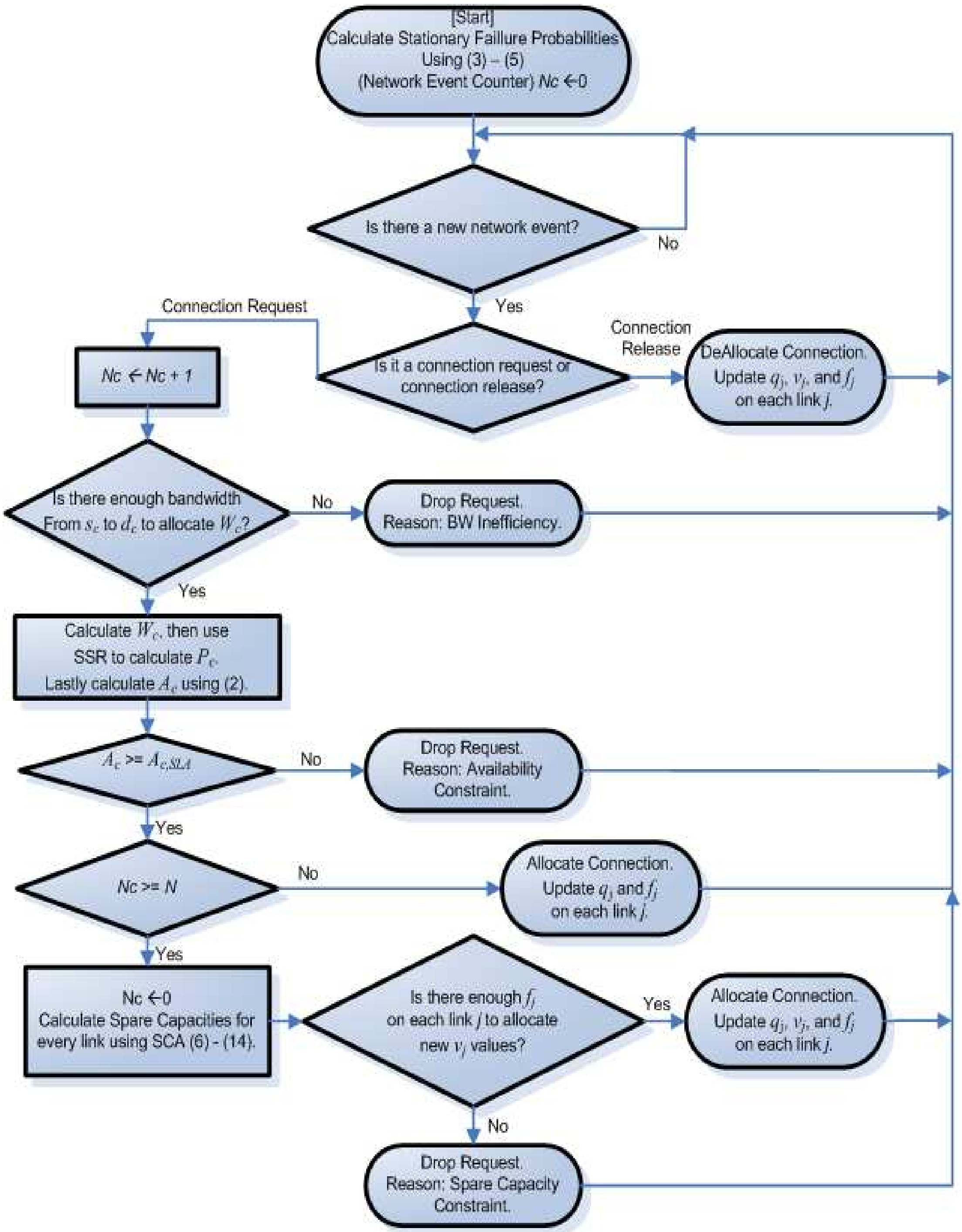

[Start]
Calculate Stationary Failure Probabilities
Using (3) – (5)
(Network Event Counter) $Nc \leftarrow 0$
Is there a new network event?
No
Yes
Connection Request
Is it a connection request or connection release?
Connection Release
DeAllocate Connection.
Update q_j, v_j, and f_j on each link j.
$Nc \leftarrow Nc + 1$
Is there enough bandwidth From s_c to d_c to allocate W_c?
No
Drop Request.
Reason: BW Inefficiency.
Yes
Calculate W_c, then use SSR to calculate P_c.
Lastly calculate A_c using (2).
$A_c >= A_{c,SLA}$
No
Drop Request.
Reason: Availability Constraint.
Yes
$Nc >= N$
No
Allocate Connection.
Update q_j and f_j on each link j.
Yes
$Nc \leftarrow 0$
Calculate Spare Capacities for every link using SCA (6) - (14).
Is there enough f_j on each link j to allocate new v_j values?
Yes
Allocate Connection.
Update q_j, v_j, and f_j on each link j.
No
Drop Request.
Reason: Spare Capacity Constraint.

Figure 4.3 : Proposed Connection Allocation Scheme

The pseudocode of proposed schema is also available in figure A.1 of appendix A.1.

The upper limit value of N_C (N) has an important role in our proposed model. It handles tuning of the algorithm according to the network size and incoming request frequency. Setting N to 1 would make the scheme work in real-time, but the due long response times of SCA Model would also make it an infeasible solution. Likewise, if N is set to a relatively big number, then the spare capacity values on each link would be out of date which would result into situations like allocating redundant capacity or bandwidth problems in recovering network failures.

4.2 Definition of Proposed Heuristics

In the real world, the SLAs of the connection requests are defined in a class-based structure. The requests with high SLA are more important for ISP's due to their high income rates. Therefore, in a path allocation scheme it should be possible to prioritize the connections according to their classes. In this section we define two additional heuristic methods that are working along with our proposed scheme to improve blocking probability of high SLA connections [28].

4.2.1 Heuristic I: Exchange Method.

In this method, if a high SLA level connection request is going to be rejected due to bandwidth inefficiency, the model tries to find a similar connection with lower SLA to drop in order to allocate the higher one. By this way, the high SLA level connections are prioritized when there is a bandwidth bottleneck on the network.

The heuristic is described in figure 4.4 as well as the pseudocode is presened in figure A.2 of appendix A.1. In a situation where a high SLA connection (c_H) is going to be dropped because of bandwidth inefficiency, three exchangeable connection candidates are chosen from current connection set C where s_c and d_c of those connections are same with $s_{C,H}$ and $d_{C,H}$, if possible. The bandwidth of those connections should be also great or equal to the bandwidth of chosen connection, $\mathrm{b}_{\mathrm{C,H}}$. If there are no possible candidates available then c_H is dropped immediately. From those possible three candidates (cc), the one with shortest operating time is chosen to be replaced with c_H. By this way, the connections with longer holding times are protected and the connection with shortest operating time could be served again with least damage done.

The connection allocation procedure continues for c_H where it has stopped. If c_H is going to be dropped in later stages due to some other reasons like availability constraint or spare capacity constraint, then the connection chosen to be exchanged is reallocated [28].

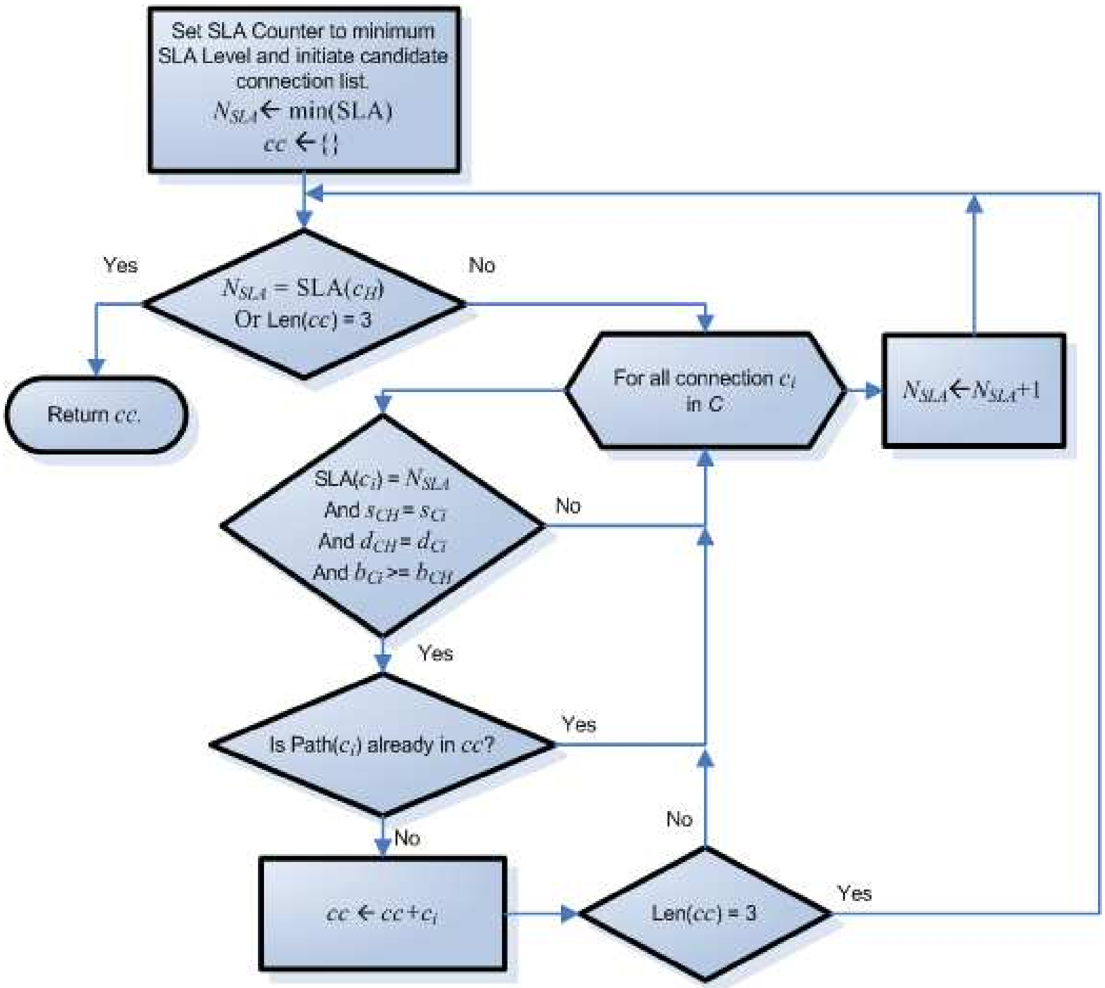

Set SLA Counter to minimum SLA Level and initiate candidate connection list.
$N_{SLA} \leftarrow$ min(SLA)
$cc \leftarrow \{\}$
Yes
No
N_{SLA} = SLA(c_H) Or Len(cc) = 3
Return cc.
For all connection c_i in C
$N_{SLA} \leftarrow N_{SLA}+1$
SLA(c_i) = N_{SLA} And $s_{CH} = s_{Ci}$ And $d_{CH} = d_{Ci}$ And $b_{Ci} >= b_{CH}$
No
Yes
Is Path(c_i) already in cc?
Yes
No
No
$cc \leftarrow cc + c_i$
Len(cc) = 3
Yes

Figure 4.4 : Heuristic I: Exchange Method

4.2.2 Heuristic II: Least Reliable Path(LRP) Method

In regular basis, the proposed schema finds the shortest path using Dijkstra's shortest path Algorithm to be assigned as WP of incoming connection requests. The cost values for the links could be actual costs for using those links or distance values on those links. In this method, we propose using availability values of each link as cost values of Dijkstra Algorithm. By this way, the produced path would be the least reliable path available to meet the request.

