NTNU – Trondheim
Norwegian University of
Science and Technology

Fulfilling efficiently SLA availability guarantees in backbone networks

Prakriti Tiwari

Master of Science in Communication Technology
Submission date: July 2014
Supervisor: Bjarne Emil Helvik, ITEM
Co-supervisor: Andres Gonzalez, ITEM

Norwegian University of Science and Technology
Department of Telematics

Problem Description

Title: Fulfilling efficiently SLA availability guaranteed in IP backbone network
Name of student: Prakriti Tiwari

Real world telecommunication networks are not failure free. Network failures not only affect the network user, but also affect the reputation of the network provider. Hence, a common policy was introduced known as Service-Level Agreements (SLA) which are contracts between the provider and receiver of the services where the guaranteed availability for a given period are established. Delivering highly available services may incur high cost for the network provider regarding high resources needed to be reserved or the penalties linked with the violation of the agreement needed to pay.

To recover from network failures, two kinds of mechanisms may be used: Protection and Restoration. When a network element fails, the recovery mechanisms attempt to recover the data delivery (service) by making use of an alternative/backup path.

Restoration techniques (e.g. OSPF and IS-IS) seek to establish a new path after a failure has occurred without any prior resource reservation. In the Restoration mechanism the alternative/backup path is computed on demand, i.e. it can be either pre-planned or dynamically allocated, however resources required by the alternative/backup paths are not allocated or reserved until a failure occurs. This yields relatively long recovery times and a path with sufficient resource capacity cannot be guaranteed. Using Protection techniques, the alternative/backup path is pre-computed and resource usage is pre-allocated either dedicated for each connection or shared. The Protection techniques yield faster recovery and (almost) guaranteed capacity at the cost of higher resource usage whereas the Restoration technique is more efficient in the resource utilization but not so reliable. Being able to achieve a Protection-like recovery speed and Restoration-like resource usage in backbone network is a beneficial technique.

Thesis Objective:

The objective of this thesis is to fulfill the SLA availability guarantee using a recovery mechanism like Protection and Restoration in an efficient way. The thesis introduces a hybrid technique which is a combination of Protection and Restoration mechanisms for recovering the failure in end-to-end connections of a backbone network. The purpose is to enable dynamic and online combination of Protection and Restoration such that network providers could get full control over the SLA risk and use only the resources that are needed.

Methodology:

SLA guaranteed availability can be efficiently achieved in backbone networks by going through various processes. Starting from the theoretical and analytical study of probability distribution of downtimes in the backbone network, thereafter study of the risk assessment (evaluating the risk of meeting or not meeting the specified availability, quantitatively) by using different recovery mechanisms. And finally propose a technique, in this case a hybrid recovery mechanism, that provides full control over the SLA risk using only the resources that are needed.

In this thesis the following questions will be addressed that will provide the solution for the thesis objective:

- What is the probability distribution of connection downtime using Protection mechanism?
- What is the probability distribution of connection downtime using Restoration mechanism?
- What are the requirements for designing a hybrid model of Protection and Restoration?
- Is the proposed hybrid model able to fulfill the SLA availability guarantee?
- What is the difference in resource utilization when different hybrid approaches are experimented with?

The thesis is divided in to four phases. The output of each phase provides the input for the next step. The following task will be done in each phase:

Phase 1 – Network Recovery

- Study the concept of Protection and Restoration mechanisms in backbone networks.
- Study the type of Protection and Restoration such as Dedicated Backup Path Protection (DBPP) and Path Restoration respectively and their specification and functionalities.

Phase 2 - Study of Probability Distribution of Downtime

- Study the numerical concept of the distribution of the accumulated downtime (total sum of downtimes during the SLA contract) and the implications with the SLA.
- Investigate the probability distribution for connection downtime using PR. Measurements from UNINETT's backbone network are used for the investigation in order to model the realistic downtime distribution of end-to-end connection that uses PR.
    - Distribution fitting is presented for the downtime data measured from the UNINETT backbone. Meaning that a shape of probability distribution of empirical data is compared and fitted with known distributions such as Gamma and Weibull.
- Investigate the probability distribution for connection downtime using DBPP. The downtimes of DBPP are evaluated using the existing knowledge and study made in previous work.
- Study the concept of Fast Fourier Transformation (FFT) and its utilization in non-parametric distribution. FFT is utilized in order to reduce the complexity of computing the convolution of downtimes.

Phase 3 – Hybrid Model

- Study the SLA risk assessment of DBPP and PR with regards to the analysis of probability distribution of accumulated downtime made in phase 2.
- Design a hybrid model with respect to the SLA risk assessment. The accumulated downtime for the hybrid model with a given availability guarantee is computed based on the result from the accumulated downtime distribution of an end-to-end connection that uses DBPP or PR.
- The transition line for the model based on the result of accumulated downtime of a hybrid model is proposed. The transition line in this context is a line that decides the switching point from DBPP to PR and vice versa in a hybrid model.
- A discrete event simulation on DEMOS platform is built to verify whether the computed transition lines fulfill the SLA requirement at the end of SLA contract.
- Examination of the resource utilization and the total cost for providing the network by the hybrid model is made considering that the network provider fulfill the SLA requirement. The examination is further made for different SLA availability guarantees (SLA risk target) in order to find the optimal risk target which provides minimal cost.

Deliverable:

A hybrid model to recover from end-to-end connection downtime in backbone networks with consideration of resource utilization.

Assignment given: February 2014
Responsible professor: Bjarne E. Helvik
Supervisor: Andres J. Gonzales

NTNU – Trondheim
Norwegian University of
Science and Technology

Fulfilling efficiently SLA availability guarantees in IP backbone network

Prakriti Tiwari

Submission date:	July 2014
Responsible professor:	Bjarne E. Helvik, Affiliation
Supervisor:	Andres Gonzales, Affiliation

Norwegian University of Science and Technology
Department of Telematics

Abstract

The availability and reliability of backbone networks is important to society. However, physical, software and unintentional human error failures affect the links and nodes in a backbone network. To overcome such failures in the network, recovery mechanisms such as Protection and Restoration are utilized. Additionally, a concept of Service Level Agreement (SLA) is introduced between the provider and the user which defines and guarantees the network availability requirements and penalty schemes. In this thesis, fulfilling the SLA availability guarantee efficiently in a backbone network is investigated.

This thesis focuses on the problem of handling end-to-end path failures on backbone networks. Some of the popular existing recovery mechanisms to handle such failures are Dedicated Backup Path Protection (DBPP) and Path Restoration (PR). A high percentage of network survivability can be achieved by DBPP with a reserved backup path for each provisioned connection. Unfortunately, it is very costly and resource demanding. Whereas, a PR based solution consumes only the needed resources but it is very slow to recover from failure which might effect the SLA availability guarantee. The work in this thesis aims at providing a hybrid network recovery model that combines the benefits of both DBPP and PR. The hybrid model switches between DBPP and PR according to the SLA availability requirement over a contract period and the current network connection state (i.e. the remaining time of the SLA and current sum of downtimes (accumulated downtime)).

Moreover, an analysis in the failure logs of UNINETT's backbone network is made to model the probability distribution of the accumulated downtime that uses PR. A distribution fitting is made for modeling the connection downtime data taken from UNINETT's backbone network where Weibull distribution proved to be a good approximation. Additionally, a model for distribution of accumulated downtime that uses DBPP for both non-simultaneous and simultaneous failures of the working path and backup path is provided. An in-depth explanation of how these distributions models can be used in the design of hybrid models is presented.

Two hybrid models were approached in this thesis. The first hybrid approach used the DBPP scheme at the beginning of the SLA duration and then it switches to PR when the calculated SLA risk assessment shows that the probability of violating the SLA requirement is lower at time t. The second hybrid approach used the PR scheme at the beginning of the SLA duration and then it switches to DBPP when the accumulated downtime at time t reach near to the threshold of the SLA risk target such that the probability of violating the SLA requirement is higher. The transition line which decides the switching between PR and DBPP are computed for each hybrid approach using the results obtained from the accumulated downtime distribution model of PR and DBPP. The transition line defined in this thesis provides information about when the connection should switch between Protection and Restoration mechanism by knowing the network connection state. The computed transition lines with a 1 percent SLA risk target is verified via discrete event simulation in DEMOS. The SLA risk target is the probability of failing the SLA, however the provider can tune the risk target by using an advanced network recovery mechanism (e.g Protection) for more or less time. The simulation results showed that the proposed hybrid models work well, fulfilling the SLA availability guarantee efficiently with respect to the resource utilization. In addition, the results also revealed that using the PR scheme at the beginning of the SLA contract provides three times better resource utilization than using the DBPP scheme at the beginning. Cost analysis for network providers are made with different SLA risk targets in order to find the optimal SLA risk target for network providers. The results from analysis suggested that the total cost for network providers decreases with the increase of SLA risk target until the total cost reaches its minimum, then it starts to increase again.

The result of this thesis might contribute to future research on developing a hybrid model to reach particular performance objectives in communication networks.

Sammendrag

Tilgjengeligheten og pålitelighet av stamnettet er viktig for samfunnet. Programvare feil eller menneskelige feil kan påvirke lenker og noder i et stamnett. For å overvinne slik svikt i nettverket, er det utviklet mekanismer som Protection og Restoration benytter. I tillegg ble et konsept av Service Level Agreement (SLA) introdusert mellom leverandøren og brukeren, som definerer eller garanterer nettverks krav til tilgjengelighet og straffeordninger. I denne masteroppgaven, oppfyller SLA tilgjengelighetsgaranti på en effektivt måte i stamnettet er undersøkt.

Denne masteroppgaven fokuserer på problemet med håndteringen av ende-til-ende-bane svikt på stamnettet. Noen av de populære eksisterende gjenvinning mekanisme for å håndtere slike feil er Dedicated Backup Path Protection (DBPP) og Path Restoration (PR). En høy andel av nettverks - overlevelsesevne kan oppnås ved DBPP, med den reserverte backup banen for hver selektiv tilkobling. Dessverre er det svært kostbart og ressurskrevende. Siden forbrukeren av PR basert løsning bare har de nødvendige ressurser, er det veldig tregt til å komme seg fra svikt som kan påvirke SLA tilgjengelighetsgaranti. Arbeidet i denne masteroppgave tar sikte på å utforske hybrid nettverk utvinning som kombinerer fordelene med både DBPP og PR. Hybridnettet utvinning modellen skifter mellom DBPP og PR i henhold til SLA tilgjengelighet krav over en kontraktsperiode, og den gjeldende nettverksforbindelsen tilstand (dvs. den gjenværende tiden av SLA og nåværende akkumulert nedetid).

Det ble videre gjort en analyse i feil logger av UNINETT stamnett gjort for å finne sannsynlighetsfordelingen for akkumulert nedetid ved hjelp av PR. Weibull fordeling viste seg å være en god tilnærming for å modellere forbindelse nedetid data hentet fra UNINETT stamnett når distribusjon montering, Quantile-Quantile modelering ble gjort. I tillegg er en modell for fordeling av akkumulert nedetid ved hjelp DBPP for begge tilfeller (med ikke-samtidig og samtidig svikt i primære banen og backup banen) er analysert. En grundig forklaring på hvordan disse distribusjonene modeller kan brukes i utformingen av hybridmodeller blir presentert.

To hybridmodeller ble representert i denne masteroppgaven. Den første hybrid tilnærming bruker DBPP ordningen på begynnelsen av SLA varighet. Deretter bytter den seg av PR når det beregnet SLA risikovurdering forteller at sannsynligheten for brudd på SLA kravet er lavere på tidspunktet t. Imidlertid, andre hybrid tilnærming bruker

PR-ordningen i begynnelsen av SLA varighet og da bytter den til DBPP når summen av nedetid på tid t rekkevidde nær ved terskelen til SLA risiko mål, slik at sannsynligheten for å krenke SLA krav er høyere. Overgangen linje som bestemmer veksling mellom PR og DBPP ble beregnet for hver hybride tilnærminger ved hjelp av resultatene fra akkumulert nedetid distribusjonsmodell for PR og DBPP. Overgangen linje definert i denne masteroppgave gir informasjon om når tilkoblingen bør veksle mellom DBPP og PR mekanismen ved å vite nettverkstilkoblingsstatus. De beregnede overgangslinjer med en prosent SLA risiko målet ble bekreftet via diskret hendelsessimulering i DEMOS. SLA risikomålet er sannsynligheten for å bomme på SLA, men leverandøren kan med avstemt risikoen målet ved hjelp av avansert nettverks utvinning mekanisme (f.eks Protection) for mer eller mindre tid. Simuleringsresultatene viste at de foreslåtte hybridmodeller fungere godt ved å oppfylle SLA tilgjengelighetsgaranti på effektivt måte . I tillegg er resultatene viste også at bruk av PR-ordningen i begynnelsen av SLA kontrakten gir tre ganger bedre ressursutnyttelse enn å bruke DBPP ordningen i begynnelsen. Kostnadsanalyse for nettverksleverandørene ble gjort med forskjellige SLA risiko mål for å finne den optimale SLA risiko mål for nettverksleverandører. Resultatene fra analysen antydet at den totale kostnaden for nettverksleverandørene avtar med økningen av SLA risikomålet til den totale kostnaden har nådd sitt minimum, så det begynner å øke igjen.

Resultatet av denne masteroppgave kan bidra til fremtidig forskning på å utvikle hybridmodell for å komme på bestemte ytelsemål i kommunikasjonsnett.

Preface

This thesis is submitted in partial fulfilment of the requirements for the degree of Master at the Norwegian University of Science and Technology (NTNU). This thesis has been supervised by Andres J. Gonzales. The work was strengthened by the help received from UNINETT by providing log of failures and repair events in its backbone network.

Acknowledgements

First and foremost I offer my sincerest gratitude to my supervisor Andres J. Gonzales, for the continuous support of my thesis, for his motivation, encouragement and immense knowledge. He has provided me with many valuable questions and important informations regarding MATLAB and DEMOS. His guidance helped me in all the time of research and writing of thesis.

Second, I would like to thank Professor Bjarne E. Helvik for his help, guidance, support and for the conceptual ideas throughout the master thesis.

UNINETT have been an important factor for my thesis by providing the log of failure and reparation events in its backbone network. Thanks to Otto J Wittner, Arne Oslebo and Olav Kvittem in the lead from UNINETT.

My sincere thanks to Alex York for his great support in correcting my master's thesis.

Lastly, I would like to thank my family (Pramita Tiwari, Krishna R. Tiwari and Prabriti Tiwari) for all the support they have provided me over my thesis period.

Contents

Appendices

List of Figures

List of Tables

List of Algorithms

Nomenclature

CDF	Cumulative Distribution Function
DBPP	Dedicated Backup Path Protection
FFT	Fast Fourier Transformation
FIB	Forwarding Information Base
IS-IS	Intermediate System To Intermediate System
LDP	Label Distribution Protocol
LFIB	Label Forwarding Table
LSP	Label Switched Path
MLE	Maximum Likelihood Estimation
MPLS	Multiple-Protocol Label Switching
ms	milliseconds
MTTF	Mean Time to Failure
n.e.d	negatively exponentially distributed
PDF	Probability Distribution Function
PP	Path Protection
PR	Path Restoration
Q-Q	Quantile-Quantile
RIB	Routing Information Base
s	second
SDN	Software Defined Network
SLA	Service Level Agreement

Chapter 1
Introduction

1.1 Project Background

Backbone networks are central channels designed to carry network traffic at high speeds. These contain switches and network routers which are connected by Ethernet or fiber optic cables. Backbone networks are considered to maximize the performance and reliability of large-scale long-distance data communications. They are properly designed and sufficiently provisioned such that there are very low packet losses and insignificant queuing delays in the network.