In this heuristic method, we calculate the LRP of incoming connection request as $W_{C,LRP}$ alongside with the shortest path from s_c to d_c as $W_{C,SP}$. If $W_{C,LRP}$ is link-wise different than $W_{C,SP}$, then $W_{C,LRP}$ is chosen as WP of the connection request. Otherwise, $W_{C,SP}$ is assigned as WP as usual.

Using this method, we are trying to prevent low SLA connections from using high-available links in their WP or BP's. As a result the connections with high SLA would be allocated using reserved high-available links [28].

5. NUMERICAL RESULTS

5.1 Simulation Environment

In order to verify the accuracy of the proposed connection allocation schema, a simulation software is developed using C# programming language. ILOG CPLEX optimization environment libraries are used to solve LP problem defined in Chapter 3 [25]. Two scenarios are considered in the simulations. In the first scenario, constant number of connections are assumed to be provisioned in advance where random failures are introduced to the network links with the given MTTF and MTTR. The failure arrivals follow a Poisson process with the arrival time of MTTF value. The MTTR value is the mean duration of the re-activation of a link. The simulated value of availability of each connection is calculated as seen in equation (5.1).

$$A_c = 1 - \sum_{\forall r \in R} t_c^r \,/\, t_{total} \qquad \textbf{(5.1)}$$

where t_c^r is the amount of the time the connection c is down and t_{total} is total simulation time. The simulated values are compared with the results that the SCA algorithm [4] produces in order to validate accuracy. The purpose of the first simulation software was to prove that SCA algorithm is implemented correctly.

The second simulation focuses on a more dynamic scenario where the connection requests are created randomly as where as the network failures are also created randomly. In this dynamic simulation environment, the connection requests are created with a random SLA availability constraint from the set {0.99, 0.999, 0.9999, 0.99999}. As in [26], for each link in network topology a predefined availability value A_i from the set {0.999, 0.9999, 0.99999} is assigned randomly and the value for that link is calculated by equation (5.2).

$$MTTF_i = MTTR_i \cdot A_i / (1 - A_i) \qquad \textbf{(5.2)}$$

where $MTTF_i$ and $MTTR_i$ are the MTTF and MTTR values for each link respectively. The computations are done for three different topologies [27]:

i.) A subset of Pan European Network (Figure 5.1)

ii.) USNET Network (Figure 5.2)

iii.) German Network (Figure 5.3)

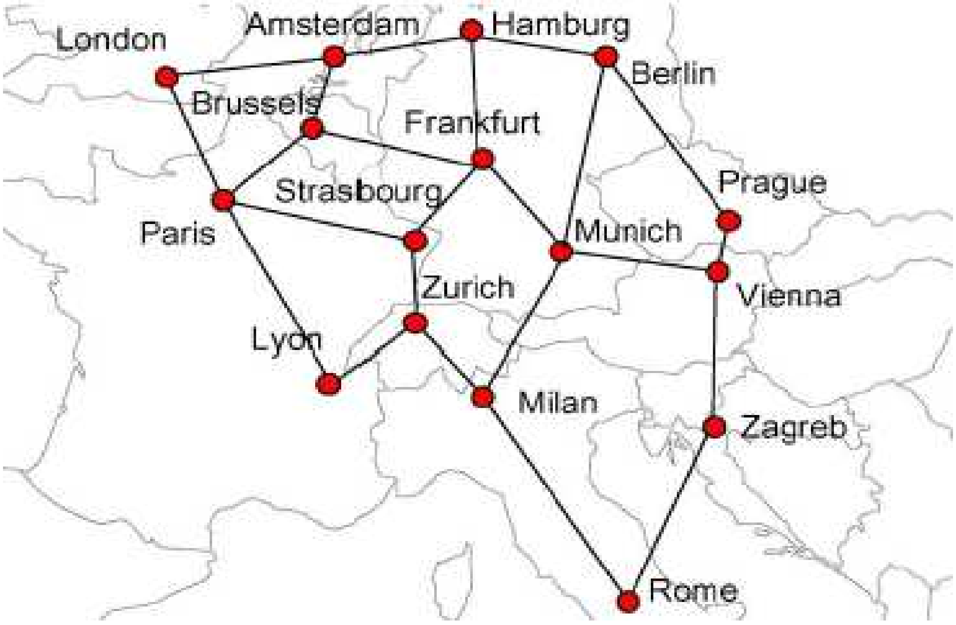


Figure 5.1 : Pan European Network (16 Nodes)

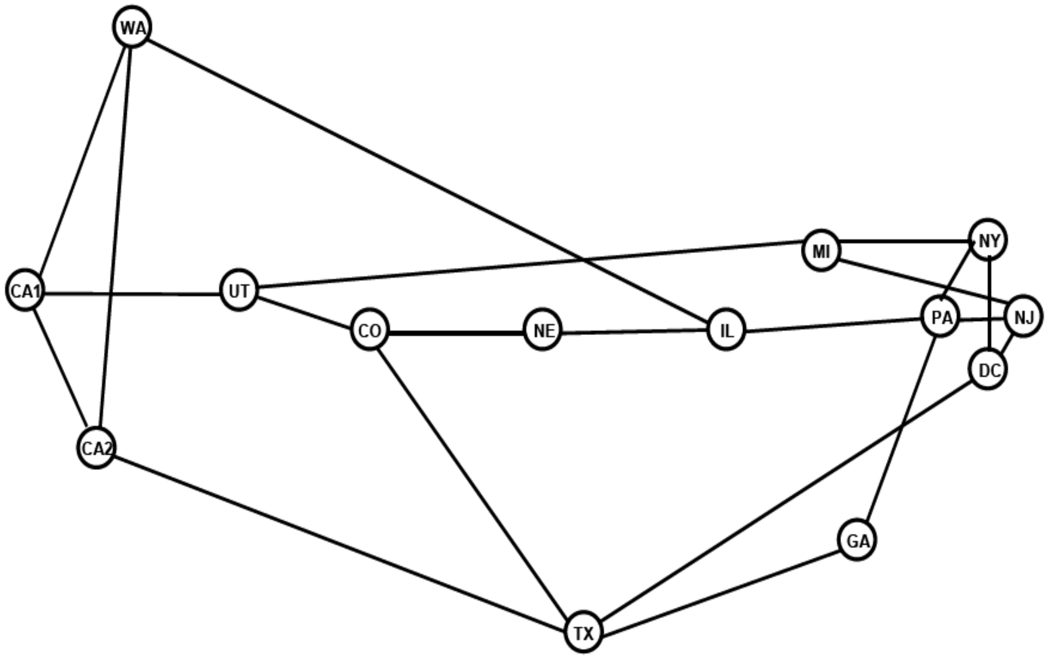


Figure 5.2 : USNET Network Topology (14 Nodes)

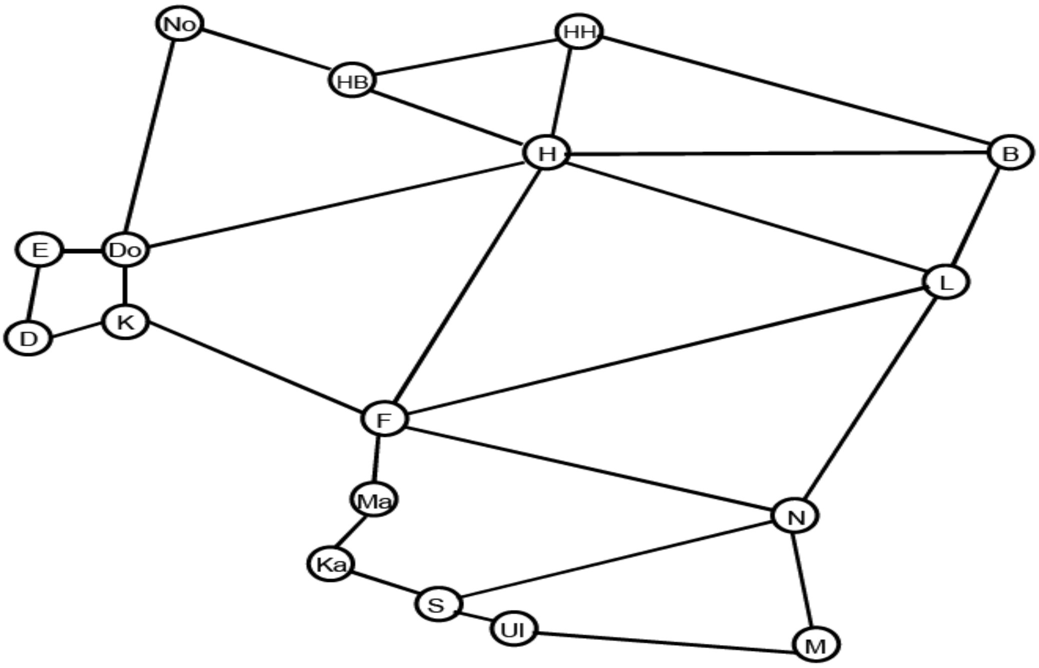


Figure 5.3 : German Network Topology (17 Nodes)

The cost values are assigned as distances between nodes also taken from [27]. The distance matrices are presented in the tables A.1, A.2 and A.3 in appendix A.2 for Pan European, USNET and German network topologies respectively. In second simulation scenario, the links are assumed to have limited bandwidth. To accomplish this task, every link is assigned a bandwidth capacity according to their yearly IP traffic converted in Gbyte/sec. from [27]. The bandwidth matrices are also presented in appendix A.2 in tables A.4 and A.5 for Pan European and USNET network topologies respectively.

5.2 Validation of Network Topologies

As stated before, firstly, the proposed model is simulated in order to validate the implementation of SCA with original paper [4]. In this first scenario, 135 Shared Backup Path Protection (SBPP) connections are allocated statically with SSR as in original paper. The MTTF of 600 FIT and MTTR of 11.4 hours values are used as input in the simulation.

The figures 5.4-5.6 show results of three different network topologies. The results shown are an average of 10 simulation runs with confidence interval of 97.5%. We can easily match the results with the results of original work for Pan European Network in [4].

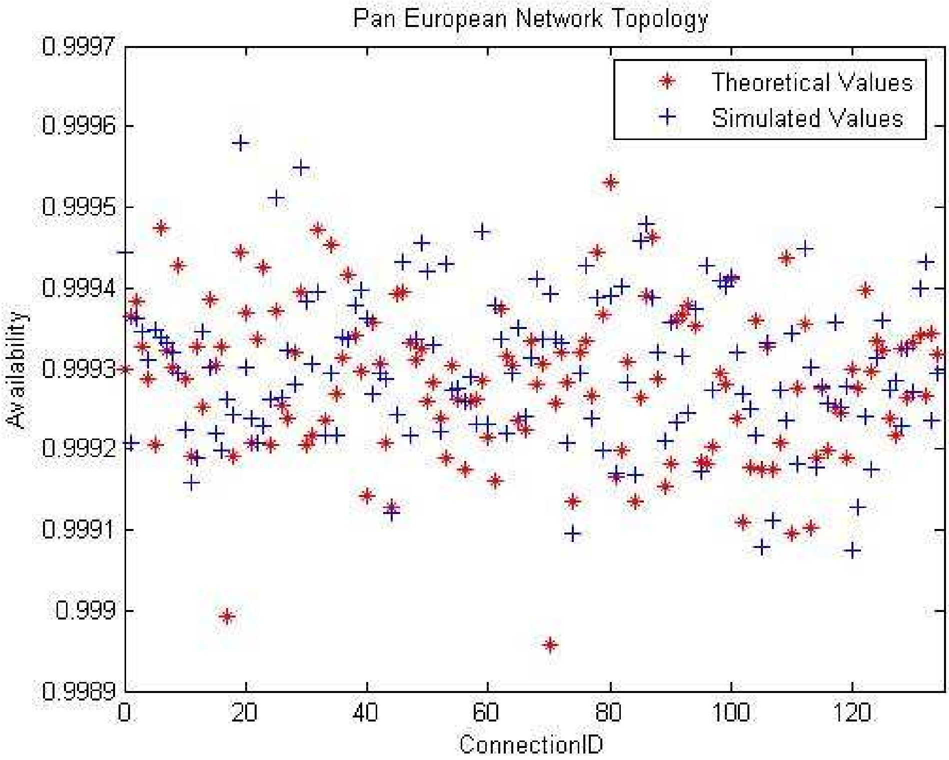


Figure 5.4 : SCA Validation for Pan European Network

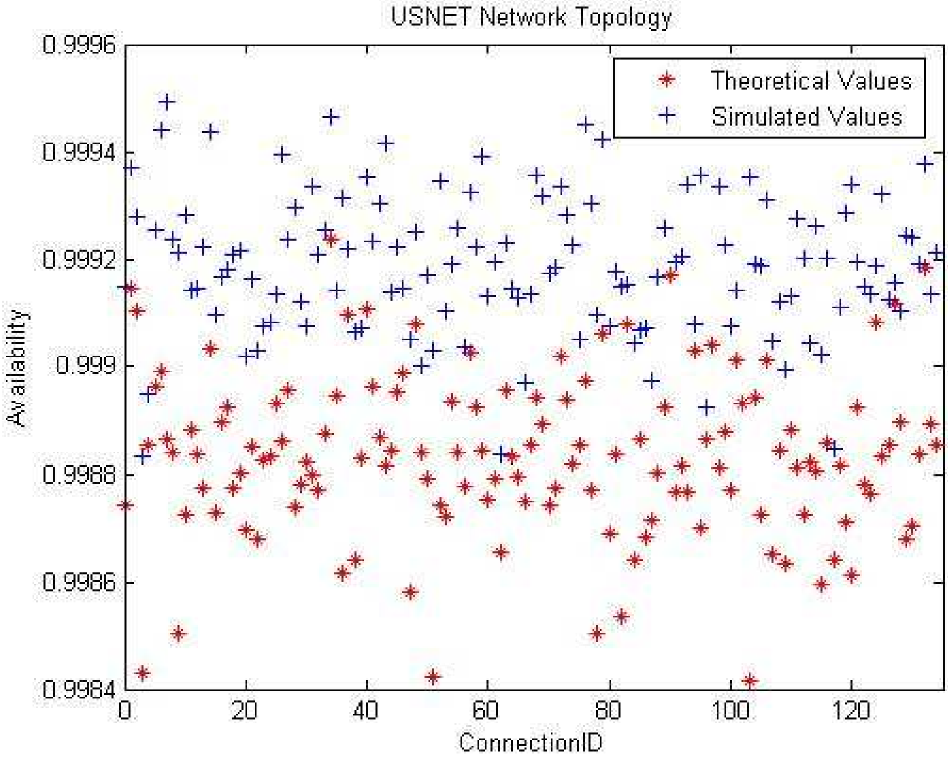


Figure 5.5 : SCA Validation for USNET Network

After comparing the results, we decided run further simulation for only Pan European Network and USNET Topologies, because most of the simulated values in the results for German Network Topology were below the theoretical values meaning that the SCA model is not suitable for that topology.

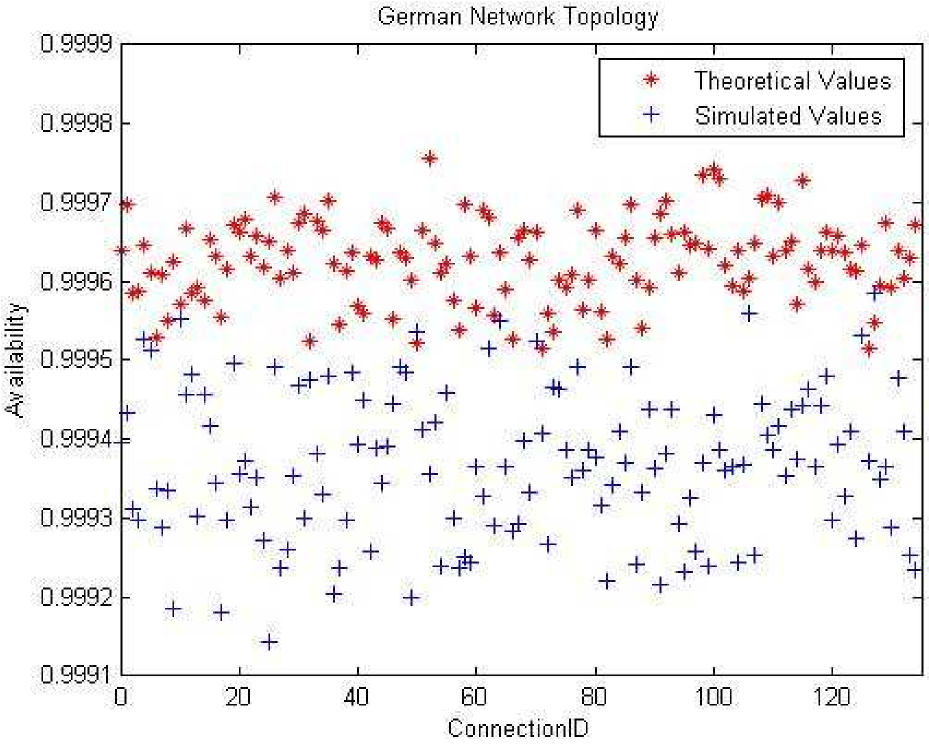


Figure 5.6 : SCA Validation for German Network

Again to validate results with SCA, we run simulation with different scaled network loads and compared the theoretical values with simulated values. The simulation is run only for Pan European network to comply with original SCA results. As it is seen in figure 5.7 the minimum value of the difference is for scaled load of 1.0 with the value 0.0017% whereas the maximum value of difference is 0.1317% for the scaled load of 2.8.