Nevertheless, in the real world, failures occur in IP backbone networks as some previous studied have shown [22, 9, 13, 15]. Thus, the occurrence and effect of failures in such robust network designs have altered the attention of network providers. Failures in these networks may be physical: fiber cuts, power outages, fires and earthquakes. The failures may also be software failures or failures resulting from unintentional human errors [23]. The impact of such failures is extremely negative to the reputation of the network providers as well as millions of users who are dependent on the services carried out by these networks. Hence, a common policy is introduced known as a Service Level Agreement (SLA).

The SLA is a contract between the provider and receiver of the services where the stipulation of the availability to be guaranteed is established for a given period [10]. SLAs used by today's network providers are based mainly on five performance measurements: availability, packet loss, latency, jitter and maximum jitter (for example, see [1]). The providers cannot promise to provide uninterrupted services due to the inescapable failure events. Thus, the provider needs to mention the percentage of time that the offered service will be available. Delivering highly available services may incur high cost for the network provider due to high resources needed to be reserved or the penalties linked with the violation of the agreement. However, the promised availability by the network provider must be commercially competitive in order to gain popularity together with a profit. A significant amount of research has been invested at providing tools for an adequate SLA definition and efficient fulfillment [19, 10, 11, 6] due to the huge impact for network providers and their customers.

1.2 Problem Outline

The starting point of this thesis is to first define an SLA where the availability in a backbone network is guaranteed. Thereafter, assessing the availability to be stipulated in the SLA with resources that must be provided to guarantee the SLA requirement. This thesis works with real connection downtime data obtained from UNINETT's backbone network such that the results from this thesis can be further implemented in real world scenarios.

Different network recovery mechanisms are utilized to recover from network failures. This thesis will study in depth the recovery mechanism such as Dedicated Backup Path Protection (DBPP) and Path Restoration (PR) for end-to-end connections. There is DBPP; a very advanced recovery mechanism which is very reliable but expensive and there is PR that is more efficient in the resource utilization but not so reliable. Thus, the objective of this thesis is to propose such a technique which grabs the advantages of both recovery mechanisms and come up with an intermediate solution where the SLA requirements are fulfilled at an efficient cost. For this purpose, this thesis introduces a hybrid recovery mechanism in a backbone network for end-to-end connection failures inspired from the study made in [11]. This hybrid model is a combination of DBPP and PR.

In this thesis, various scenarios are considered in which the proposed hybrid solution can be implemented, where its specific capabilities are represented in terms of resource utilization and the probability of succeeding the guaranteed availability. The SLA risk assessment, which is based on a mathematical model that allows to have control over the probability that the accumulated downtime exceeds some threshold is modeled in a clear way such that it is easy to design a transition line to be used in a hybrid system. The transition line refers to the line that provides information about when the connection should switch between the Protection and the Restoration by knowing the status of its current accumulated downtime and the remaining SLA time.

With regards to the network connection, in this report the following terms are defined as:
Network connection: A group of interconnected links and routers which provide end-to-end service [12]. In this case, an end-to-end connection in a backbone network.
Network provider and customer: A network provider owns a network infrastructure providing connectivity among different points. A customer pays for the provided

connectivity. Both parties negotiate the limits and obligations of the service to be provided and define an SLA.
Single downtime: When a network connection is down.
Accumulated downtime: The total sum of all downtimes in the network connection throughout the SLA contract.
SLA availability requirement: The availability of the network connection throughout the SLA period defined in the SLA contract.
SLA risk: The probability of failing the SLA over the SLA contract period.
SLA risk target: The same as SLA risk but the provider can tune the risk target by using the advanced network recovery mechanism (e.g Protection) for more or less time.
Maximum allowed accumulated downtime: It is the threshold of accumulated downtime that is allowed before the provider violates the SLA and pays the penalty.

1.3 Research Questions

This masters project was carried out to answer the following research questions:
How to guarantee the SLA availability in a cost efficient way in a connection-oriented backbone network?

1.4 Limitations

The hybrid policy of recovery mechanisms in backbone networks is currently a new research topic, meaning that it is still in the starting phase of development, therefore many challenges and limitations can be met.

The thesis used discrete event simulation, mathematical modeling and the real data from UNINETT backbone networks. UNINETT is a state owned company responsible for Norway's National Research and Education Network. UNINETT has provided the measurement of data transmission in end-to-end connection of their backbone network. These data were needed in order to model the distribution of the connection downtime periods which uses PR. There were more than ten thousand failure logs[1] of UNINETT's network from years 2001 to 2013 among different cities in Norway. Due to the time limitation, there was no opportunity to go through all the failure logs of UNINETT's network. The result shown in this thesis are based on measurements made from January 2012 to July 2012.

---

[1] The failure logs of UNINETT referred to the log where all the down events are registered

1.5 Previous/Related work

The mechanism used to recover backbone failures (fault tolerance techniques) are hot research topics, where several approaches has been proposed [21, 19, 24, 25, 34]. Most of the common approaches for ensuring survivability when the failure occurs include Protection and Restoration mechanism at the optical layer and IP layer. This thesis contributes in providing a comparison of the different schemes (utilize either Protection or Restoration mechanism) for resource utilization. The schemes are compared by simulation.

Previous studies suggested to use Protection mechanism and in case of simultaneous failure using Restoration mechanism is a beneficial approach for two-link failure in a mesh network [30]. Some studies made in [30, 5] suggest the use of both Protection and Restoration mechanisms in order to recover from network failures. However, none of these studies or previous works based on a combination of Protection and Restoration has taken into the consideration of SLA risk assessment[2] and do not consider a dynamic and online combination of the two recovery mechanisms. The new concept introduced as well as the main contribution of this thesis is a hybrid recovery mechanism that considers dynamic and online combination of DBPP and PR such that network providers could get full control over the SLA risk and use only the resources that are needed. This concept was first introduced in [11] where the study proposed two hybrid policies to gain control of the SLA risk successfully by cost efficient tools in a cloud computing environment. This thesis will further study the implementation of those two proposed hybrid policies in end-to-end connections in backbone networks by using the real data of UNINETT's backbone network and considering 1 percent of SLA risk target.

The study in operational logs from UNINETT's backbone network is made in [22, 9, 13] to analyze the characteristics of router and link failures. This thesis is focused on end-to end path failure. It contributes on collecting and extracting the failure log of UNINETT's backbone (from January 2012 – July 2012) from Oslo to Trondheim and studies distribution of the connection downtime.

1.6 Methodology

This thesis focuses on creating a model which is robust, reliable, expandable and compatible using the recovery mechanism: Path Protection (PP) and PR. There has been many literature studies of network recovery and their possibilities. Moreover, trying to define a model based on the existing knowledge and experimenting with different scenarios.

---

[2] The SLA risk assessment is defined as the evaluation of the probability of failing or succeeding the SLA requirement over the contracted period

While working on this thesis an iterative series of steps have been considered. The steps are literature study, experiment and evaluation of the results. The list of definitions and notations used in this thesis is defined in appendix D.

The following guidelines were made on how to work on this thesis based on discussions with my supervisor, professor and my own reasoning:

1. Study network recovery in backbone networks to get familiar with the concept of network recovery mechanisms in backbone networks and their types; Protection and Restoration.

2. Study the Multiprotocol Label Switching (MPLS) and Software Defined Network (SDN) networks to gain knowledge about the latest network control technologies and whether the hybrid model is compatible with them.

3. Analyze the numerical concept of the distribution of the accumulated downtime, and the implications with the SLA which is further used to calculate the accumulated downtime of end-to-end connections with given SLA risk target over an SLA duration.

4. Collection of the failure logs of end-to-end connections from UNINETT's backbone network in order to model the realistic downtime distribution of end-to-end connections that uses PR. The failure logs are filtered using an AWK script to obtain the single downtime durations. The failure arrival and duration of the downtimes obtained from the filtered failure logs are evaluated in order to observe the failure characteristics of end-to-end connections. Through this evaluation, a probability distribution for connection downtime of PR is made and distribution fitting is performed with known distributions such as Weibull and Gamma. A fitted model of the connection downtimes from UNINETT's backbone is presented using a MATLAB tool called "dfittool".

5. Study the concept of Fast Fourier Transformation (FFT) and its utilization in non-parametric distribution. FFT is utilized in order to reduce the complexity of computing the convolution of downtimes.

6. Compute the accumulated downtime distribution of end-to-end connections that uses DBPP. The downtimes of DBPP are evaluated using the existing knowledge and study made in [31].

7. Evaluate the difference between accumulated downtime distribution model of end-to-end connections that uses DBPP and PR in order to see the gap between the DBPP and PR schemes. Mathematical tool "MATLAB R2013b" is used to compute and plot the downtime distribution model for PR and DBPP.

8. Introduce the hybrid model of DBPP and PR with two approaches: "Save and Spend" and "Spend and Save". The accumulated downtime for each approach with 1 percent SLA risk target is computed based on the result from accumulated downtime distribution of end-to-end connection that uses DBPP or PR.
9. The transition lines for each approach with 1 percent SLA risk target is calculated in Microsoft Excel based on the result of accumulated downtime of each approach.
10. Build a discrete event simulation on DEMOS platform using SIMULA as a programming language to probe whether the computed transition lines fulfill the SLA requirement, in this case 1 percent SLA risk target, at the end of the SLA contract.
11. Build a discrete event simulation to analyze the resource utilization by both approaches considering that the network provider needs to fulfill the SLA requirement resource efficiently.
12. Evaluate the resource utilization, thereby the total cost for providing the network with different SLA risk targets in order to find the optimal risk target which provides minimal cost.
13. Draw conclusions based on results obtained from discrete event simulations and resource and cost analysis.

1.7 Structure of the Project

This masters thesis has been organized in a structure which first introduces the background of network recovery; then the concept of SLA between a network provider and a customer; and then the research question of this thesis. After, it works on to the related work and literature evolving network recovery and fulfilling the SLA guaranteed availability. Following that, come the chapters involving the experiments and discussion of the research question: first, numerical analysis of accumulated downtimes distribution and the implication with the SLA; second, in-depth analysis of accumulated downtime distributions of end-to-end connections that uses PR schemes based on the data collected from UNINETT's backbone; third, in-depth analysis of accumulated downtime distributions of end-to-end connection that uses DBPP schemes. After analyzing downtime distribution of PR and DBPP, the thesis moves on to designing the hybrid model of PR and DBPP combined based on the downtime distribution analyzation. It will first introduce the two hybrid approaches "Spend and Save" and "Save and Spend" inspired from [11], then compute the accumulated downtime distribution for each approach using the downtime distribution of PR and DBPP made earlier, then drawing a transition line based on their accumulated downtime distribution with 1 percent SLA risk target for them. The hybrid approaches with the computed transition lines are simulated via discrete event simulation in order to see if they fulfill the SLA requirements. If both approaches succeed in fulfilling the SLA requirement verified from the simulation, a brief comparison between them on resource utilization is then presented. The hybrid approach that utilizes fewer resources is further analyzed with different SLA risk target in order to find the optimal SLA risk target that gives least cost to the network provider. Lastly, the thesis ends with a conclusion about the proposed hybrid approaches in end-to-end connections of backbone networks based on the obtained results and suggests some future works.

In detail, the paper is organized in the following chapters:

1.7.1 Chapter 2 – Network Recovery

This chapter briefly describes the types of network recovery mechanisms: Protection and Restoration. It quickly presents the differences between Protection and Restoration. Additionally, MPLS and SDN networks are briefly explained and compared. However, this chapter will not go into the details about MPLS and SDN network architectures, but rather focus on the implementation of Protection and Restoration in these architectures.

1.7.2 Chapter 3 – Computation of Accumulated Downtime Distribution

This chapter is divided into three main sections. The first section gives a brief numerical concept of probability distribution of accumulated downtime and the implications on SLAs. The second section goes through the study of the probability distribution of connection downtimes from the measured failure logs of UNINETT's backbone network that uses PR. It includes an explanation of the distribution of both failure arrivals and connection downtimes. The third section studies the probability distribution of the connection downtime which uses DBPP. An equation to compute the Probability Distribution Function (PDF) of the connection downtime using DBPP is proposed at the end of this section.

1.7.3 Chapter 4 – Hybrid Model - DBPP + PR

This chapter provides the description of hybrid approaches. The result obtained from chapter 3 is used in this chapter to compute the accumulated downtime distribution of hybrid approaches as they are a combination of PR and DBPP. It explains from computing the accumulated downtime distribution then drawing a transition line based on this distribution with 1 percent SLA risk target for each hybrid approach. The verification of whether the computed transition line of each approach fulfills the 1 percent SLA risk target over a SLA contract time is made via discrete event simulation. This chapter further provides the comparison between two hybrid approaches on resource utilization. In addition a brief study on optimal SLA risk target is presented.

1.7.4 Chapter 5 – Conclusion and Future work

Chapter 5 concludes the thesis. Some guidelines to future work are also mentioned in this chapter.

Chapter 2

Network Recovery

This chapter succinctly explains path recovery mechanisms: PP and PR. In addition, technologies such as MPLS and SDN are briefly explained in the context of this thesis. A brief comparison between MPLS and SDN is made in terms of network reliability, high communication speed and controlling the network. At the end, this chapter will analyze the use of PP and PR in MPLS and SDN. The goal is to find out if it is possible to utilize the proposed hybrid approaches efficiently in MPLS and SDN.

This thesis addresses the resilience of a network (known as network recovery) which enables a mechanism to react to failures and redirect the traffic from paths affected by failures to alternative, failure-free paths [23].

A broad variety of approaches have been researched and implemented for detection of network failure and its recovery. Prompted by the high requirement of reliability and high speed communication to be robust to failures in backbone networks, there are mechanisms which imply self-healing to automatically restore functionality. The study of self-healing networks is categorized into three different criteria [3]:

- Link rerouteing versus path (end-to-end) rerouteing.
- Centralized computation versus distributed computation.
- Precomputed versus dynamically computed routes.

Theoretically, the Protection mechanisms are precomputed at a single location so it is centralized. A Restoration mechanism is centralized when a central manager allocates a new path. Additionally, there are many recovery techniques in both Protection and Restoration such as PP and PR, channel Protection/Restoration, link Protection/Restoration and segment-Protection/Restoration [33], [25].

2.1 Recovery Mechanism - Protection and Restoration

Restoration techniques seek to establish a new path after a failure has occurred without any prior resource reservation. In Restoration mechanism the backup path[1] is computed on demand, i.e., it can be either preplanned or dynamically allocated, however resources required by the backup paths are not allocated or reserved until a failure occurs. This yields relatively long recovery times and a path with sufficient resource capacity cannot be guaranteed. Using Protection techniques, the backup path is pre-computed and resources usage are pre-allocated either dedicated for each connection or shared. The Protection techniques yield faster recovery and (almost) guaranteed capacity at the cost of higher resource usage. The classification of Protection and Restoration mechanisms based on resource usage and path allocation are illustrated in figure 2.1.