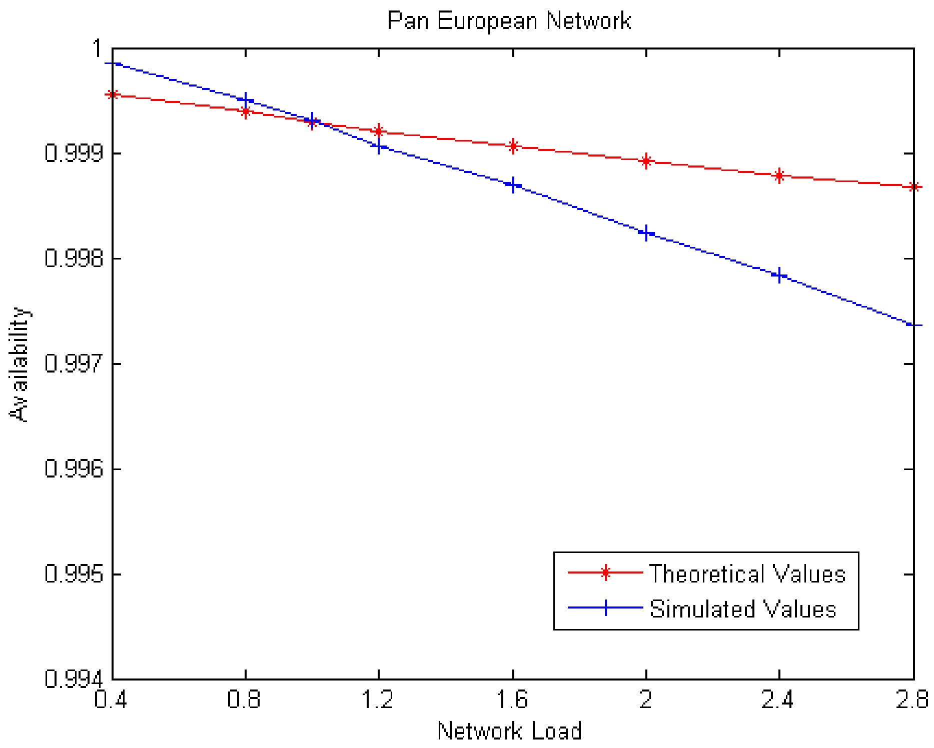


Figure 5.7 : Validation of SCA in different loads (PANEU)

5.3 Pan European Network Results

In the further stages, we run simulation to measure blocking probability of connection requests with our proposed model and additional heuristics. The capacity of every link is assigned as total network traffic from a range of 140 to 2892 Mbps according to network bandwidth capacity matrices in tables A.4 and A.5. Every connection has a holding time of 1 hour to simplify network load calculations and a bandwidth request from a range of 120 to 360 Mbps. Inter-arrival time between two connections is negative exponentially distributed with mean 0.8 hours. At each run, the total number of connection demands is fixed to a number ranging from 10 to 100 so that network load is varied. We run the simulation programs for a virtual duration of 270 days.

The results in figure 5.8 indicate that Heuristic II, LRP, reduces the blocking probability values by an average of 5.5% compared to the other methods. Heuristic I, Exchange Method, has almost no effect to overall blocking probability as expected since the dropped connection during the exchange is also included to blocking probability calculations. All the results shown have confidence interval value of %90.

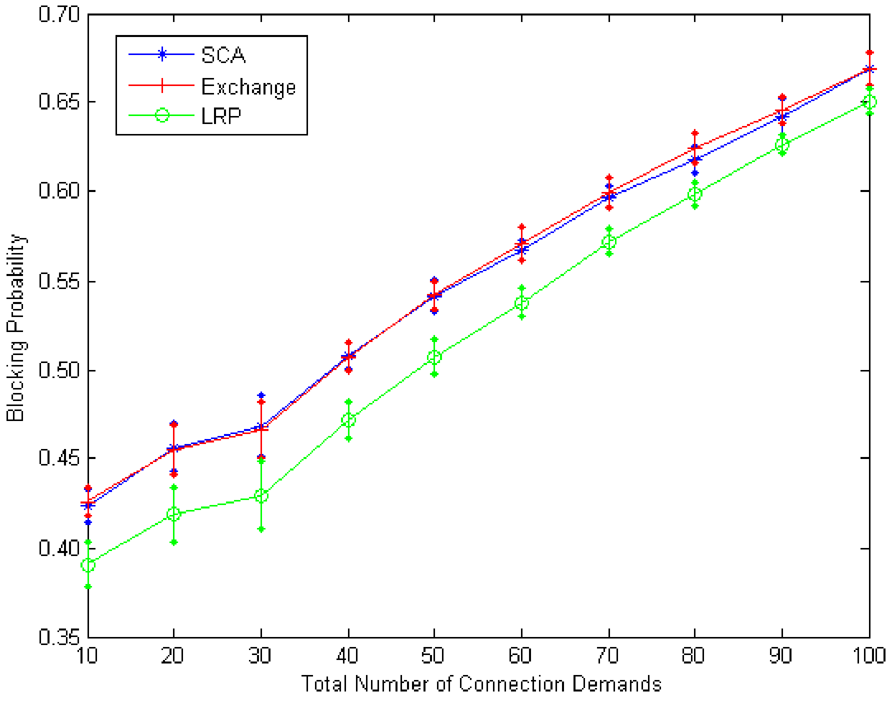


Figure 5.8 : Blocking Probability Comparison Methods (PANEU)

In order to further investigate the results, we classified the blocking reason of the connections into two sections: Bandwidth Inefficiency (Bw) and Availability Constraint (Av). The connections dropped due to SCA calculations and due to Exchange Method are included in Bw section. The figures 5.9-5.12 show the blocking probability values detailed for each connection class and blocking probability reason. The value titles ending are organized as <Connection Class><Method><[Bw-Av.]>. The suffix Bw shows the blocked connection ratio due to bandwidth limit where Av shows blocking probability due to availability constraint. The blocking probability due to lack of bandwidth is almost same for all connection classes where there is a slight increase in values of LRP as the load increases. For the blocking probability values due to availability constraints, there is nearly no blocking for low SLA connections. LRP method improves blocking probability by an average of 8.1% for 0.9999 connections and by 7.5% for 0.99999 connections compared to others. This shows that LRP method is successful for prioritizing high-SLA connections whereas Exchange Method has made almost no difference. The results for 0.99 and 0.999 are almost identical since the minimum link availability in topology is 0.999 and the connection requess are uniformly distributed among all class connections.

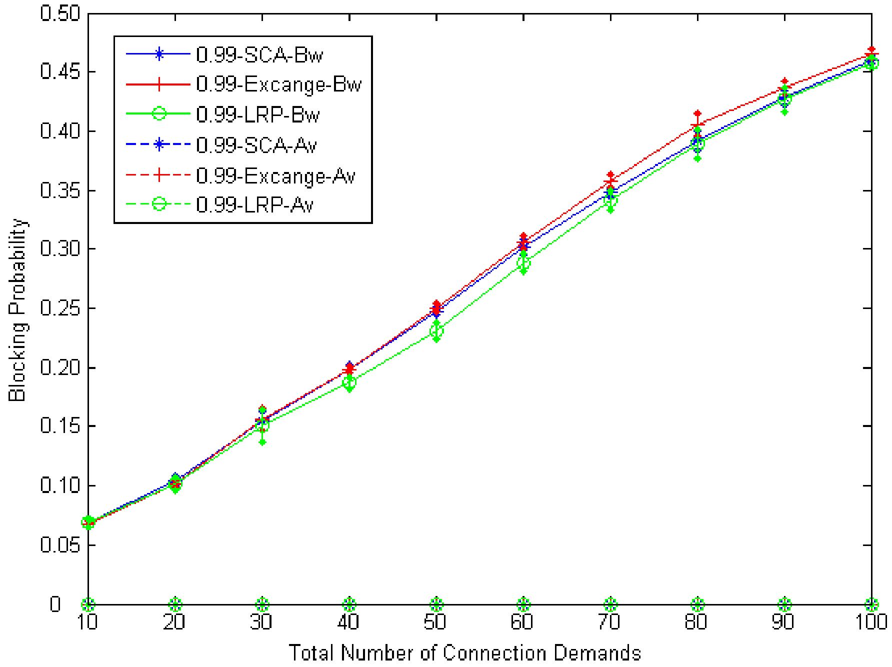


Figure 5.9 : Blocking Probability Detail for 0.99 connections (PANEU)

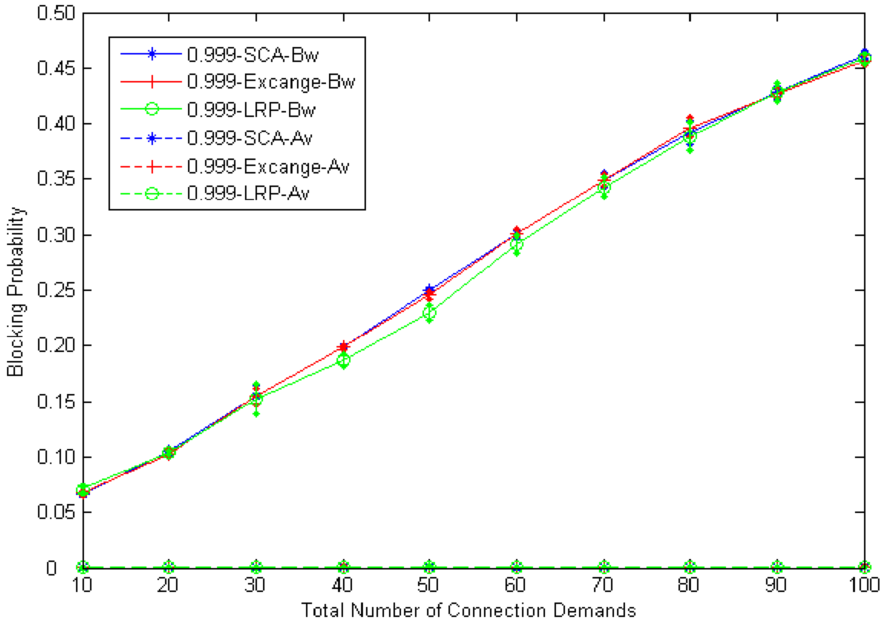


Figure 5.10 : Blocking Probability Detail for 0.999 connections (PANEU)

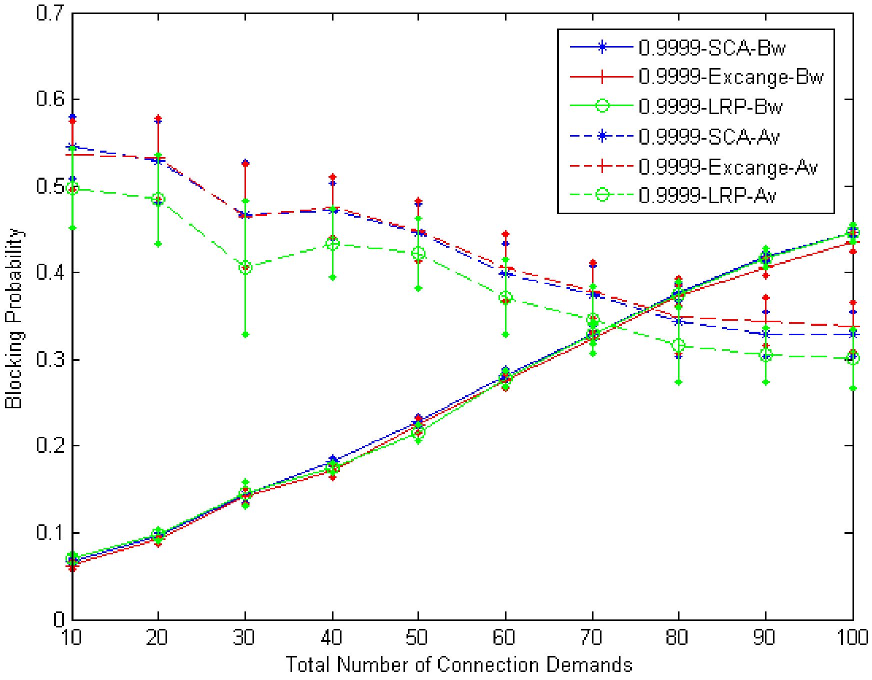


Figure 5.11 : Blocking Probability Detail for 0.9999 connections (PANEU)