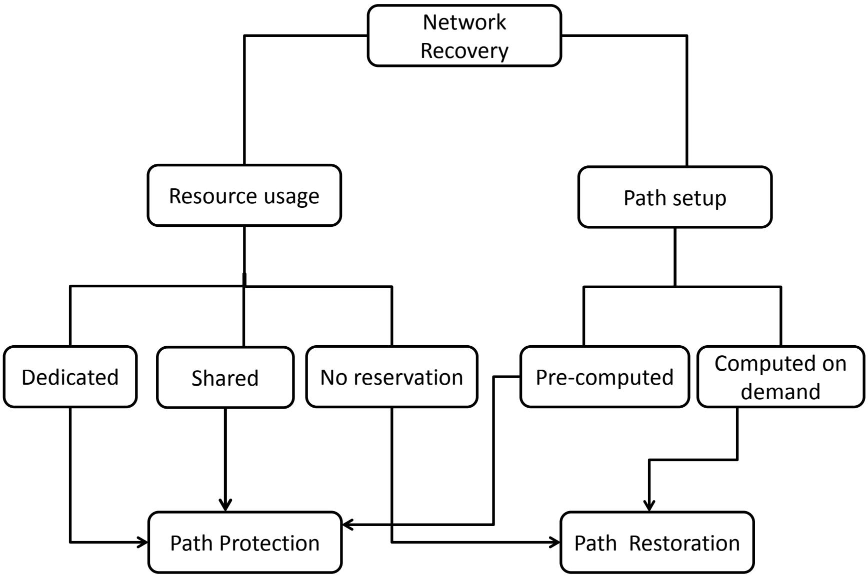

Figure 2.1: Overview of network recovery mechanisms

---

[1] Backup path refers to alternative path of a network.

2.1.1 Path Protection

PP is an end-to-end Protection scheme used in telecommunication networks against failures. If the failure occurred at any point along the path of a network, the end nodes will move the traffic to or from an alternate route.

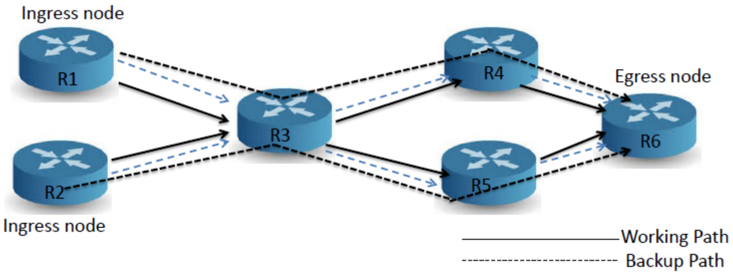

Figure 2.2: Illustrates the end-to-end DBPP

In figure 2.2 and 2.3 the blue lines represent the connection in the end-to-end network. There are many types of PP in a network but the type of PP focused in this thesis is DBPP.

Dedicated Backup Path Protection

In general, a dedicated backup path refers to a backup path which corresponds to one particular working path[2]. In DBPP, each working path has one dedicated backup path and both the working path and backup path carry the traffic end to end [33] shown in figure 2.2. The receiver thus chooses either one of the two incoming traffic. DBPP is known to be the fastest currently available Protection scheme because there is no involvement of signaling between source node[3] and destination node[4]. Therefore, the destination node only needs to detect the failure and switch the traffic over to the backup path. The study [31] has proved that DBPP can provide the protection in a backbone network within 50 milliseconds.

Providing DBPP to all users is however very demanding for the network provider in terms of bandwidth usage and cost. Keeping in mind the thesis' research objective, a mechanism which can fulfill the availability demanded in the SLA and at the same time keep the bandwidth usage as low as possible is needed. Hence, the target is to utilize DBPP scheme as infrequently as possible while designing the hybrid model.

---

[2] Working path refers to primary path of a network.

[3] Ingress node.

[4] Egress node.

2.1.2 Path Restoration

In PR each interrupted or failure path is independently rerouted over one or more available paths between the source and the destination node (using the spare or available capacity of the network) [34] shown in figure 2.3. PR is considered to be more bandwidth efficient compared to DBPP. The cost of transmission using fibers or cables are still considered the main cost in nation-wide transport networks, thus PR appears to be appealing for backbone networks.

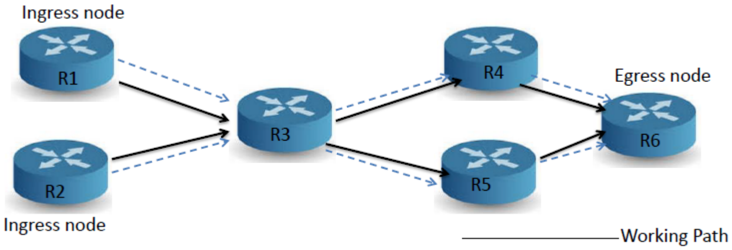

Figure 2.3: Illustrates the end-to-end PR

The target of this thesis is to achieve DBPP-like recovery speed and PR-like bandwidth usage through the hybrid model, in order to fulfill the SLA availability guarantees in a backbone network.

2.2 Multiprotocol Label Switching (MPLS) vs Software Defined Network (SDN)

MPLS and SDN are the technologies to provide mechanisms that control the forwarding of packets over the network. When failure occurs in the routed networks, MPLS and SDN recovery must assure that traffic can continue to flow with the same quality as before the failure. Hence, the networks needs to detect a failure and switch over to a alternate failure free path. In order to respond to failure events and switch the traffic path, the control plane in the network architecture is needed. SDN and MPLS implements the control plane to react to failure events in the backbone network.

The control plane, the data plane and the management plane are the three fundamental components of a telecommunications architecture [29]. The data plane carries the traffic in the network and is managed and controlled by the management plane and control plane respectively [29]. It transfers the data to and from the clients, handling multiple conversations through diverse protocols. The control plane is responsible for routing the traffic [28]. It has a function for management and system configuration. The basic overview of control plane and data plane can be seen in figure 2.4.

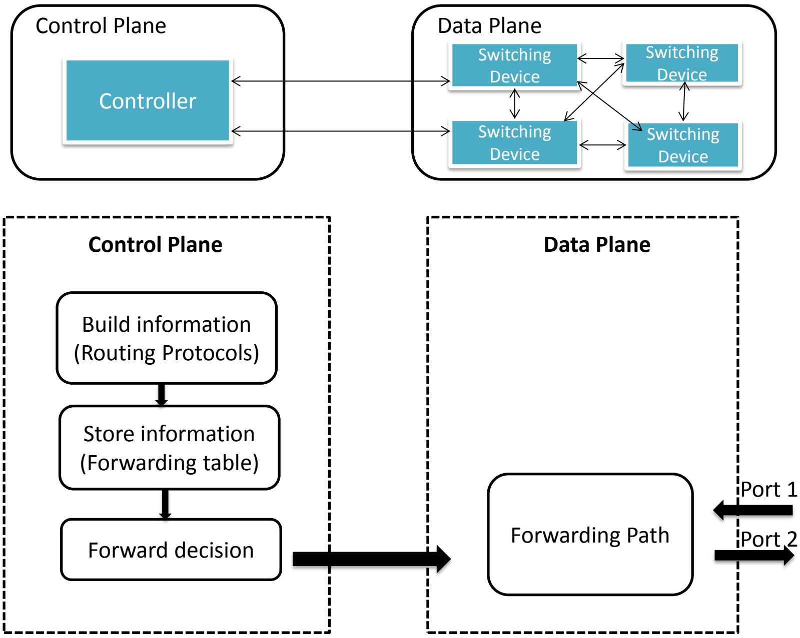

Figure 2.4: Overview of control plane and data plane

2.2.1 Control Plane and Data Plane in MPLS Networks

Inside the control plane of MPLS networks, there is the routing protocol, IP routing table (Routing Information Base (RIB)) and Label Distribution Protocol (LDP). The control plane consists of a mechanism to exchange routing information (OSPF, IS-IS) and labels (BGP, TDP). MPLS has a distributed control plane i.e. intelligent on each router. The responsibility of a routing protocol is to build the RIB. LDP is an important protocol in MPLS which creates, maintains and distributes the labels of MPLS. The data plane contains an IP forwarding table (Forwarding Information Base (FIB)) and a Label Forwarding Table (LFIB). It is responsible for forwarding packets based on IP header and labels.

In MPLS, the first device (for instance router) does a routing lookup and finds the final destination router by knowing the predetermined path from initial to final router, unlike the traditional IP networking method which determines a next-hop and forwards the packet to that next-hop. In MPLS, the router uses the label to route the traffic without needing to perform additional IP lookups. This saves the time needed for the router to look for the address of the next node where the packet will be forwarded to. The label is removed by the final router at the final destination (end of label-switched path (LSP)). Then the packet is delivered via normal IP routing. An LSP is required for any MPLS forwarding to occur.

2.2.2 Control Plane and Data Plane in SDN Networks

An SDN network separates the data plane from the control plane and instead implements the control plane in software enabling the programmatic access which makes network administration more flexible.

The concept of SDN is to have a centralized control network in a control plane which provides the centralized view of the overall network. The routers/switches in SDN do not have intelligence and depend on the central controller. Through the centralized controller, network administrators make the decision quickly on how the routers will forward the traffic in the data plane. Currently, the most common protocol used in SDN networks for communicating between the centralized controller and the routers is OpenFlow. OpenFlow is an open standard for a communication protocol that enables the centralized controller to interact with the forwarding routers [2].

If a link goes down, multiple packets will be lost before the network has time to reroute the traffic to another link. In SDN networks the concept of a group table enables the network to adopt DBPP [31]. It has the technique that enables the switch itself to take control of the data traffic, thus no need to contact the controller each time in case of a failure in the link.

2.2.3 Comparison Between MPLS and SDN

The key diference between MPLS and SDN is that MPLS can operate with a distributed control, but SDN uses a centralized control. The big advantage of SDN over MPLS is allowing dynamic access and administration of the network. It allows a network administrator to analyze the traffic and set up services to address changing business requirements, without going through each individual router while forwarding in the data plane. In addition, SDN has the possibility to be reprogrammed in a very flexible way given that it is open.

Taking fault tolerance techniques into account for MPLS and SDN networks, several approaches has been made in [27] [31]. They clarify that both Protection and Restoration mechanisms can be implemented in MPLS and SDN networks. The question is whether the hybrid model can be implemented in MPLS or SDN. By observing the dynamic monitoring and switching characteristics as well as open nature of an SDN network suggests that the hybrid model is implementable. The study made in [14] suggests that the hybrid of Protection and Restoration is also implementable in an MPLS network. This study proposed a hybrid algorithm of Protection switching and dynamic path rerouteing with consideration of fault recovery time, packet loss, packet reordering and tolerance of multiple faults. By observing these facts, it may be assumed that the proposed hybrid model in this thesis is compatible in both MPLS and SDN. In theory the hybrid model proposed in this thesis might be easier to implement in SDN because of its central brain making the information process easier, however SDN has the disadvantage of depending on a central system. In this case MPLS has a better architecture as the intelligence of network controlling is distributed.

Nevertheless, this is not a main concern of this thesis, but just given a brief observation and analysis of currently popular networks and whether they can utilize the proposed hybrid model.

Chapter 3

Computation of Accumulated Downtime Distribution

This chapter analyzes the distribution of the accumulated downtime both theoretically and numerically. The chapter is divided into three sections where each section provides valuable results and analysis. Each section provides the study on the following topics:

1. A numerical concept on the distribution of accumulated downtime, and the implications on SLA.
2. Distribution of the end-to-end connection downtime when PR is utilized. For this, a downtime data of UNINETT's backbone is taken such that a realistic scenario can be considered.
3. Distribution of the end-to-end connection downtime when DBPP is utilized.

The objective of this chapter is to obtain the distribution of accumulated downtime when the connection uses PR and DBPP respectively and to observe the difference in accumulated downtime over a time period between PR and DBPP. The result obtained from this chapter will be used in chapter 4 to compute the downtime distribution of hybrid approaches as they are combination of PR and DBPP.

3.1 Numerical analysis of distribution of accumulated downtime - Part 1

Probability distribution of accumulated downtime $D(t)$ and single downtimes $h_n(t)$ shown in figure 3.1 is studied thoroughly in this chapter. A study [7] has shown that assessing the probability that the accumulated downtime will be bigger than the guaranteed SLA availability based on expected values is a risky option, and that a tool that considers the entire stochastic behavior of the network is needed. The network providers have to consider the entire probability distribution of the accumulated downtime with the intention of fulfilling the guaranteed SLA availability. Therefore, a numerical method to estimate the probability distribution of the accumulated downtime of the network has to be considered.

The accumulated downtime over the SLA duration (τ) is associated with the interval availability of the network. The interval availability $A(\tau)$ is a stochastic variable which measures the time that a network is available/working during τ [7]. The accumulated downtime $D(t)$ at time t measures the total time that a connection has been down at interval $0 - t$. The Cumulative Distribution Function (CDF) and PDF of $D(t)$ over an SLA duration τ will be defined as $\Omega(\tau, t)$ and $\omega(\tau, t)$ respectively. The general expression for $\Omega(\tau, t)$ and $\omega(\tau, t)$ is derived from the approximation of the Tacakas equation [32].

$$\Omega(\tau, t) = \sum_{n=0}^{\infty} H_n(t)[G_n(\tau - t) - G_{n+1}(\tau - t)] \tag{3.1}$$

And the approximated equation from [11] to determine the PDF of the accumulated downtime is equation 3.2.

$$\omega(\tau, t) = \sum_{n=0}^{\infty} P(N(\tau) = n) h_n^*(t) \tag{3.2}$$

In equation 3.1, the failure and repair processes are described by independently and identically distributed (i.i.d) uptime and downtimes with CDF $G(t)$ and $H(t)$ respectively [11], where n represents the n-fold Stieltjes convolution [7]. The PDF of the total accumulated downtime is given by the n-fold convolution $h_n^*(t)$ illustrated in figure 3.1.

The n-fold convolution posed the convolution for calculating specific failure and repair processes. The $\Omega(\tau, t)$ in equation 3.1 is an approximation for general distribution of short intervals. However, the SLA duration is normally several months or a year. Thus, the distribution should be considered for several months. The duration of each down event (when a failure occurs) is assumed to be i.i.d. A deterministic number of down events is considered when $t = \tau$. The realization of accumulated downtime $D(\tau)$ in the connection is the sum of realization of each single downtime ($D(t) = h_1 + h_2 + h_3 + \ldots + h_n$). Thus, the PDF of $D(t)$ denoted as $\omega(\tau, t)$ can be expressed by the convolution $h_n^*(t) = h^1(t) * h^2(t) * h^3(t) * \ldots * h^n(t)$ as demonstrated in figure 3.1. Hence, if the number of down events is known, the PDF of accumulated downtime $\omega(\tau, t)$ can easily be defined.

Note that equation 3.2 considers all possible scenarios (zero failure, single failure, multiple failure). Each scenario has a probability $P(N(t) = n)$. When there is zero failure, n equals 0, i.e., no down events. Or n equals 1 where there is a single failure

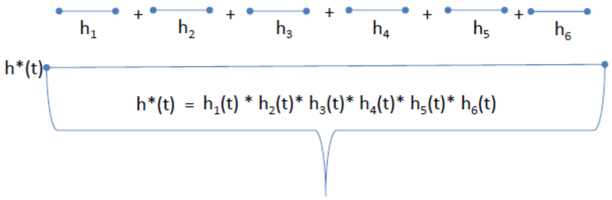

Figure 3.1: Convolution $h_n^*(t)$ and a distribution of the accumulated downtime of six down events

over the SLA duration. For this case, the distribution of a single downtime is applied. Only in the case where there are multiple failures, i.e., $n \geq 2$, the distribution of the sum of total downtimes is applied and computed using convolution.

Based on the study made in [11], for computation of $\omega(\tau, t)$, stochastic characteristics of a number of down events are considered. The downtime duration is assumed to be extremely small compared to the duration of uptimes. Thus, the probability of n downtimes during τ, $P(N(\tau) = n)$ in equation 3.2 can be approximated only by the uptime distribution of the networks $g(t)$. $P(N(\tau) = n)$ can be found by using renewal theory and counting models [7].

The approximation made in [11] simplifies the complexity of equation 3.2 by dividing $P(N(\tau) = n)$ and $h_n^*(t)$ into two problems. By making the convolution of only the downtime distribution at first and then obtaining $P(N(\tau) = n)$, which is lead only by the uptime distribution $g(t)$. The numerical analysis made in this section is used to examine the PDF and CDF of Restoration and Protection downtime models.

3.1.1 SLA Risk and Success Probability

SLA was defined in the introduction chapter as where the provider guarantees an availability α for a given SLA duration τ. It is important for the provider to know the probability that the availability after τ will be higher than or equal to the specified availability guarantee.

In this thesis, the SLA success probability $S(\tau, \alpha)$ is the probability that a provider fulfills the SLA availability guarantee α over the SLA duration τ. Whereas, the SLA risk $(1 - S(\tau, \alpha))$ is defined as the probability that α will not be met over τ.

Figure 3.2 shows the PDF of interval availability $A(\tau)$ which represents the time that the connection has been up during τ. The PDF of $A(\tau)$ changes according to the duration of SLA. The $A(\tau)$ is one until the first down event occurs. The number

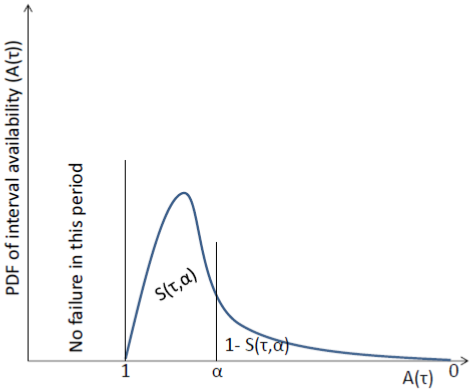

Figure 3.2: An overview of success and risk probability of SLA over τ

of down events is acceptable in the SLA duration until it passes the threshold of α. The SLA risk target is the value that represents the probability for failing the SLA. If the risk target is 1 percent, that means that the probability of failing the SLA availability requirement will never be bigger than 1 percent. This thesis will provide the tools to network providers in order to have controlled risk targets, using network resources efficiently.

After the numerical analysis of accumulated downtime distribution and SLA risk assessment, the study will further move on to describing the characteristics of end-to-end connection downtime events when recovery mechanisms such as PR and DBPP are used respectively.

3.2 Restoration Model

The investigation in this section is based on network data transmission logs made available by UNINETT. The examination is made of the distribution of failure arrivals and connection downtime from the measured data of UNINETT's backbone network which uses Restoration mechanism. The objective is to fit the observed empirical data with well-known distribution such that its replication can be used in further studies.

3.2.1 UNINETT Log Description and Analysis

The core of the UNINETT network interconnects to the main cities in Norway through optical fiber connections (2.5 and 10 gigabit per second) [9]. In this thesis, the set-up of network measurements contain two measurement nodes located inside Norway; one node located at the UNINETT facility in Trondheim (Academic And

Research Institutions) with IP address 158.38.0.230 and one at the UNINETT facility in Oslo (UNINETT, The Norwegian University & Research Network) with IP address 129.240.100.122. More details on UNINETT topology can be read in UNINETT [4]. A UDP packet is sent every 10ms from the source node (Oslo) to the destination node (Trondheim). IS-IS routing protocol is used for internal routing. This means that a Restoration scheme is utilized to recover UNINETT's backbone network. Therefore, it is possible to model the downtime distribution of the Restoration mechanism using UNINETT's dataset.

Logs provided by UNINETT are available since January 2001, however, the data that will be used in this thesis is chosen from January 2012 to July 2012 because the core network and its topology did not undergo any relevant changes, making it likely that the processes are uninterrupted during this period. Only UDP packets were chosen because of the difficulties in tracking the sequential number of TCP packets when it is lost. The downtime duration in the backbone are registered with a precision of seconds and milliseconds. Rude/crude is the program which was used to generate and receive packet streams [17].

The log provided by UNINETT contains summaries of events of each day on raw rude/crude data. The log contains the ID of the network, the packet sequence number, IP address of the source node and destination node and the size of the packets. Timestamps of both when the packet was transmitted from the source node and when the packet was received at the destination node is also registered in the log so that packet delay and loss duration can be obtained. Each log was filtered to obtain the downtime duration using AWK scripting in LINUX. The AWK script used in thesis is provided in appendix C. The obtained results were verified with the employees from UNINETT who were responsible for capturing the data and creating the log.

Since the data collected from UNINETT is empirical data, in order to explain the distribution of downtime, it is useful to first look at empirical probability distribution function. The fitting procedure of empirical data is explained in section 3.2.5.

3.2.2 Empirical Distribution Function

Empirical distribution is a distribution whose parameters are the observed values in a sample of data[26]. An empirical distribution can be used in cases where it is impossible or unnecessary to determine any particular parametric distribution of random variables.

The PDF of empirical distribution in this thesis will be analyzed by hypothesizing a distributional form for the downtime data by comparing the shape of PDF to a histogram of the data and understanding if this could relate to a known distribution.

3.2.3 Distribution of Failure arrivals

Failures in the network can happen for many different reasons at various protocol layers as briefly described in the introduction chapter. The expected availability time during the months January – May is consistent, but the months June and July have large occurrence of failure as shown in figure 3.3. The occurrence of each failure observed was 12 to 15 days on average. The reason behind the large amount of packet loss in the months of June and July could have been due to network components such as routers or optical fibers shared by multiple links, meaning a failure in one link would effect many links. Therefore, it was observed that when failure occurs in the network, the packets tended to be lost often on that particular day creating a delay in sending the next packets to the destination. As a result, more downtime duration was registered on particular days whereas no downtime duration was registered on other days. However, in general the failure arrival times seemed to be independent of other failure arrival times.

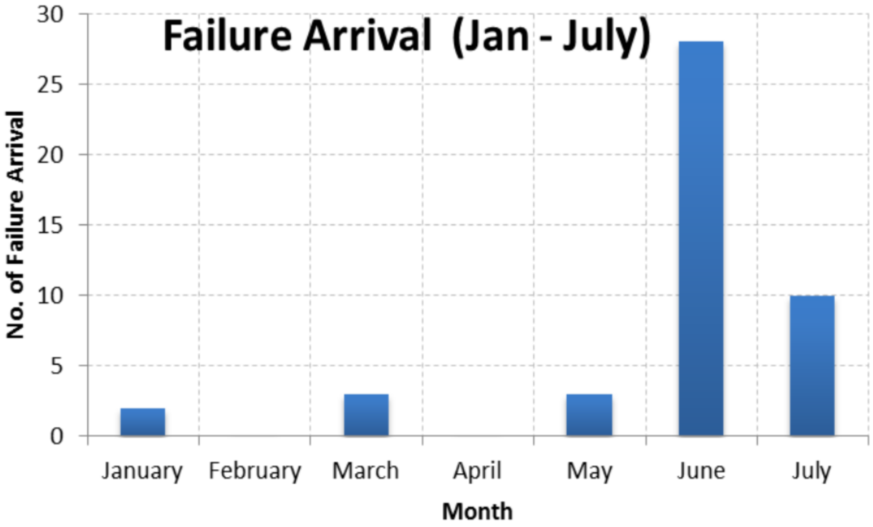

Figure 3.3: Failure Arrival from January to July in UNINETT's backbone network

In figure3.4, the purple line denotes the empirical data and red line denotes the CDF of exponential distribution. One can observe that the empirical data slightly fits with the exponential distribution when bother of their CDF are compared.

Karagiannis et al [16] studied the possibility of modeling IP backbone traffic as Poisson packet arrivals at various time scales. The observation of failure arrival in this research are stochastic and independent of other failure arrival times and approximately fitted with exponential distribution, indicates that the failure arrival in

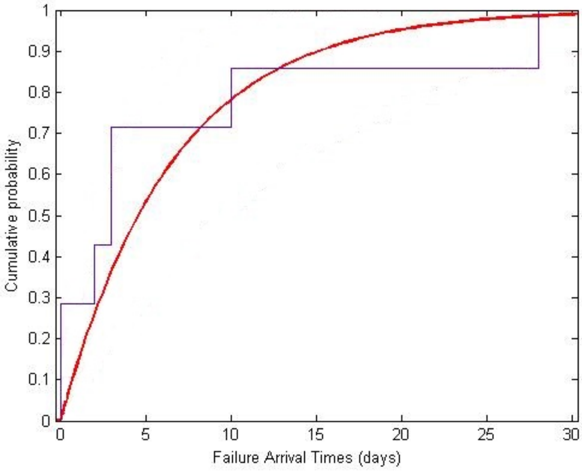

Figure 3.4: Fitting the inter-arrival times of failure with exponential distribution

the provided UNINETT's backbone can be a Poisson process. However, the data set observed is very small to prove that statement and show that the time between each failure arrival is exponential distribution. Nonetheless, for the analytic simplicity, Poisson is regarded as an accurate way to model failure arrival based on [16] and some observation made from the figure 3.4.

3.2.4 Distribution of end-to-end connection downtime

The UNINETT's backbone network relies on IP layer restoration via IS-IS protocol for failure recovery. It is considered that reasoning or concluding the causes from the observed IS-IS failures is a difficult reverse engineering problem [15]. Therefore, it is difficult to define exact causes of downtime events from the failure log of UNINETT's backbone. When multiple lost packets are detected in the network, it is assumed that there is a down event. Downtimes with duration longer than one hour are due to planned maintenance or links being decommissioned rather than to accidental failure, therefore those failures are excluded in this research.

The general behavior of an end-to-end network connection with downtime durations h_i and uptime durations g_i is shown in figure 3.5. The failure i ($i = 1, 2, \dots, n$) (where n is total number of failures) occurs at time t_i.

Obtaining the Down Events from the Failure Log

As mentioned earlier, the UNINETT's data transmission log contains ID of the network, packet sequence number, IP address of source node and destination node,

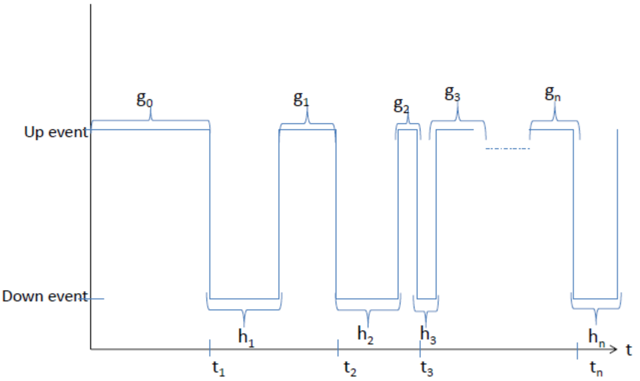

Figure 3.5: End-to-end network connection downtime [19]

the size of the packets and timestamps of a packet transmission and arrival. Using the information provided in the log file, the following steps were performed in order to obtain a downtime duration:

1. The packet sequence number, transmission time and receiving time are extracted from the log file.
2. If the difference between the previous and current packet sequence number is greater than two, the down event is registered in the log referred as failure log. The failure log contains all the down events with its timestamps for packet transmission, packet arrival and next packet transmission.
3. The downtime duration is then computed from the difference between the time of packet arriving at the destination node and the time when next packet is send from the source node.
4. The process is iterated for each log file[1]. Note that the extraction and filtration of the log file is made using AWK script presented in appendix C. The list of down events from January to July, 2012 is shown in table 3.1.

Table 3.1 shows a quick summary of the observed downtime period from January 2012 to July 2012. One can see that the downtime duration between the range of 10s to 1s has the highest number of events. By this, it can be assumed that the probability distribution of end-to-end connection downtime will be highest between 10s to 1s. Moreover, the downtime duration is directly proportional to the number of packet loss as seen in figure 3.6. It is approximately ten times the number of packets

---

[1] The log file contains summaries of events of each day generated by rude/crude software

Downtime duration	Number of events
60s – 10s	7
10s – 1s	23
1s - 100ms	12
100ms – 50ms	4
Total number of events	46
Total downtime duration	264s

Table 3.1: Summary of downtime duration from UNINETT log

lost or dropped. For instance, if there are 10 missing packets then the duration of downtime is around 93-100 milliseconds, similarly if there is 50 packets missing then the downtime duration is approximately 500 milliseconds. One can use this pattern to calculate the downtime duration of any number of packet loss.

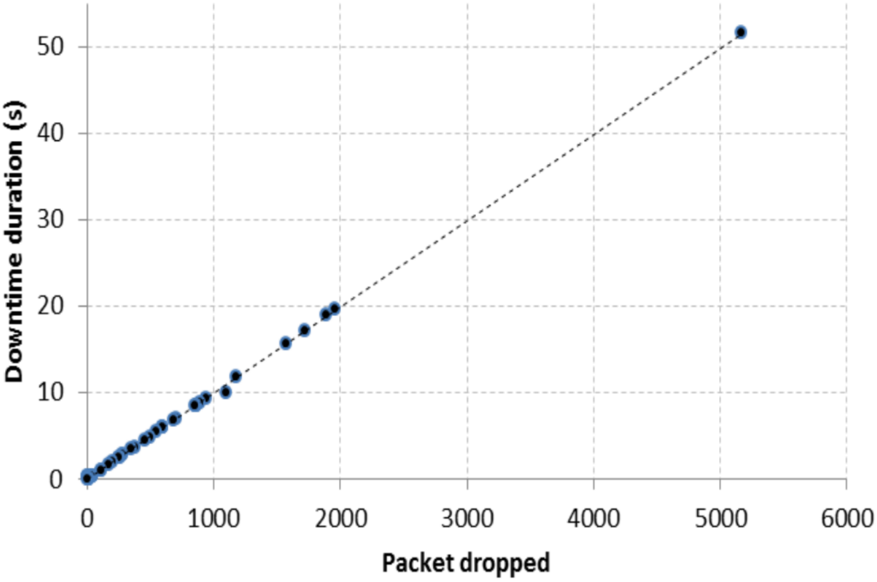

Figure 3.6: Number of dropped packets proportional to the downtime duration

The studies [8], [18] have proposed that the failure processes and repair processes can be modeled by Weibull distribution and Gamma distribution. Another study in [20] suggested that Weibull or two-staged hyper-exponential are convenient distributions to estimate the time between failures and times to repair for elements in a large wireless telecommunication network. To support if these known distributions are capable of modeling the downtime data from UNINETT's backbone network, distribution fitting has to be made. The method for distribution fitting is explained in section 3.2.5.