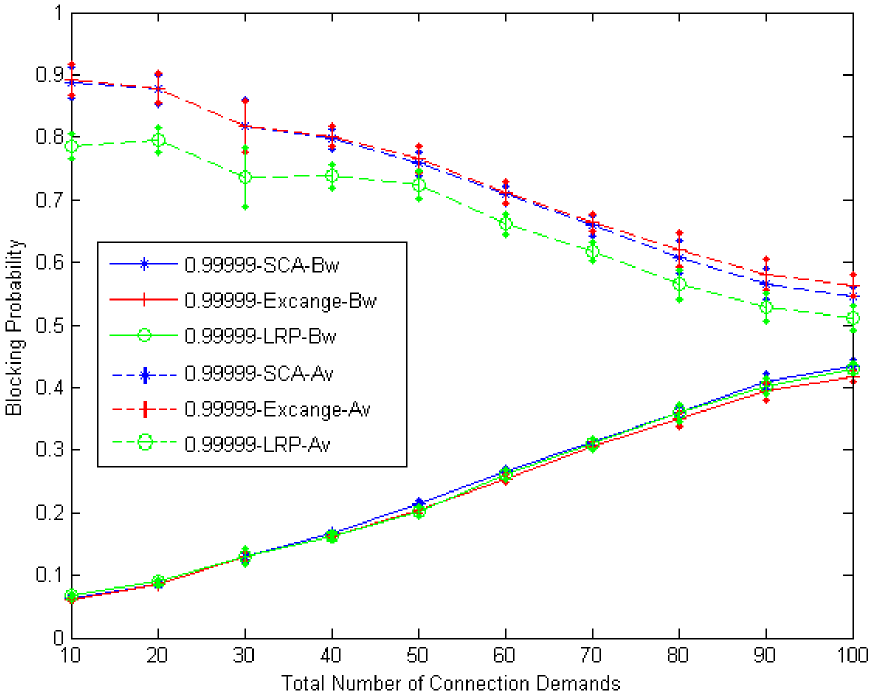


Figure 5.12 : Blocking Probability Detail for 0.99999 connections (PANEU)

Finally, the figure 5.13 shows the resource overbuild values for all methods with different network loads in Pan European Network Topology. Resource overbuild values are decreasing as the network load increases as expected where values of all three methods are very near to each other.

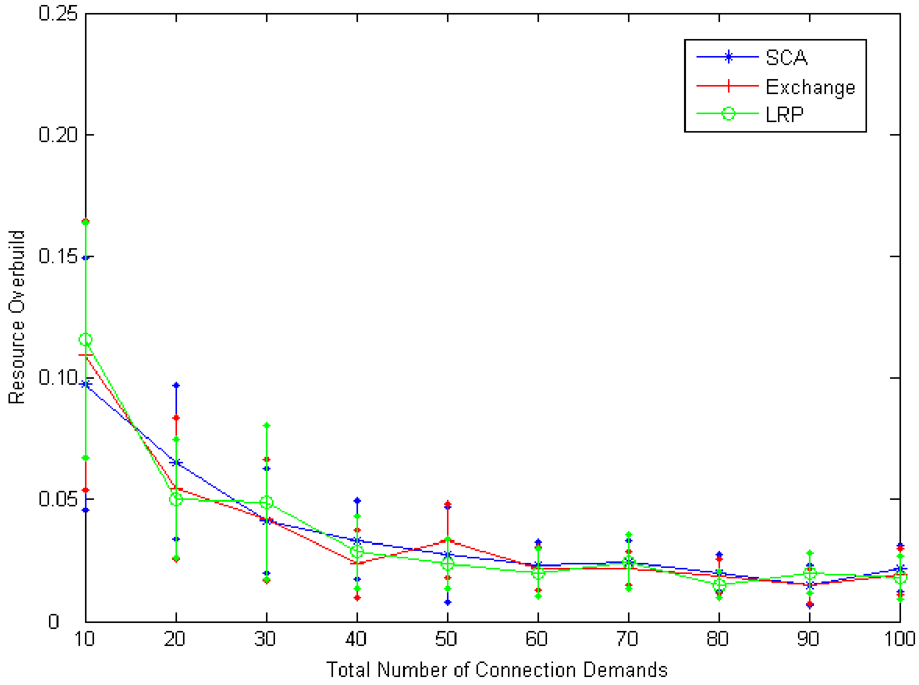


Figure 5.13 : Resource Overbuild (PANEU)

5.4 Results for USNET Network

The following results are obtained from USNET network topology with the same simulation configuration that is used with Pan European network topology. The capacity of every link is assigned as total network traffic from the table A.5. Every connection has a holding time of 1 hour to simplify network load calculations and a bandwidth request from a range of 120 to 360 Mbps. Inter-arrival time between two connections is negative exponentially distributed with mean 0.8 hours. At each run, the total number of connection demands is fixed to a number ranging from 10 to 100 so that network load is varied. We run the simulation programs for a virtual duration of 270 days.

The results in figure 5.14 indicate that Heuristic II, LRP, reduces the blocking probability values by an average of 13.2% compared to the other methods. Heuristic I, Exchange Method, again has almost no effect to overall blocking probability as expected since the dropped connection during the exchange is also included to blocking probability calculations. All the results shown have confidence interval value of %90. Here it should be noted that since the link capacities of USNET network topology are much higher compared to Pan European Network Topology, therefore the blocking probability changes very slighty. The the total connection demands could not create a bandwidth bottleneck in topology until 90 connection demands, the change in blocking probability is very slow.

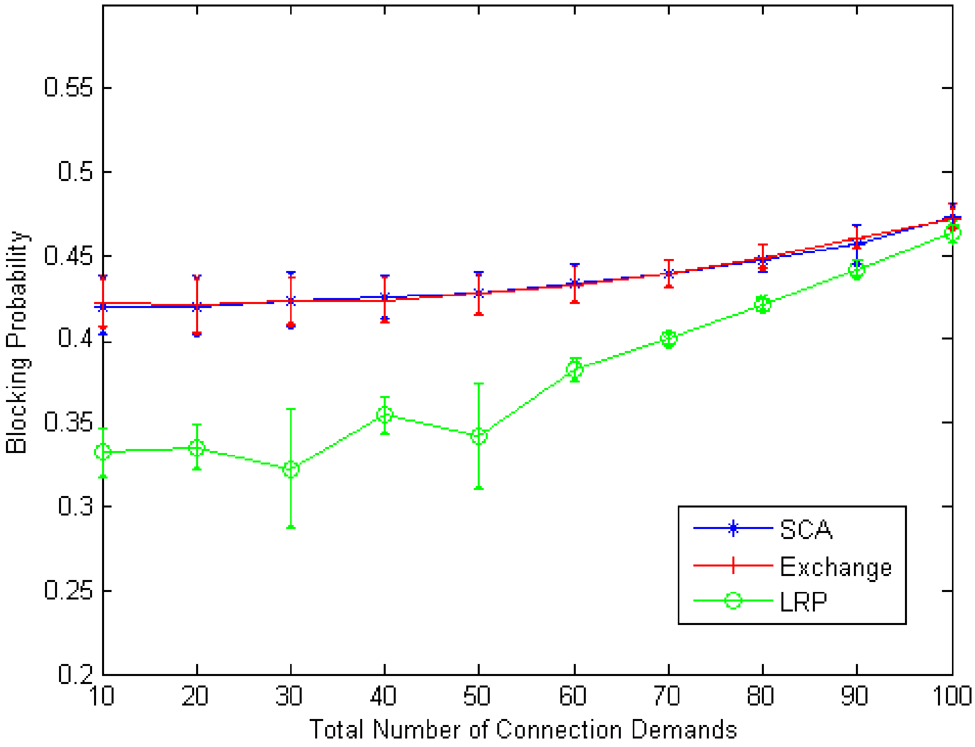


Figure 5.14 : Blocking Probability Comparison Methods (USNET)

The figures 5.15-518. show the blocking probability values detailed for each connection class and blocking probability reason. Again, LRP method improves blocking probability by an average of 19.1% for 0.9999 connections and by 15.7% for 0.99999 connections compared to others. Again, the results for 0.99 and 0.999 are almost identical since the minimum link availability in topology is 0.999 and the connection request are uniformly distributed among all class connections.

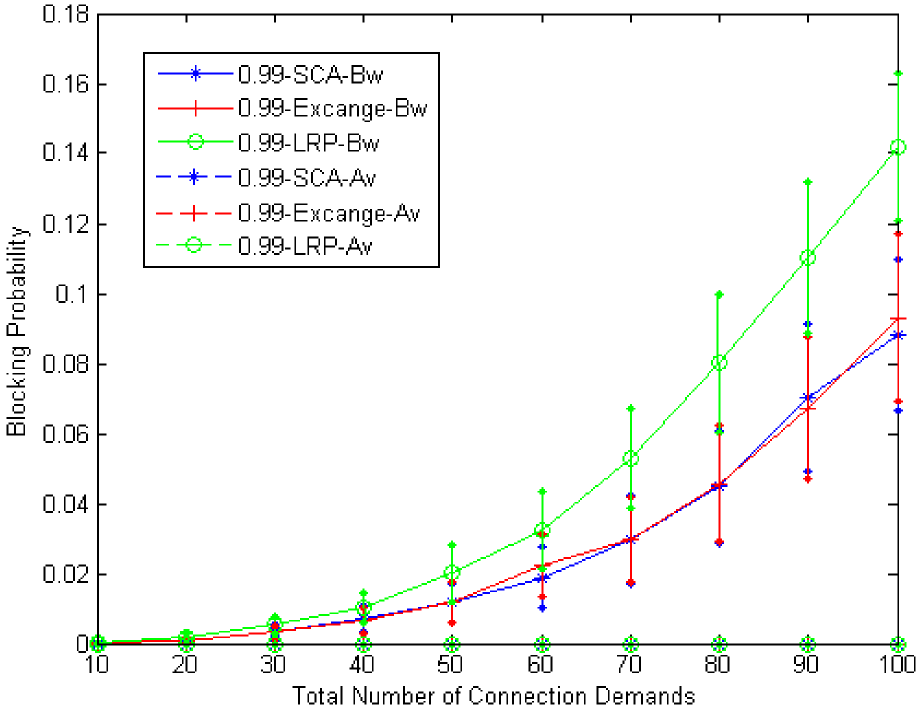


Figure 5.15 : Blocking Probability Detail for 0.99 connections (USNET)

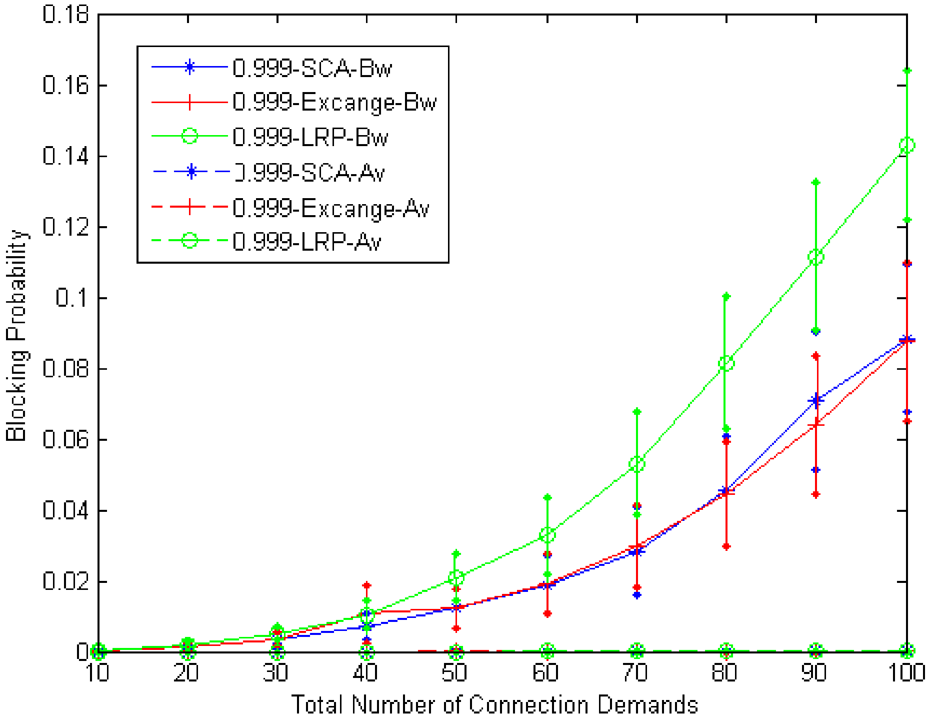


Figure 5.16 : Blocking Probability Detail for 0.999 connections (USNET)

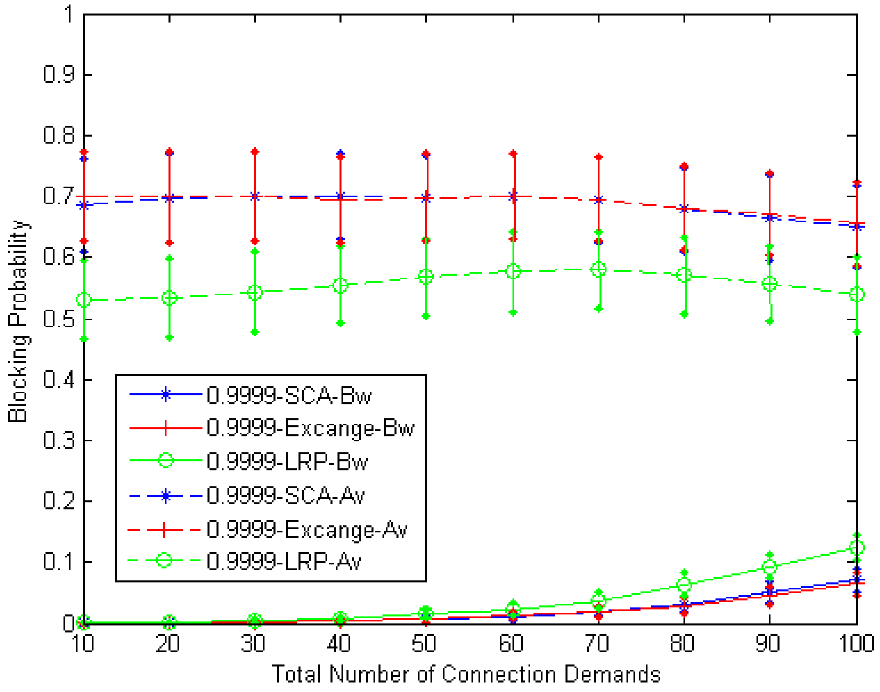


Figure 5.17 : Blocking Probability Detail for 0.9999 connections (USNET)

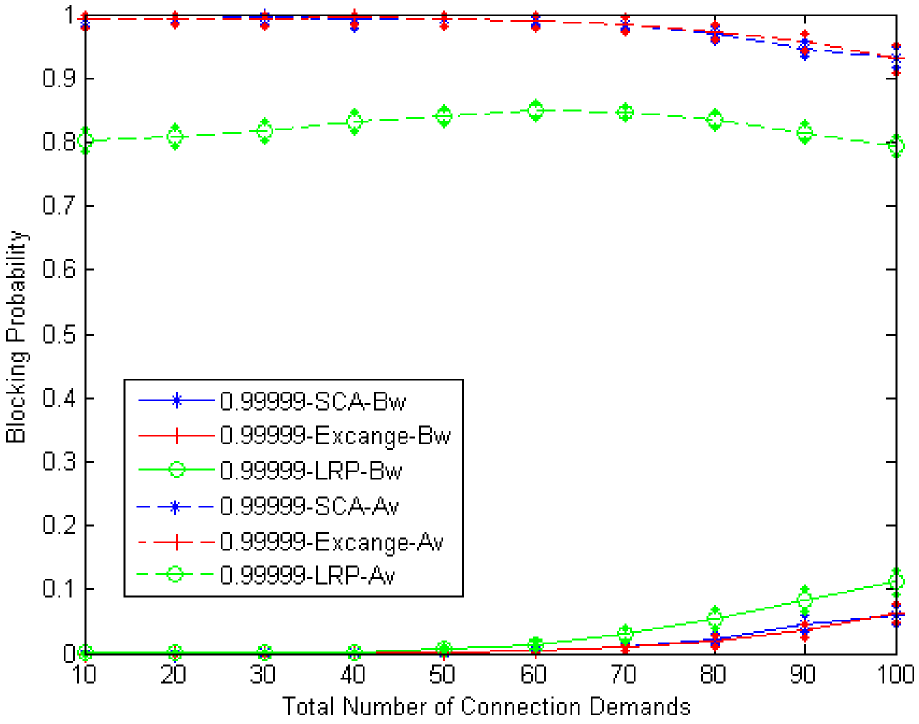


Figure 5.18 : Blocking Probability Detail for 0.99999 connections (USNET)

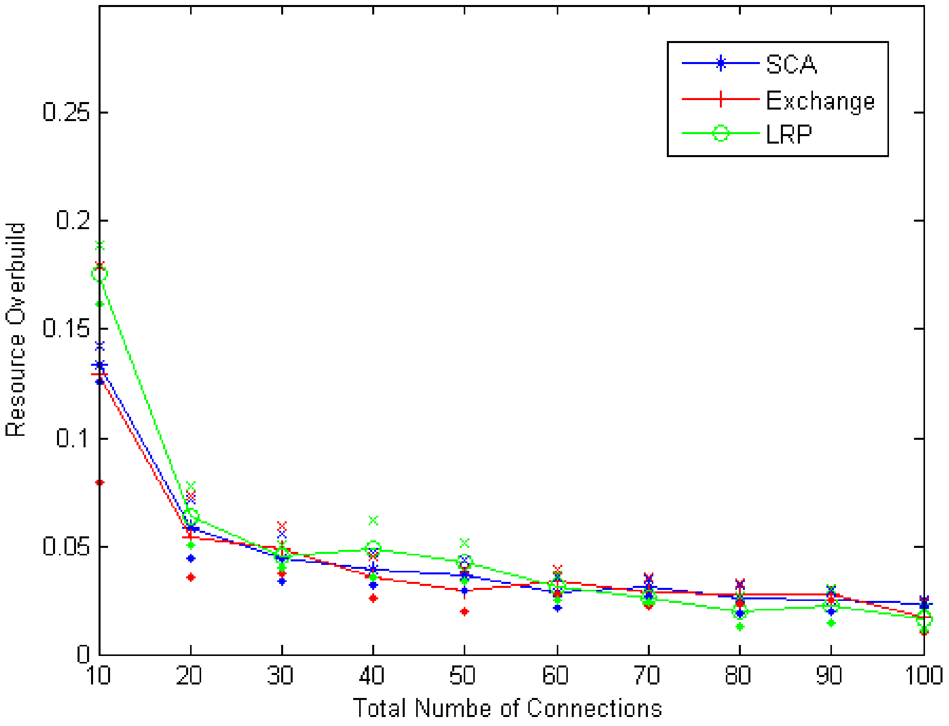


Figure 5.19 : Resource Overbuild (USNET)

At last, the figure 5.19 shows the resource overbuild values for all methods with different network loads in USNET network topology. Resource overbuild values are decreasing as the network load increases as expected where values of all three methods are very near to each other.

6. CONCLUSION

In this thesis, we proposed a new path protection scheme which aims to minimize backup resource consumption by deploying the optimized SCA method with an availability guarantee. We defined Network Event Counter *(N_c)* in order to make our model scalable. Moreover, we defined two heuristic methods to reduce blocking probability of incoming connection requests with high SLA levels. The proposed model is first validated on a static environment with 135 SPP connections. The validation is done with three different topologies namely Pan European network, USNET network and German network. The results are compared with original SCA algorithm results.