3.2.5 Distribution Fitting of Downtimes

The fitting techniques are described in this section for estimating the parameter distributions. The verification of the downtime data filtered from the UNINETT's failure log to be modelled by Weibull distribution and Gamma distribution is presented using Quantile-Quantile (Q-Q) plot with parametric distributions. For this MATLAB "dfittool" is used.

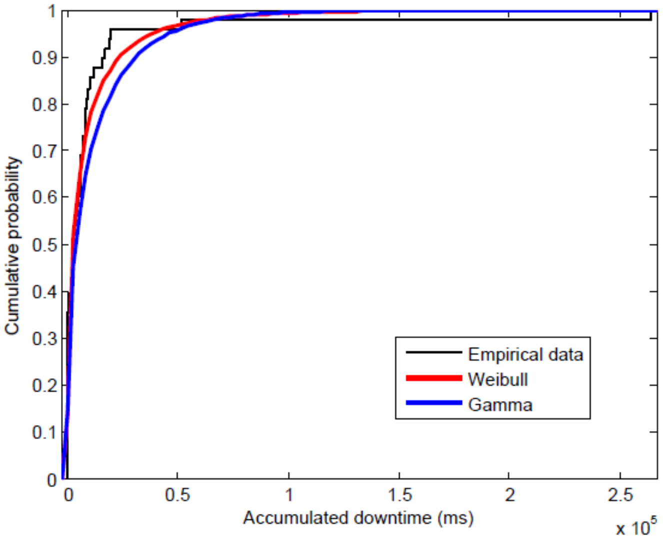

Figure 3.7: Fitted Distribution with Weibull and Gamma

Figure 3.7 shows an example describing the behavior of downtime durations of UNINETT's backbone. It shows maximum likelihood estimation (MLE) for Weibull and Gamma distributions.

From figure 3.7, it can be observed that only Weibull distribution is convenient to model the downtime distribution of failure log data provided by UNINETT as its tail is closer to the tail of the empirical data than the tail of Gamma distribution. The distribution of Restoration downtime model is therefore approximated by using MLE of Weibull distribution with scale and shape parameters of 5079.97 ms and 0.54 respectively. Thus the PDF and CDF of Weibull distribution is utilized in this thesis to study the accumulated downtime distribution with PR.

Weibull Distribution
Probability Density Function

$$h(t) = \begin{cases} \frac{\theta}{\beta}(\frac{t}{\beta})^{\theta-1}\exp^{-(\frac{t}{\beta})^{\theta}} & t \geq 0 \\ 0 & t < 0 \end{cases}$$

Cumulative Distribution Function

$$H(t) = \begin{cases} 1 - \exp^{-(\frac{t}{\beta})^{\theta}} & x \geq 0 \\ 0 & t < 0 \end{cases}$$

where β is the shape parameter and θ is the scale parameter in time units.

3.3 Protection Downtime Model

In this section, a method to evaluate the distribution of the accumulated downtime with Protection scheme is studied.

The study [31] states that the downtime distributions of DBPP is uniformly distributed between 40 to 50 millisecond. Since DBPP mechanism uses its backup path when the working path fails, the study [13] shows that there is a possibility of simultaneous and potentially correlated failures in routers and links of an IP backbone network because of random and overlapping data traffic. For that case, the connection might need to wait for the working path to be repaired. This might take a relatively long time (around an hour) for the path to be fully recovered and carry the traffic which would lead to a disaster in terms of availability in the network. Hence to cope with such a situation, a connection using DBPP should also use the available path in its network and not only its dedicated backup path. This means DBPP scheme should perform like PR which chose an alternative unaffected available path in case of failure. The study made in [30] suggests that in case of simultaneous failure in working path and backup path of a network using Protection scheme, applying a dynamic rerouteing nature of Restoration which can quickly restore the traffic by computing the backup path around the failed link is a beneficial approach.

Proposal of Equation for Distribution of Downtime with DBPP

To calculate the PDF of downtime distribution with DBPP scheme, two conditions are chosen:

- **Perfect condition:** No simultaneous failure in the connection.

- **Flawed condition:** Simultaneous failure of working path and backup path in the connection. In this case the connection behaves like PR.

Notations	Explanation
$\omega_{PR}(\tau, t)$	PDF of connection downtime with PR^2
$\omega_{DBPP}(\tau, t)$	PDF of connection downtime with DBPP with perfect condition
ω_c	PDF of connection downtime with DBPP whwn both condition applied
$\Omega_{PR}(\tau, t)$	CDF of connection downtime with PR
$\Omega_c(\tau, t)$	CDF of connection downtime with DBPP when both condition applied
PS	Probability for flawed condition (simultaneous failure

Table 3.2: Notations used in this section with its explanation

It is assumed that $\omega_{DBPP}(\tau, t)$ which is the perfect condition is the delimited uniform distribution between 40 to 50 ms based on the study made in [31]. The equation for $\omega_c(\tau, t)$ providing the fact that if there is simultaneous failure DBPP acts like PR else it recovers the failure within 50 ms, is presented as the following:

$$\omega_c = PS \times \omega_{DBPP}(\tau, t) + (1 - PS) \times \omega_{PR}(\tau, t) \tag{3.3}$$

Note that ω_{PR} is approximated as a PDF of Weibull distribution with 5079.97 ms and 0.54 of scale and shape parameter respectively, based on the result from section 3.2.5. The $\Omega(\tau, t)_{DBPP}$ and $\Omega(\tau, t)_{PR}$ can be seen in figure 3.8.

In figure 3.8 the red line represents $\Omega(\tau, t)_{DBPP}$ whereas the blue line represents $\Omega(\tau, t)_{PR}$. Figure 3.8 illustrates that there is a big gap in accumulated downtime between PR and DBPP. This is one of the motivations for making the hybrid of both recovery mechanisms to find the balanced accumulated downtime over an SLA duration.

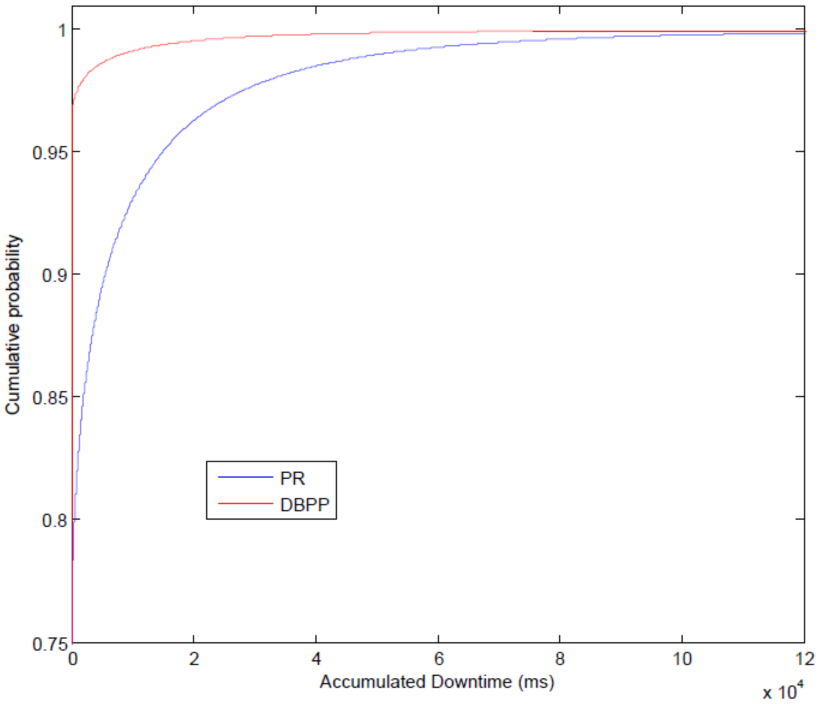

Figure 3.8: Comparison between PR and DBPP

Chapter 4
Hybrid Recovery Mechanism

This chapter gives a full description of the hybrid model proposed in this thesis. Two approaches "Save and Spend" and "Spend and Save" suggested from [11] are analyzed in detail to be used in backbone networks. The computation of distribution of accumulated downtime using both approaches, thereby calculating a transition line for them with 1 percent SLA risk target is explained in detail. The theory of FFT is used to compute the accumulated downtime of the two approaches. The hybrid model is simulated in real case scenarios with the given transition line. This transition line plays a key role in the hybrid model since it provides the information to the system about when to switch between DBPP and PR. The transition frontier with 1 percent SLA risk target is verified via discrete event simulation in DEMOS. The objective of this chapter is to solve the question - Will the computed transition line of each approach succeed in fulfilling the SLA availability guarantee efficiently with respect to resources?.

4.1 Hybrid Model Description

The word hybrid as described in Oxford dictionary is something of mixed origin or composition. In the context of this thesis hybrid is a combination of two different recovery mechanisms: DBPP and PR that switches from DBPP to PR and vice versa over the SLA duration according to the current network connection state (i.e. the remaining time of the SLA and current accumulated downtime) at a given time t. The switching between DBPP and PR is decided according to the three defined zones illustrated in figure 4.1. When failure occurs and the accumulated downtime reaches near to the threshold of the SLA risk target, the connection using PR at the beginning of the SLA duration must switch to the advanced and highly reliable mechanism DBPP in order to survive from crossing the SLA risk target. This zone is denoted by the color red. The zone where the probability of violating the SLA requirement is lower, thus the provider uses PR with consideration of resource utilization, is denoted by the color blue. The zone where the probability of violating the SLA requirement is neither high nor low, thus the provider have the flexibility to choose any technology that it wants, is denoted by the color green. These areas are obtained after a numerical analysis made in MATLAB, using the concepts presented in section 3.1. The graphic demonstration of the hybrid solution is shown in figure 4.1. The lines in figure 4.1 represent the replica of transition lines.

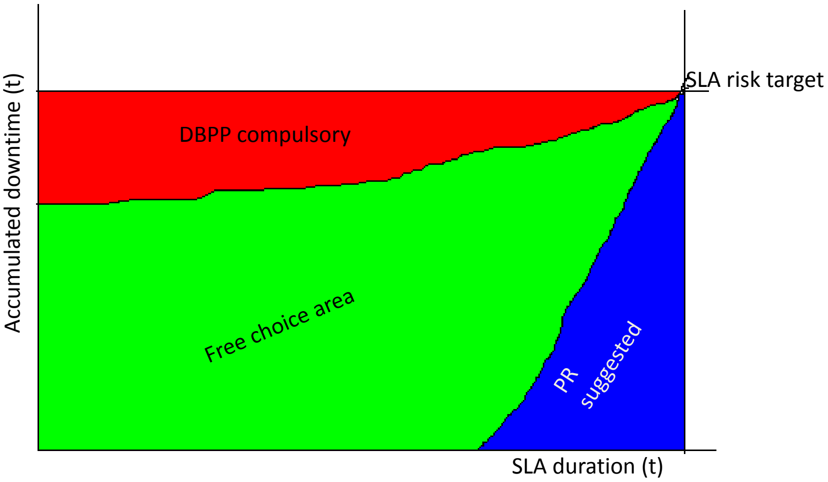

Figure 4.1: Design of proposed hybrid solution illustrating the transition lines with three zones

In figure 4.2, the flow chart illustrates an example of the process of switching in the hybrid model that uses PR at the beginning of SLA contract period. First the failure is detected in the network, then the accumulated downtime is computed and registered. At time *t*, there will be remaining downtime budget. The downtime budget refers to the remaining maximum allowed accumulated downtime in SLA. This risk of failing and succeeding the SLA is computed using the registered accumulated downtime and remaining downtime budget. If the registered accumulated downtime is in the red zone, meaning the renaming downtime budget is extremely low, the provider will switch to DBPP, otherwise it will continue using PR. Numerical analysis is needed to calculate the remaining downtime budget. The numerical analysis of the hybrid solution is explained in upcoming sections.

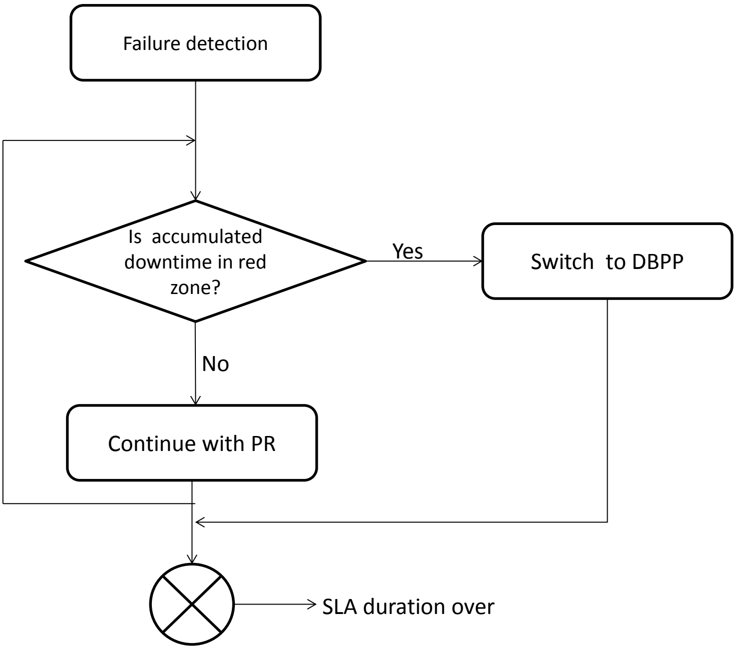

Figure 4.2: Flow chart for the proposed hybrid solution that uses PR at the beginning

4.2 Two Approaches of Hybrid Solution

The phase which uses DBPP is as denoted as the word "Save" and the phase that uses PR is denoted as the word "Spend" in this thesis. The following section 4.2.1 4.2.2 will explain in detail about the two hybrid solutions: "Save and Spend" and "Spend and Save".

4.2.1 Save and Spend

The Save and Spend (Save-Spend) solution will start using the DBPP scheme at the beginning of the SLA duration. Hence, the initial phase in this solution is called save, since the probability of the accumulated downtime to cross the SLA risk target is very small [11]. Note that the use of DBPP demands double the resources compared to PR so it is a more expensive mechanism. Thus, switching to PR which is a *spend* phase is an attractive approach. The transition from DBPP to PR can be done easily with the help of computed transition line.

4.2.2 Spend and Save

The Spend and Save (Spend-Save) solution will start using the recovery mechanism PR at the beginning of the SLA duration so the initial phase in this solution is called spend due to the high probability of obtaining an accumulated downtime bigger than SLA risk target [11]. Thus, to reduce the risk of failing the SLA, the connection should switch to DBPP considered as a *save* phase for recovery.