Further simulations are run to test the heuristic methods. In these simulations we measured the blocking probability of connection requests. It is shown that proposed Least Reliable Path (LRP) method improves blocking probability values at least by 7.5% in Pan European network whereas Exchange Method makes no change in results.

As a future extension, we are going to simulate our model on using spare/dense network topologies. We also include evaluating the effect of partially wavelength/waveband convertible and wavelength/waveband continuous networks on our proposed scheme in the future extension of this work.

REFERENCES

[1] **Metzler J.,** 2006: The Cost And Management Challenges of MPLS Services. *IT Impact Brief*. Retrieved September 10, 2009 from

http://www.netscout.com/docs/itimpactbriefs/NetScout_iib_Metzler_0506_Cost_MPLS.pdf

[2] **Arci D., Maier G., Pattavina A., Petecchit D., Tornatore M.,** 2003: Availability models for protection techniques in WDM networks, *Design of Reliable Communication Networks (DRCN),* Banff, Alberta, Canada

[3] **Mukherjee D. S., Assi C., Agarwal A.,** 2006: An Alternative Approach for Enhanced Availability Analysis and Design methods in p-Cycle-based networks, *IEEE Journal on Selected Areas in Communications, Vol. 24, No. 12*

[4] **Ho P., Tapolcai J., Haque A.,** 2008: Spare Capacity Reprovisioning for Shared Backup Path Protection in Dynamic Generalized Multi-Protocol Label Switched Networks, *IEEE Transactions on Reliability, Vol. 57, No. 4*

[5] **Doucette J., Clouqueur M., Grower W.,** On the availability and capacity requirements of shared backup path-protected mesh networks, *Optical Network Magazine, Vol. 4, pp. 29-44 Nov-Dec.*

[6] **Ebeling, Charles E.,** 1997: An Introduction to Reliability and Maintainability Engineering, *McGraw-Hill Companies, Inc., Boston*.

[7] **Tornatore M., Maier G., Pattavina A.,** 2005: Availability Design of Optical Networks, *IEEE Journal on Selected Areas of Communications, Vol. 23, No. 8, Aug.*

[8] **Saradhi C.V., Murthy C.S.R.,** 2003: Segmented Protection Paths in WDM Mesh Networks, *High Performance Routing and Switching, (pp. 311-316)*

[9] **Grover W.D., Stamatelakis D.,** 1998: Cycle-oriented distributed preconfiguration: ring-like speed with mesh-like capacity for self-planning network restoration, *IEEE International Conference on Communications, Vol. 1 (pp. 537 -543)*

[10] **Leon-Garcia A., Widjaja I.,** 2006: *Communication Networks: Fundamental Concepts and Key Architechtures,* (2nd ed.), Singapore: McGraw-Hill, pp. 739-740.

[11] **Yin Y., Kuo G.,** 2005: An Improved OSPF-TE in GMPLS-Based Optical Networks, *High Performance Switching and Routing*.

[12] **Cugini F., Andriolli N., Castoldi P.,** 2004: A novel OSPF extension including node architectural constraints for GMPLS networks, *11th International Telecommunications Network Strategy and Planning Symposium, (pp. 291-296)*

[13] **Zuliani L.G.,; Savasini M., Pavani G.S., Pasquini R., Verdi F.L., Magalhaes M.,** 2006: An implementation of an OSPF-TE to support GMPLS-controlled All-Optical WDM Networks, *International Telecommunications Symposium, (pp. 300-305)*

[14] **Liu H., Bouillet E., Pendarakis D., Komaee N., Labourdette J., Chaudhuri S.,** 2004: Extending OSPF routing protocol for shared mesh restoration, *13th IEEE Workshop on Local and Metropolitan Area Networks, (pp. 97-101)*

[15] **Huang C., Li M., Srinivasan A.,** 2007: A Scalable Path Protection Mechanism for Guaranteed Network Reliability Under Multiple Failures, *IEEE Transactions on Reliability, Vol. 56, No. 2.*

[16] **Ho P., Topalcai J., Haque A.,** 2006: A Study on Dynamic Survivable Routing with Availability Constraint for GMPLS-Based Recovery, *3rd International Conference on Broadband Communications, Networks and System*s, *(pp. 1-10)*

[17] **Velasco L., Spadaro S., Commellas J., Junyent G.,** 2006: Failure Aware Diverse Routing: A Novel Algorithm to Improve Availability in ASON/GMPLS Networks, *International Conference on Transparent Optical Networks, (pp. 195-198)*

[18] **Chava V. S., Salvadori E., Zanardi A., Dalsass S., Piesiewicz R.,** 2009: Impairment aware GMPLS-based control plane architectures to realize dynamically reconfigurable transparent optical networks, *International Conference on Photonics in Switching, (pp. 1-2)*

[19] **Aslam F., Uzmi Z. A., Farrel A., Pioro M.,** 2007: Inter-Domain Path Computation using Improved Crankback Signaling in Label Switched Networks, *IEEE International Conference on Communications, (pp. 2023-2029)*

[20] **Staessens D., Audenaert P., Colle D., Lievens I., Pickavet M., Demeester P.,** 2008: Survivability over multiple GMPLS domains, *International Conference on Transparent Optical Networks, Vol 3, (pp. 31-33)*

[21] **Staessens D., Colle D., Lievens U., Pickavet M.; Demeester P.; Colitti W., Nowe A., Steenhaut K., Romeral R.,** 2008: Enabling High Availability over Multiple Optical Network, *IEEE Communications Magazine, Vol 46, Issue 6 (pp. 120-126)*

[22] **Liu Y., Tipper D. A., Siripongwutikorn P.,** 2005: Approximating Optimal Spare Capacity Allocation by Successive Survivable Routing, *IEEE/ACM Transactions on Networking, Vol. 13, No.1, Feb.*

[23] **Qi Guo, Pin-Han Ho, Haque A., Mouftah H.T.,** 2007: Availability-Constrained Shared Backup Path Protection (SBPP) for GMPLS-Based Spare Capacity Reprovisioning, *IEEE International Conference on Communications, (pp. 2186-2191)*

[24] **Mello D.A.A., Schupke D.A., Waldman H.,** 2005: A Matrix-Based Analytical Approach to Connection Unavailability Estimation in Shared Backup Path Protection, *IEEE Communications Letters, Vol. 9, No 9, Sep.*

[25] No-Date: IBM ILOG CPLEX: Hi-Perf. Mathematical programming engine, http://www-01.ibm.com/software/integration/optimization/cplex/ , retrieved on 4th April 2010.

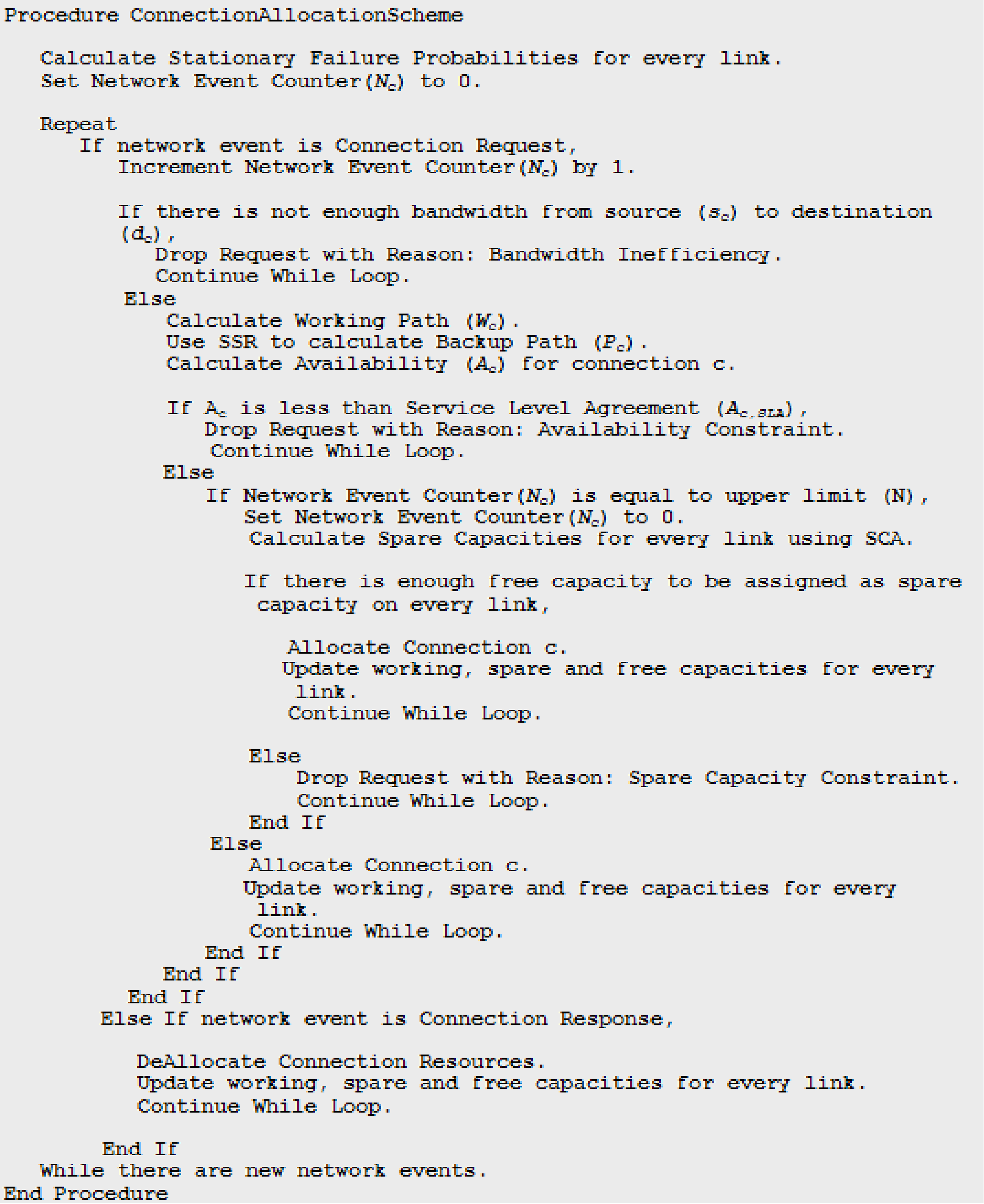
[26] **Kantarci B., Mouftah H. T., Oktuğ S. F.,** 2009: Adaptive Schemes for Differentiated Availability-Aware Connection Provisioning in Optical Transport Networks, *Journal of Lightwave Technology, Vol. 27, Issue 20, (pp. 4595-4602).*

[27] **Betker A., Gerlach C., Hülsermann R., Jäger M.,** 2003: Reference Transport Network Scenarios, *MultiTeraNet Report.* http://www.ikr.uni-stuttgart.de/IKRSimLib/Usage/Referenz_Netze_v14_full.pdf, retrieved on 4th April 2010.

[28] **Sancak A., Kantarci B., Oktug S.,** 2010: Class Based Availability Considerations in GMPLS Networks, accepted to be presented at *IEEE Symposium on Computers and Communications (ISCC 2010).*

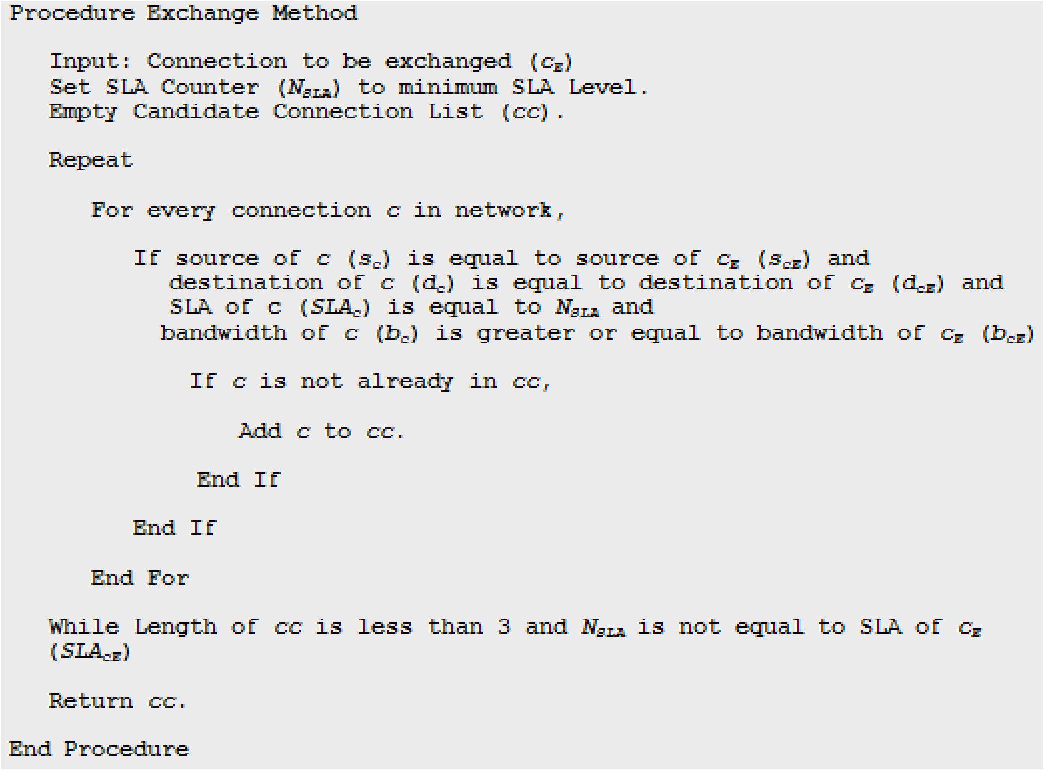
APPENDICES

APPENDIX A.1: The pseudo code representations of proposed schemas.



```
Procedure ConnectionAllocationScheme

   Calculate Stationary Failure Probabilities for every link.
   Set Network Event Counter($N_c$) to 0.

   Repeat
      If network event is Connection Request,
         Increment Network Event Counter($N_c$) by 1.

         If there is not enough bandwidth from source ($s_c$) to destination
         ($d_c$),
            Drop Request with Reason: Bandwidth Inefficiency.
            Continue While Loop.
         Else
            Calculate Working Path ($W_c$).
            Use SSR to calculate Backup Path ($P_c$).
            Calculate Availability ($A_c$) for connection c.

            If $A_c$ is less than Service Level Agreement ($A_{c,SLA}$),
               Drop Request with Reason: Availability Constraint.
               Continue While Loop.
            Else
               If Network Event Counter($N_c$) is equal to upper limit (N),
                  Set Network Event Counter($N_c$) to 0.
                  Calculate Spare Capacities for every link using SCA.

                  If there is enough free capacity to be assigned as spare
                  capacity on every link,

                     Allocate Connection c.
                     Update working, spare and free capacities for every
                     link.
                     Continue While Loop.

                  Else
                     Drop Request with Reason: Spare Capacity Constraint.
                     Continue While Loop.
                  End If
               Else
                  Allocate Connection c.
                  Update working, spare and free capacities for every
                  link.
                  Continue While Loop.
               End If
            End If
         End If
      Else If network event is Connection Response,

         DeAllocate Connection Resources.
         Update working, spare and free capacities for every link.
         Continue While Loop.

      End If
   While there are new network events.
End Procedure
```

Figure A.1 : The pseudo code representation of proposed schema



```
Procedure Exchange Method

   Input: Connection to be exchanged ($c_E$)
   Set SLA Counter ($N_{SLA}$) to minimum SLA Level.
   Empty Candidate Connection List ($cc$).

   Repeat

      For every connection $c$ in network,

         If source of $c$ ($s_c$) is equal to source of $c_E$ ($s_{cE}$) and
            destination of $c$ ($d_c$) is equal to destination of $c_E$ ($d_{cE}$) and
            SLA of c ($SLA_c$) is equal to $N_{SLA}$ and
           bandwidth of $c$ ($b_c$) is greater or equal to bandwidth of $c_E$ ($b_{cE}$)

             If $c$ is not already in $cc$,

                Add $c$ to $cc$.

             End If

         End If

      End For

   While Length of $cc$ is less than 3 and $N_{SLA}$ is not equal to SLA of $c_E$
   ($SLA_{cE}$)

   Return $cc$.

End Procedure
```

Figure A.2 : The pseudo code representation of LRP

APPENDIX A.2: The distance and traffic matrices of network topologies [27].

	Lon	Par	Bru	Ams	Lyn	Zur	Str	Fra	Ham	Mil	Mun	Ber	Rom	Zag	Vie	Pra
London		514		540												
Paris	514		393		594		600									
Brussels		393		259				474								
Amsterdam	540		259						552							
Lyon		594				507										
Zurich					507		218			327						
Strasbourg		600				218		271								
Frankfurt			474				271		592		456					
Hamburg				552				592				381				
Milan						327					522		720			
Munich								456		522		757			534	
Berlin									381		757					420
Rome										720				783		
Zagreb													783		400	
Vienna											534			400		376
Prague												420			376	

Table A.1 : The distance matrix of Pan European Network (in km's)

	WA	CA1	CA2	UT	CO	TX	NE	IL	PA	GA	MI	NY	NJ	DC
WA		1338	2056					3048						
CA1	1338		834	1152										
CA2	2056	834					2520							
UT		1152			684				2820					
CO				684		870	1746							
TX					870			864						
NE			2520		1746					1350				2364
IL	3048					864						846		
PA				2820							720		942	
GA							1350					1008		
MI									720			438		468
NY								846		1008	438		540	
NJ									942			540		312
DC							2364				468		312	

Table A.2 : The distance matrix of USNET Network (in km's)

	Nor	Ess	Dus	Kol	Fra	Man	Kar	Bre	Dor	Ham	Han	Stu	Ulm	Ber	Lei	Nur	Mun
Norden								144	278								
Essen			36						37								
Dusseldorf		36		41													
Koln			41		182				88								
Frankfurt				182		85					316				353	224	
Mannheim					85		64										
Karlsruhe						64						74					
Bremen	144									114	120						
Dortmund	278	37		88							208						
Hamburg								114			157			306			
Hannover					316			120	208	157				298	258		
Stuttgart							74						86			187	
Ulm												86					143
Berlin										306	298				174		
Leipzig					353						258			174		275	
Nurnberg					224							187			275		179
Munchen													143			179	

Table A.3 : The distance matrix of German Network (in km's)

	Lon	Par	Bru	Ams	Lyn	Zur	Str	Fra	Ham	Mil	Mun	Ber	Rom	Zag	Vie	Pra
London		1962		2892												
Paris	1962		596		670		667									
Brussels		596		954				908								
Amsterdam	2892		954						1582							
Lyon		670				484										
Zurich					484		730			1119						
Strasbourg		667				730		1656								
Frankfurt			908				1656		1904		2135					
Hamburg				1582				1904				2318				
Milan						1119					2224		2138			
Munich								2135		2224		1721			1044	
Berlin									2318		1721					753
Rome										2138				305		
Zagreb													305		140	
Vienna											753			140		412
Prague												1044			412	

Table A.4 : The bandwidth matrix of Pan European Network (in MByte/s)

	WA	CA1	CA2	UT	CO	TX	NE	IL	PA	GA	MI	NY	NJ	DC
WA		1338	2056					3048						
CA1	3644		834	1152										
CA2	4784	8108					2520							
UT		3206			684				2820					
CO				2408		870	1746							
TX					6176			864						
NE			3149		1822					1350				2364
IL	5162					16192						846		
PA				4388							720		942	
GA							6991					1008		
MI									13504			438		468
NY								17923		28901	17332		540	
NJ									37320			26708		312
DC							3359				11014		9538	

Table A.5 : The bandwidth matrix of USNET Network (in MByte/s)

CURRICULUM VITA

Adnan Sancak was born in 1984 in Istanbul, TURKEY. He finished his primary, secondary and high school educations in Istanbul. He obtained his bachelor degree in Computer Engineering from Istanbul Technical University in 2007. Afterwards, he started his M.Sc. in Computer Engineering in ITU in 2007. Starting from 2007, he is working for Arçelik A.Ş. as software engineer in Istanbul. He is still a M.Sc. student in Istanbul Technical University.

Publications:

▪ **Sancak A., Kantarcı B., Oktuğ S.,** 2010: Class Based Availability Considerations in GMPLS Networks, accepted to be presented at *IEEE Symposium on Computers and Communications (ISCC 2010)*.