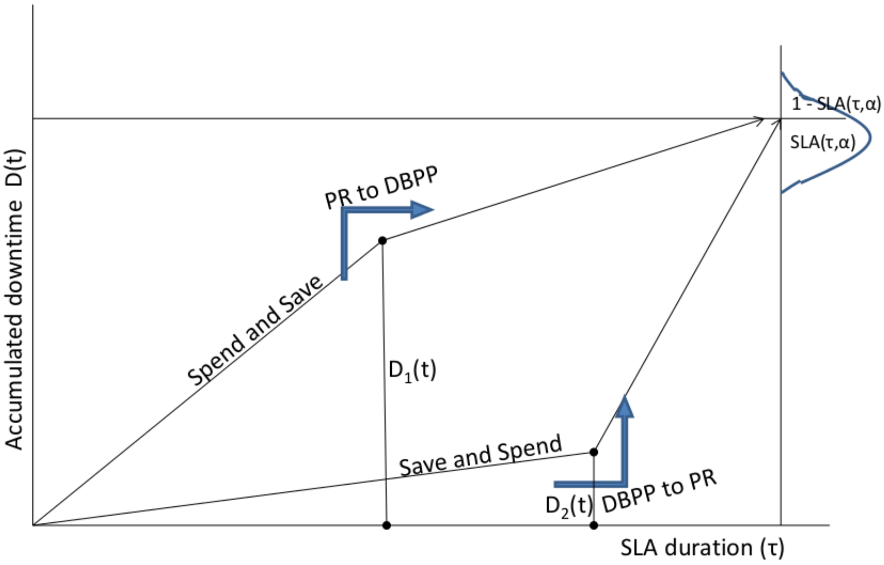

Figure 4.3: Save-Spend Approach vs. Spend-Save Approach

Figure 4.3 presents an example of a hybrid solution with two different approaches: Save-Spend and Spend-Save. $D(t_1)$ and $D(t_2)$ denotes the accumulated downtime in the network by using PR and DBPP, respectively. The remaining allowed accumulated downtime of the SLA is $\alpha - D(t_1)$ and $\alpha - D(t_2)$ respectively for each approach. By using this information, the target is to come up with such transition lines that provide the information about switching time when the given approaches are implemented in the network.

4.3 Numerical Analysis of Accumulated Downtime Distribution - Part 2

This section is connected to chapter 3.1 where numerical analysis of accumulated downtime distribution for Spend-Save and Save-Spend is made. Their accumulated downtime distribution over an SLA duration are computed with regards to the analysis made in chapter 3 of accumulated downtime distribution of DBPP and PR model. The MATLAB code is formulated using the theory of FFT and PDF of Weibull distribution, Uniform distribution and the proposed equation in chapter 3.3. The code is run in MATLAB giving the accumulated downtime distribution with 1 percent SLA risk target over an SLA duration τ (one year). The MATLAB code used in this section is shown in appendix A.

Computing the accumulated downtime as presented in 4.1 is complex for distributions different to exponential distributions. Hence, FFT is utilized in this thesis for simplicity and computation agility to calculate the accumulated downtime of an end-to-end connection.

4.3.1 Theoretical Background - Fast Fourier Transformation (FFT)

FFT is a discrete Fourier transformation algorithm which reduces the number of computations needed for N points from 2N2 to 2N lg N, where lg is the base-2 logarithm [36]. FFT is computed to investigate the effect of n factors on measured quantity [36]. In this project the factors are the recovery mechanisms and the measured quantity is the downtimes collected from UNINETT's backbone network.

FFT is a powerful mathematical tool for efficiently calculating the convolution. FFT is used to model and assess the PDF of non-parametric distribution. In this thesis, FFT is used to calculate the convolution of accumulated downtimes.

4.4 Matlab Computation of Accumulated Downtime

The parameters used to compute the accumulated downtime are shown in table 4.1.

Parameter	Value
Mean time to Failure (MTTF)	1360860s
Least Mean Downtime (LMDT)	2.4s
Probability for Simultaneous failure (PS)	0.00112
SLA Duration	3150000s
Maximum allowed accumulated downtime	315s
SLA risk target	1 percent
Weibull parameters	scale = 5.079s shape = 0.54

Table 4.1: Parameters value used for computing the transition line

4.4.1 Computation of Transition Lines

By considering the accumulated downtime distribution of the Save-Spend and Spend-Save approaches, a transition line is calculated in this section by taking into account SLA target of 1 percent.

As mentioned earlier, in the Save-Spend approach, the first failure in the network is recovered by DBPP. The PDF accumulated downtime using DBPP where both conditions (simultaneous and non-simultaneous failures) are considered $\omega_c(\tau, t)$ is applied for the first failure in the network. Then, the theory of Fast Fourier transformation is applied to calculate the rest of the failure occurring in the network until the SLA duration τ recovered with the PDF of accumulated downtime using PR $\omega_{PR}(\tau, t)$. Consequently, in the Spend-Save approach the first failure in the network is recovered by using PR so $\omega_P R(\tau, t)$ is applied for the first failure in the network and the rest of the failure is recovered with $\omega_c(\tau, t)$ using the theory of FFT. See appendix A for the MATLAB codes.

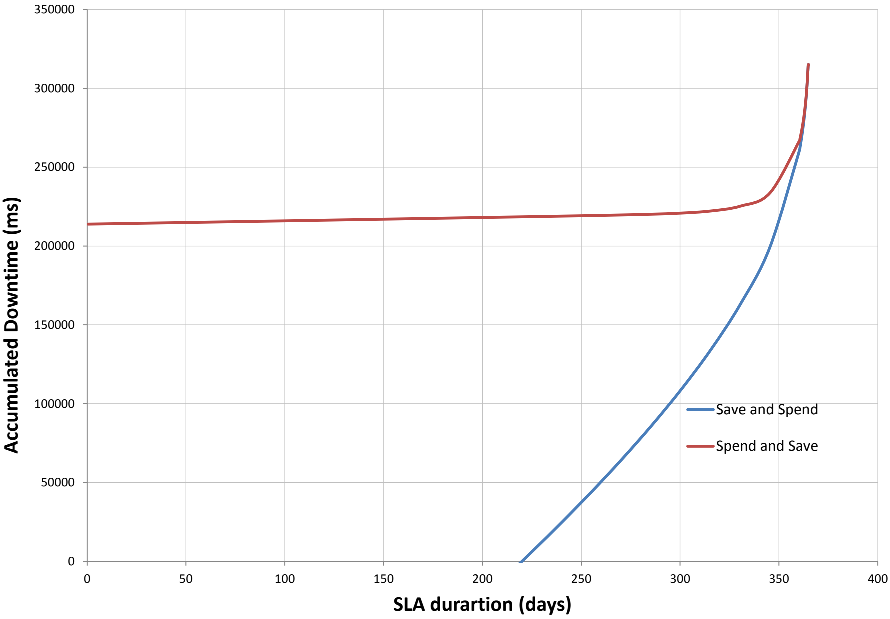

Figure 4.4: Switching transition lines for Save-Spend and Save-Spend

Figure 4.4 presents the transition lines (switching time) where the connection switches between DBPP and PR with 1 percent of SLA risk target when Save-Spend approach and Spend-Save is applied respectively. Note that figure 4.4 is a computed version of the sample figure 4.1. For instance, the proposed hybrid model in figure 4.4 will then decide that if the accumulated downtime in the network crosses above the red line then the model will switch to the DBPP mechanism. A small correction on the transition frontier for Spend-Save approach was made and its accuracy to obtain 1 percent SLA risk target was proven via discrete event simulation. The correction in Spend-Save approach is shown in appendix A.

However, the proposed hybrid approaches need to be verified if it can fulfill a 1 percent SLA risk target. In other words, whether the computed transition lines are well calculated and the risk that is estimated will stand for real case situations needs to be probed. For this, a discrete event simulation is run in DEMOS platform. The following section will explain the part of the discrete event simulation made in this thesis. The section 4.5 will provide the description of simulation environment and an explanation of simulation process with pseudo code. The full simulation code is provided in appendix B.

4.5 Simulation Environment

The scenario in the simulation consists of paths and each connection is assigned to a path. The path in this thesis is referred to the path or route from source node to the destination node. Each connection C_i (where $i = 1, 2, \ldots, n$) is assigned to a working path W_i (where $i = 1, 2, \ldots, n$). Upon failure of a W_i, the C_i takes an alternative path known to be backup path B_i (where $i = 1, 2, \ldots, n$). The recovery time of C_i depends on which recovery mechanism (PR or DBPP) the C_i has used. If there is no B_i available then C_i waits until any potential working path is available.

Three assumptions are made while running the simulation. First, only path failures are considered based on the measurements from UNINETT's backbone. Second, the probabilities of the path failure are assumed to be known by the network provider, either based on measurements or in general models such as [8]. Third, paths are assumed to failed and be repaired independently.

The performance of the model is evaluated through a case study. To ease the interpretation of the result, the parameters used in the simulation throughout the case study are stated in table 4.2. The failure rate is based on the result from chapter 3 section 3.2.3, where the failure arrives on average of 15 days in the backbone network. The probability for simultaneous failure is taken from the study made in [13]. The parameter values of Weibull distribution are based on the result obtained in chapter 3, section 3.2.5. Time to failure distribution is set to be a negative exponential distribution (n.e.d) based on the analysis made in chapter 3 section 3.2.3 that the

Parameter	Value
Simulation period time	1 year
Number of replicated simulation	500000
Probability for simultaneous failure	0.005120
Weibull shape parameter	5.079/60 minutes
Weibull scale parameter	0.54
Path failure rate	22681 minutes per path[1]
Time to failure distribution	Negative exponential

Table 4.2: Parameters value used in simulation scenario for Spend-Save and Save-Spend approach

distribution of failure arrival can be regarded as exponential and independent of other failure arrival times, thereby referring to Poisson process. Based on the study made in [30], it is supposed that if there is simultaneous failure with the C_i using DBPP, the recovery distribution for C_i will be of PR, in this case a Weibull distribution. The simulation process of Save-Spend and Spend-Save approaches is explained with pseudo code in 4.1 and 4.2.

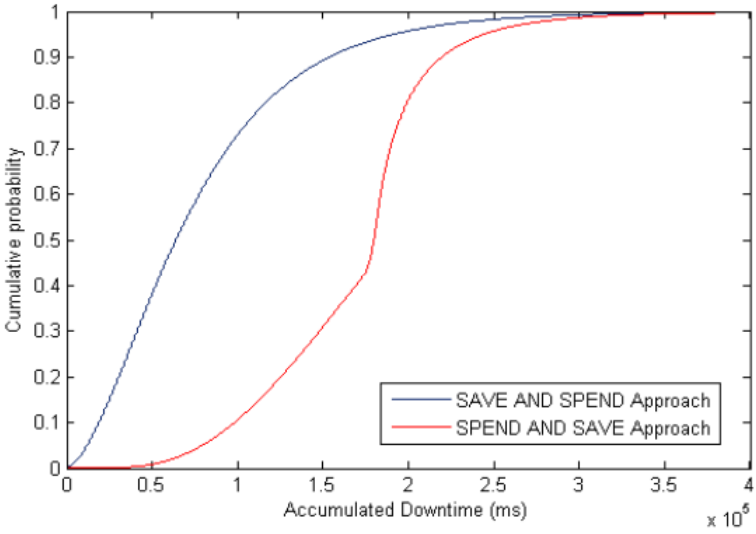

Figure 4.5: Comparison between Spend-Save and Save-Spend approach

Figure 4.5 presents the result from the discrete event simulation made for Spend-

Algorithm 4.1 Pseudocode for Save-Spend simulation, program in DEMOS.

```
Entity class Connection
Input: connection_id
begin
 Connection START in DBPP
 LOOP
 Connection_State is Up
 hold(dobule simulation time)

 IF interruption THEN
  Connection_State is Down AT time t1
  Register the downtime for connection_id

 IF connection_id is DBPP THEN
IF Simultaneous_failure THEN
   hold (Weibull_failure_distribution)
 ELSE
  hold (Uniform_distribution(40ms,50ms))
 END

 IF connection_id is PR THEN
  hold(Weibull_failure_distribution)
 END

 Register the total_downtime(Connection_id)
 IF (total_downtime(connection_id) AT time t1 < transition_line_Save-Spend) THEN
  Switch TO PR

 DISPLAY 500000 replications of Accumulated Downtimes
 END
```

Save and Save-Spend approaches using the computed transition line to switch between DBPP and PR. In figure 4.5, one can see that cumulative probability is greater than 0.99 at SLA risk target of 315000 ms. Meaning that the probability to succeed the SLA availability guarantee of 31500 ms within a year is greater than 0.99. Voila! Hence, based on the results from the simulation both approaches seemed to succeed in fulling the 1 percent SLA risk target at the end of SLA contract time.

Nonetheless, the objective is to fulfill the SLA availability guarantee in a cost efficient way by using as few resources as possible. The following section will analyze the resource usage by the proposed hybrid approaches. In addition, the approaches will be analyzed economically based on the resource used.

Algorithm 4.2 Pseudocode for Spend-Save simulation, program in DEMOS.

```
Entity class Connection
Input: connection_id
begin
Connection START in PR
 LOOP
 Connection_State is Up
 hold(dobule simulation time)

 IF interruption THEN
  Connection_State is Down AT time t2
  Register the downtime for connection_id

 IF connection_id is DBPP THEN
IF Simultaneous_failure THEN
   hold(Weibull_failure_distribution)
 ELSE
  hold (Uniform_distribution(40ms,50ms))
 END

 IF connection_id is PR THEN
  hold(Weibull_failure_distribution)
 END

 Register the total_downtime(Connection_id)
 IF (total_downtime(connection_id) AT time t2 > transition_line_Spend-Save) THEN
  Switch TO DBPP

 DISPLAY 500000 replications of Accumulated Downtimes
 END
```

4.6 Resource Usage of Hybrid Approaches

The resource consumption and network costs play a vital role for network providers. Thus, it is important to analyze the resource consumption of the proposed model. The study made in [35] shows that DBPP uses more than double the resource compared to PR. Keep in mind that DBPP is a resource demanding and economically costly scheme. The resource usage by the proposed hybrid approaches is examined in terms of utilization of DBPP. It is expected that the more DBPP is utilized by the network the more resources it uses. The following section 4.6.1 explains the process of computing the resource utilization by Spend-Save and Save-Spend approaches and evaluates the result.

4.6.1 Computing the Resource Utilization

To compute the resource utilization of each hybrid approach a discrete event simulation is performed where a variable switching time is registered. Switching time is denoted as $switchtime(1 : numPath)$ in appendix C. In the case of Spend-Save approach, the switching time refers to the time from the connection switches to DBPP until the simulation period. Whereas, in case of Save-Spend approach it refers to the time until the connection switches to PR. Hence, in both cases the switching time refers to the period of time where only DBPP is utilized. 500,000 replications of simulation were made to provide results with a negligible error. The average switching time of 500,000 replications is calculated. Thereafter, the ratio of average switching time to the total simulation time is calculated and a percentage of DBPP utilization is achieved. The result obtained at the end is shown in figure 4.6.

Figure 4.6: Resources usage by Save-Spend and Save-Spend

Note that, figure 4.6 represents the 1 percent SLA target risk and the verification was made via the discrete event simulation made in DEMOS.

Figure 4.6 illustrates that the utilization of DBPP in approach Save-Spend is about 62 percent whereas the utilization of DBPP in approach Spend-Save is only about 18 percent. There is almost three times the difference between the two hybrid approaches in terms of utilization of DBPP. Meaning that, Save-Spend approach is not an optimal resource efficient policy due to its high utilization of DBPP making the hybrid solution more resource demanding compared to Spend-Save approach. On the other hand, Spend-Save approach seems to be the most efficient hybrid solution as this approach only utilizes 18 percent of DBPP throughout the SLA contract time.

Thus, it can be concluded that the proposed Spend-Save approach is chosen for the hybrid model.

Additionally, it would be interesting to see if the changes in the SLA risk target of Spend-Save approach has any impact on the resource utilization and therefore on the total network cost for network providers. The changes in SLA risk targets were made by adjusting the transition line of Spend-Save. If the transition line in figure 4.4 for Spend-Save is lowered, then this will decrease the SLA risk target, which would result in an increase of the utilization of DBPP. If the transition line is raised, the SLA risk target will increase, leading to decrease the utilization of DBPP since the SLA requirements can cope with longer accumulated downtime.

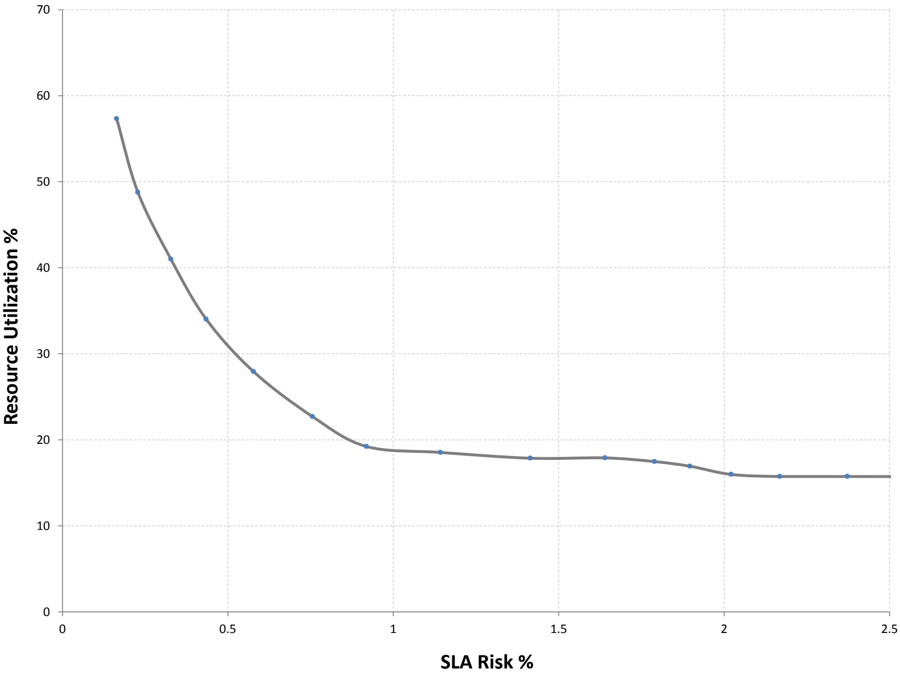

Figure 4.7: The relationship between SLA risk and resource (DBPP) utilization

One can see in figure 4.7 that the consumption of resources decrease as the SLA risk target increases. The reason was explained earlier: the switching time decreases (leads to increase in amount of time of using PR) with the increase of SLA risk target. The slope of the function starts to flatten out after approaching the risk of 1 percent because the difference in utilization of DBPP with increasing risk target tends to decrease. The reason is that at some point, lets say 1 percent of risk target, using PR scheme the downtime budget starts to get equal with increasing risk target thereby the switching time will also tend to be similar.

The next chapter will study the cost for network providers with different SLA risk targets. The motive is to find the optimal SLA risk target that utilizes least percentage of DBPP and gives the least cost price for the network providers to fulfill the SLA availability guarantee.

4.7 Economic analysis and Optimal SLA Risk Target of Spend-Save Approach

This section will study the relationship between the cost for fulfilling the SLA availability guarantee and SLA risk by using the Spend-Save hybrid approach with consideration of two parameters: cost of utilization of DBPP and cost of expected penalty[2]. The objective is to find the optimal SLA risk target that provides the least total cost for network providers.

4.7.1 Computation to Achieve SLA Risk Target

A case study was made with different SLA risk targets with price for utilization of DBPP of \$30 and penalty price per each violation of \$0.005. The penalty price increases linearly with the gradient of 0.005 after the SLA violation. The SLA risk target were set from range of 0.15 percent to 12.65 percent. The total cost for network providers for each SLA risk target consists of the sum of operational cost and expected penalty cost. The operational cost was computed by taking the product of probability of DBPP utilization and the cost price for DBPP utilization to fulfill the respective SLA risk target. The total expected penalty cost was computed by taking the average of the single penalty costs. Single penalty cost is the product of: 1 divided by the total number of simulation replication ($Simulation_{total}$); penalty price per each penalty ($P_{penalty}$); and the difference between SLA risk target (SLA_{risk}) and the downtime duration that went above the risk target ($D_{voilation}$). Mathematically, single penalty cost $= Simulation_{total} \times P_{penalty} \times (SLA_{risk} - D_{voilation})$

Analyzing the figures 4.8 and 4.9 and the table 4.3, one can conclude that the relationship between total cost price and SLA risk is like a concave shape. The cost decreases at the increase of SLA risk target until it reaches its minimum point. Thereafter, total cost starts to increase again until it reaches the point where there is zero utilization of DBPP scheme. Meaning that, when the network does not use DBPP scheme (no switching from PR to DBPP) the total cost (production cost and penalty cost) will start to even out. The reason is that the accumulated downtime

---

[2] The network provider needs to pay the penalty if the accumulated downtime crosses SLA risk target

SLA risk percent	Total Expected Penalty cost	Operational cost	Total cost
0.164	0.547	17.199	17.746
0.228	0.745	14.633	15.378
0.328	1.063	12.300	13.363
0.435	1.381	10.206	11.587
0.578	1.771	8.379	10.150
0.756	2.223	6.809	9.032
0.919	2.644	5.769	8.413
1.143	3.195	4.794	7.989
1.415	3.823	3.956	7.779
1.640	4.329	3.467	7.796
1.789	4.644	3.204	7.848
1.896	4.878	3.054	7.932
2.021	5.142	2.888	8.030
2.168	5.460	2.731	8.192
2.373	5.873	2.521	8.394
12.643	36.422	0.324	36.746

Table 4.3: The list of different SLA risk targets used in this section

for any transition line with SLA risk target more than 12 percent will give same cost for penalty, and no utilization of DBPP provides same production cost. From figure 4.9 one can observe that the cost price for the network provider is lowest around 1.4 percent of risk target. Thus for this case study, using the Spend-Save hybrid approach with an SLA risk target of 1.4 percent can be an optimal SLA risk target which provides the least total cost for network providers.

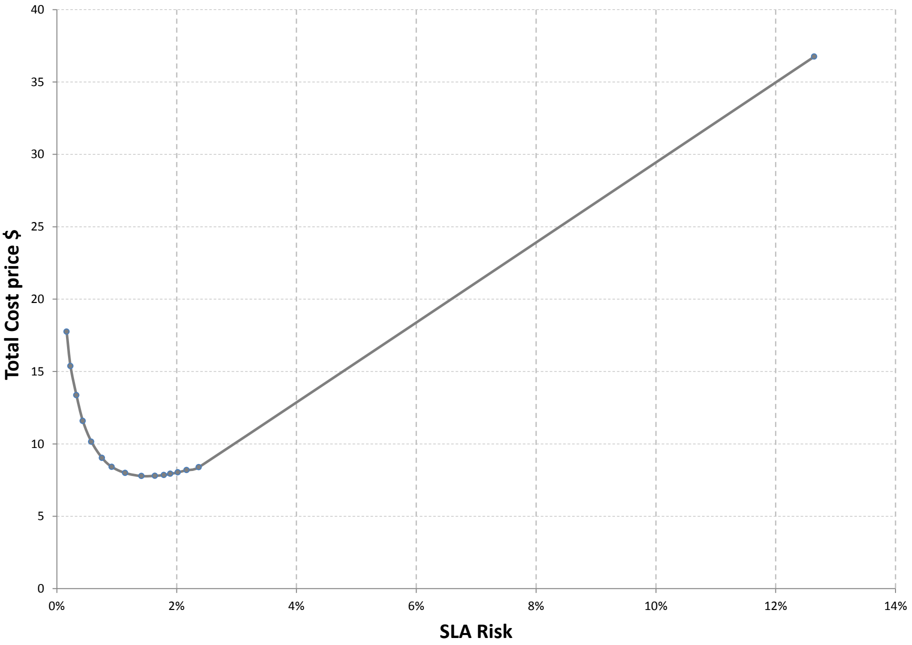

Figure 4.8: The relationship between SLA risk and total cost price

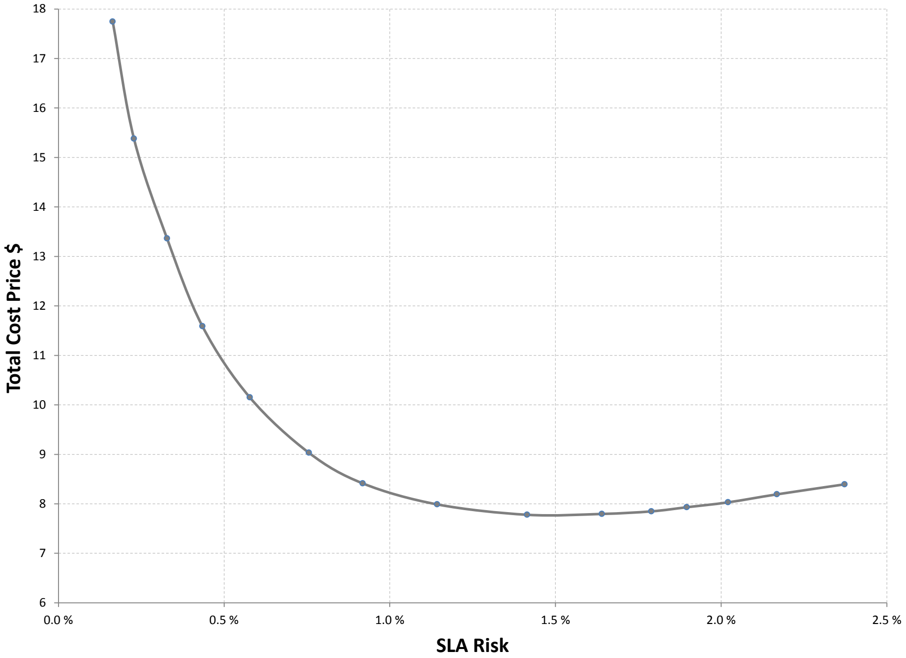

Figure 4.9: Zoomed out version of the SLA risk and total cost price

Chapter 5

Conclusion

5.1 Summary

Two network recovery mechanisms have been discussed throughout this thesis: Protection and Restoration (DBPP and PR), creating a hybrid model which was to focus on fulfilling the SLA availability guarantee using the resources efficiently in the backbone network. There have been provided theoretical background and previously related works in this thesis. However, the hybrid of recovery mechanisms in backbone networks is a new research topic so there weren't many previous works done directly related to this.

Different types of focus have been iterated to achieve results with respect to the research question: "fulfilling the SLA availability guarantee by using as few resources as possible". Different possible scenarios have been studied while working on the thesis. The quality in the SLA risk control relies on the precise assessment of the distribution of accumulated downtime [11]. This thesis explains a complete framework to model the SLA risk assessment under various failure and repair processes.

It started with filtering the failure data set from UNINETT's backbone network to obtain the distribution of failure arrival and end-to-end downtime duration in a network. This went smoothly and gave knowledge about the failures in networks in operational environments. Thereafter, step by step guidelines mentioned in the introduction chapter were followed and a hybrid model was developed which solved the research question of this thesis. The proposed schemes were simulated in real case scenarios, and compared based on resource utilization and total expected network cost.

5.2 Evaluation

The thesis was accomplished by going through three sophisticated phases where each phase was dependent on each other and provided a valuable solution (result) which was then used in the other phases.

5.2.1 Phase 1 – Filtration and Analysis of data set from UNINETT backbone network

In this phase, seven months of IS-IS routing update logs from UNINETT's backbone to characterize failures that leads to packet delay were investigated. The investigation indicated that failures occur every 12-15 days. The other findings were that the downtime duration is directly proportional to the loss of packets. Talking about the probability distribution of failure, it was concluded that the empirical CDF (the CDF from UNINETT downtime data) can be modeled by Weibull distribution with scale and shape parameters value of 5.07997s and 0.54, respectively.

5.2.2 Phase 2 - Computation of transition line

In this phase, a transition line was computed with regards to 1 percent SLA risk target using the theory of FFT and accumulated downtime distribution based on Save-Spend and Spend-Save hybrid approaches. The computed transition lines for both the approaches were verified and validated. The result showed that both hybrid approaches succeed in fulfilling the 1 percent SLA risk target at the end of the SLA contract time.

5.2.3 Phase 3 – Resource utilization and Cost analysis

In this phase, an analysis of the resource usage (meaning the utilization of DBPP) by the proposed hybrid approaches is made. Thereafter an optimal cost analysis to use the hybrid solution is studied. The result of resource usage analysis shows that the use of DBPP in Save-Spend is three times bigger than in the Spend-Save. Hence, the proposed Spend-Save hybrid approach is concluded to be the most efficient hybrid model for network providers based on resource utilization. Moreover, a cost analysis was made using Spend-Save with consideration of two parameters: cost of utilization of DBPP and expected penalty cost. The cost analysis was made with different SLA risk targets. The numerical results showed that total cost for network providers decreases with the increase of SLA risk until the risk target reach its minimum of 1.4 percent. Thus, it can be suggested that the proposed Spend-Save approach with SLA risk target around 1.4 percent gives the optimal hybrid solution for network providers in this case study.

5.2.4 Focus on Research questions

The research questions had a focus on resource utilization and fulfilling SLA availability guarantee.

Is it possible to fulfil the SLA availability guarantee efficiently when a hybrid of DBPP and PR is implemented?
The proposed hybrid model is very modularized and the transition line used in this model is created based on an SLA risk assessment of a real data set from UNINETT's backbone network.

The results presented in this thesis shows the assets of using a hybrid model as it provides a delicate way to manage the risk of failing the SLA and a cheaper option in terms of resource utilization and network cost.

For instance, Spend-Save has proved to use the resources efficiently and fulfill the SLA requirement. While designing this model, simultaneous failures in the network were also considered. Therefore, it is possible to use this hybrid model for any given measured data set from network providers in both simultaneous and non-simultaneous failure scenarios.

5.3 Future Work

The data log from UNINETT's network could not be examined for a longer period due to time and capacity constraints. Thus if possible, studies of the failure characteristics of more real data of the backbone network (e.g many years) could be made in order to get more precise results.

This thesis has mainly looked at hybrid recovery of PR and DBPP of end-to-end path failure in backbone networks. Further research can be done in applying the hybrid recovery model with a combination of other recovery schemes.

During work on this thesis, some case studies were tested for efficient recovery of the backbone network. Further study can be done in developing good open source case studies for simulating the hybrid model. There are likely further improvements and developments on this model.

References

[1] (2014). Global IP network SLA[online]. Available at: http://www.us.ntt.net/support/sla/network.cfm.

[2] (2014). What is openflow? [online]. Available at: http://www.sdncentral.com/what-is-openflow/.

[3] Banerjea, A., Parris, C. J., and Ferrari, D. (1994). Recovering guaranteed performance service connections from single and multiple faults. In *Global Telecommunications Conference, 1994. GLOBECOM'94. Communications: The Global Bridge., IEEE*, pages 162–168. IEEE.

[4] Engen, V., Kvittem, O., Mellati, A., and Bergem, G. G. (2014). Geographic map UNINETT [online]. Available at: http://drift.uninett.no/kartg/last/uninett/norge/geo/nuh.

[5] Felske, K., Gruber, J., and Wang, G. (2003). Two stage, hybrid logical ring protection with rapid path restoration over mesh networks. EP Patent App. EP20,010,302,630.

[6] Filsfils, C. and Evans, J. (2005). Deploying diffserv in backbone networks for tight SLA control. *Internet Computing, IEEE*, 9(1):66–74.

[7] González, A. J. and Helvik, B. E. (2010). Latincon08-guaranteeing service availability in SLAs; a study of the risk associated with contract period and failure process. *Latin America Transactions, IEEE (Revista IEEE America Latina)*, 8(4):410–416.

[8] González, A. J. and Helvik, B. E. (2011). Analysis of failures characteristics in the UNINETT IP backbone network. In *Advanced Information Networking and Applications (WAINA), 2011 IEEE Workshops of International Conference on*, pages 198–203. IEEE.

[9] Gonzalez, A. J. and Helvik, B. E. (2012a). Characterisation of router and link failure processes in UNINETT's IP backbone network. *International Journal of Space-Based and Situated Computing*, 2(1):3–11.

[10] Gonzalez, A. J. and Helvik, B. E. (2012b). A study of the interval availability and its impact on SLAs risk. In *Advances in Computer Science, Engineering & Applications*, pages 879–890. Springer.

[11] Gonzalez, A. J. and Helvik, B. E. (2013a). Hybrid cloud management to comply efficiently with SLA availability guarantees. In *Network Computing and Applications (NCA), 2013 12th IEEE International Symposium on*, pages 127–134. IEEE.

[12] Gonzalez, A. J. and Helvik, B. E. (2013b). SLA success probability assessment in networks with correlated failures. *Computer Communications*, 36(6):708–717.

[13] Gonzalez, A. J., Helvik, B. E., Hellan, J. K., and Kuusela, P. (2010). Analysis of dependencies between failures in the UNINETT IP backbone network. In *Dependable Computing (PRDC), 2010 IEEE 16th Pacific Rim International Symposium on*, pages 149–156. IEEE.

[14] Hadjiona, M., Georgiou, C., Papa, M., and Vassiliou, V. (2008). A hybrid fault-tolerant algorithm for mpls networks. In *Wired/Wireless Internet Communications*, pages 41–52. Springer.

[15] Iannaccone, G., Chuah, C.-n., Mortier, R., Bhattacharyya, S., and Diot, C. (2002). Analysis of link failures in an IP backbone. In *Proceedings of the 2nd ACM SIGCOMM Workshop on Internet measurment*, pages 237–242. ACM.

[16] Karagiannis, T., Molle, M., Faloutsos, M., and Broido, A. (2004). A non-stationary poisson view of internet traffic. In *INFOCOM 2004. Twenty-third AnnualJoint Conference of the IEEE Computer and Communications Societies*, volume 3, pages 1558–1569. IEEE.

[17] Laine, J., Saaristo, S., and Prior, R. (2002). Rude and crude[online]. Available at: http://rude.sourceforge.net.

[18] Markopoulou, A., Iannaccone, G., Bhattacharyya, S., Chuah, C.-N., and Diot, C. (2004). Characterization of failures in an IP backbone. In *INFOCOM 2004. Twenty-third AnnualJoint Conference of the IEEE Computer and Communications Societies*, volume 4, pages 2307–2317. IEEE.

[19] Martinez, A. J. G. (2013). *Methods For Guaranteeing Contracted Availability In Connection Oriented Networks.* PhD thesis, Norwegian University of Science and Technology.

[20] Matz, S. M., Votta, L. G., and Malkawi, M. (2002). Analysis of failure and recovery rates in a wireless telecommunications system. In *Dependable Systems and Networks, 2002. DSN 2002. Proceedings. International Conference on*, pages 687–693. IEEE.

[21] Médard, M. and Lumetta, S. S. (2003). Network reliability and fault tolerance. *Encyclopedia of Telecommunications.*

[22] Myakotnykh, E., Helvik, B., Hellan, J., Kvittem, O., Skjesol, T., Wittner, O., and Oslebo, A. (2010). Analyzing causes of failures in the global research network using active measurements. In *Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 2010 International Congress on*, pages 565–570.

[23] Mykkeltveit, A. (2008). *Dependability differentiation in communication networks*. PhD thesis, PhD Thesis, Norwegian University of Science and Technology, Trondheim, Norway.

[24] Mykkeltveit, A. and Helvik, B. E. (2007). Provision of connection-specific availability guarantees in communication networks. In *Design and Reliable Communication Networks, 2007. DRCN 2007. 6th International Workshop on*, pages 1–8. IEEE.

[25] Mykkeltveit, A. and Helvik, B. E. (2008). Comparison of schemes for provision of differentiated availability-guaranteed services using dedicated protection. In *Networking, 2008. ICN 2008. Seventh International Conference on*, pages 78–86. IEEE.

[26] Nelson, B. L., Carson, J. S., and Banks, J. (2001). *Discrete event system simulation*. Prentice hall.

[27] Petersson, J. M. O. (2005). MPLS based recovery mechanisms. *University in Oslo, Institute of Informatics*.

[28] Rouse, M. (2013a). control plane(CP)[online]. Available at: http://searchsdn.techtarget.com/definition/control-plane-cp.

[29] Rouse, M. (2013b). data plane(DP)[online]. Available at: http://searchsdn.techtarget.com/definition/data-plane-dp.

[30] Ruan, L. and Feng, T. (2010). A hybrid protection/restoration scheme for two-link failure in wdm mesh networks. In *Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE*, pages 1–5. IEEE.

[31] Sharma, S., Staessens, D., Colle, D., Pickavet, M., and Demeester, P. (2013). Openflow: Meeting carrier-grade recovery requirements. *Computer Communications*, 36(6):656–665.

[32] Takacs, L. (1957). On certain sojourn time problems in the theory of stochastic processes. *Acta Mathematica Hungarica*, 8(1):169–191.

[33] Vasseur, J.-P., Pickavet, M., and Demeester, P. (2004). *Network recovery: Protection and Restoration of Optical, SONET-SDH, IP, and MPLS*. Elsevier.

[34] Venkatesan, S., Patel, M., and Mittal, N. (2005). A distributed algorithm for path restoration in circuit switched communication networks. In *Reliable Distributed Systems, 2005. SRDS 2005. 24th IEEE Symposium on*, pages 226–235. IEEE.

[35] Verbrugge, S., Colle, D., Demeester, P., Huelsermann, R., and Jaeger, M. (2005). General availability model for multilayer transport networks. In *Design of Reliable Communication Networks, 2005.(DRCN 2005). Proceedings. 5th International Workshop on*, pages 8–pp. IEEE.

[36] Weisstein, E. W. (2007). Fast fourier transform. *From MathWorld–A Wolfram Web Resource. http://mathworld. wolfram. com/FastFourierTransform. html.*

Appendix A

Matlab simulation script

The Matlab script used to simulate Save-Spend and Spend Save approach. This script generate the distribution of accumulated downtime for each hybrid approach.

```
Save-Spend Approach

t=0:1:500000;
t1=t(2:500000);

failureMTTF = 1360860000;
BestMDDT = 24000;
ProbSimultaneous =0.00512;

% The following codes generate the PDF of uniform distribution with values from 40ms 50ms for DBPP with peferfect condition.
f0 = unifpdf(t1,40,50);
cdf0=cumsum(f0);
f0=f0/max(cdf0);
cdf01=cumsum(f0);


% The following codes generate the PDF of weibull distribution with values from 5079.97ms as scale and 0.54 as shape for PR.
f1 = wblpdf(t1,5079.97,0.54);
cdf1=cumsum(f1);
f1=f1/max(cdf1);
cdf11=cumsum(f1);
f10= [f1  zeros(1,500000) ];

```

```
% The following codes generate the PDF of DBPP when both conditions are applied.
f2 = (1-ProbSimultaneous)*f0 + (ProbSimultaneous)*f1;
cdf=cumsum(f2);
f20= [f2  zeros(1,500000) ];

gap= 1296000000; % the gap between each failure to occur
Res99= [];
timeXaxis = [];

for SLAMonth = 1:25
tiM=31500000000  -(gap*(SLAMonth-1)) ;
A= tiM; % Availability of SLA duration.

% z contains the distribution (PDF) of the accumulated downtime. First It
z= (A/failureMTTF) * ( exp(-A/failureMTTF) ) *  f20; % First downtime event in the connection is recovered by DBPP (f20).
w=f20;
cdw=cumsum(w);
w=w/max(cdw);
for n = 1:50    % number of failures over a SLA period.
        w = ifft(    fft(w).*fft(f10)    ) ; % Taking inverse of FFT to set in time domain and taking convolution of all the  downtime event.
        cdw=cumsum(w); % sum of all the convolution
        w=w/max(cdw);
        z= (    (((A/failureMTTF)^(n+1))/factorial(n+1)) * ( exp(-A/failureMTTF) ) * w )  + z ;
end

z(1)=exp(-A/failureMTTF);
cdz=cumsum(z);
z=z/max(cdz);
cdz=cumsum(z);

i=0.99*max(cdz); % Setting SLA risk target of 0.99.
j=1;
while i>cdz(j)
        j=j+1;
```

```
end
Res99= [Res99  j];
timeXaxis = [timeXaxis   A];
end
```

```
Spend-Save Approach

t=0:1:500000;
t1=t(2:500000);
failureMTTF = 1360860000;
BestMDDT = 24000;
ProbSimultaneous =0.00512;

f0 = unifpdf(t1,40,50);
cdf0=cumsum(f0);
f0=f0/max(cdf0);
cdf01=cumsum(f0);
f0x =f0(1:489524);

f1 = wblpdf(t1,5079.97,0.54);
cdf1=cumsum(f1);
f1=f1/max(cdf1);
cdf11=cumsum(f1);
f10= [f1   zeros(1,500000) ];

fx = f1(10476:499999);
cdfx=cumsum(fx);
fx=fx/max(cdfx);
cdfx=cumsum(fx);
fx0= [fx   zeros(1,500000) ];

f2 = (1-ProbSimultaneous)*f0x + (ProbSimultaneous)*fx;
cdf=cumsum(f2);
f2=f2/max(cdf);
cdf=cumsum(f2);
f20= [f2   zeros(1,500000) ];

gap= 1296000000;
Res99= [];
timeXaxis = [];
for SLAMonth = 1:25
tiM= 31500000000    -(gap*(SLAMonth-1))    ;
```

```
A= tiM;
z= (A/failureMTTF) * ( exp(-A/failureMTTF) ) *  fx0;
w=fx0;
cdw=cumsum(w);
w=w/max(cdw);
for n = 1:50
        w = ifft(    fft(w).*fft(f20)    ) ;
        cdw=cumsum(w);
        w=w/max(cdw);
        z= (   (((A/failureMTTF)^(n+1))/factorial(n+1)) * (
           exp(-A/failureMTTF) ) * w )  + z ;
end
z(1)=exp(-A/failureMTTF);
cdz=cumsum(z);
z=z/max(cdz);
cdz=cumsum(z);

i=0.99*max(cdz);
j=1;
while i>cdz(j)
        j=j+1;
end
Res99= [Res99 j];
timeXaxis = [timeXaxis  A];
end
```

The variable name in both approaches represent the same. For instance f1 and f2 in both approaches represent PDF of PR and DBPP respectively.

Appendix B

Discrete Event Simulation script

The simulation script written in SIMULA langauge is used to simulate Save-Spend and Spend Save approach in DEMOS platform:

```
begin
  external class demos = "C:\cim\demos.atr";
  demos begin

    long real simtimePER =525000;
    integer numOfReplication = 500000;
    integer numOBS = 1;
        long real simultaneusProb = 0.005120;

    long real shapef = 0.54; !Weibull shape parameter
    long real scalef = 5.079/60; !Weibull scale parameter

    long real failure_rate_path = 22681;

        integer numPath = 1 ;

    long real weibullDistTime,tempTimeDistribution;

    ref(RDist) unidf;

        ref(bdist) array u(1:numPath);

        ref(rdist)array failureC(1:numPath); ! Each Path has different failure distribution;
        ref(rdist)array failure2(1:numPath); ! Each Path has different failure distribution;

```

```
    long real Array LastDown(1:numPath);
long real Array totaltimedown(1:numPath);
    long real Array switchtime(1:numPath);
    integer Array Connection_in_B(1:numPath);
    integer Array Marker(1:numPath);

    !  *********  ENTITY Path DEFINITION ************;
    !  *********  ENTITY Path DEFINITION ************;

Entity class Path(num); integer num;
begin
            boolean IfSimultaneous;

    loop:
                    hold( failureC(num).sample  ); ! ********** Wait Failure;
                    LastDown(num):= time;

                    if (Connection_in_B(num) = 1 ) then begin

                            IfSimultaneous := u(num).sample;
                            if IfSimultaneous then begin
                                    ! ********  WEIBULL FAILURE *******;
                                    weibullDistTime := scalef*( ( (-LN(1-(unidf.sample))) )**(1/shapef));
                                    hold( weibullDistTime );
                            end
                            else begin
                                    weibullDistTime :=50/60000;
                                    hold( 50/60000 );
                            end;
        end;
```

```

                if (Connection_in_B(num) = 0 ) then begin
                                        weibullDistTime :=  scalef*(
                                            ( (-LN(1-(unidf.sample))
                                          ) )**(1/shapef) );
                    hold( weibullDistTime );
                                        tempTimeDistribution    :=
                                            totaltimedown(num);
                end;

                          totaltimedown(num) := totaltimedown(
                              num) + ( weibullDistTime );
                !totaltimedown(num) := totaltimedown(num) + (
                    time - LastDown(num) );

                if ( Connection_in_B(num) = 0) then begin
                                        if (   (( 0.0000004059596*
                                            time) + (157000/60000) )
                                              < totaltimedown(num)
                                               ) then begin
                                                Connection_in_B(num)
                                                    := 1;
                                                if (
                                                   tempTimeDistribution
                                                    > 0) then begin
                                                        Marker(num)
                                                           := 0;
                                                end;
                                                !totaltimedown(num)
                                                   := totaltimedown(
                                                   num) -
                                                   tempTimeDistribution
                                                   ;
                                                switchtime(num):=
                                                   simtimePER - time
                                                   ;
                                        end;
                          end;
    repeat;
end;
! ********** END ENTITY Path *************;
```

```
!  **********  END  ENTITY Path  **************;


    !  ********** VARIABLE DEFFINITION *********;

    integer i,j,w,shift, state, newinic, shiftregistered
        , position, finalorder;
integer numevents, runt;

unidf :- new uniform("failire", 0.0, 1.0);

for i:= 1 step 1 until numPath do
    failureC(i) :- new NegExp( (edit("failc_",i)) ,(1/
        failure_rate_path));

    for i:= 1 step 1 until numPath do
    failure2(i) :- new NegExp( (edit("fail2_",i))
        ,(60/20));

    for i:= 1 step 1 until numPath do
            u(i) :- new draw(edit("u",i),simultaneusProb
                );

!*************************** REPLICATE START
    ****************;

    for j:=1 step 1 until numOfReplication do
    begin

        !trace;
        runt:=runt+1;

        setseed(j);

                    for i:=1 step 1 until numPath do
                        begin
                            totaltimedown(i) := 0;
                            Connection_in_B(i) := 0;
                            switchtime(i) := 0;
                            Marker(i) := 0;
                    end;
```

```

             for i:=1 step 1 until numPath do
                 new Path(edit("Path",i),i).schedule(0.0);

             hold(simtimePER);

                          !if ( Marker(1) = 1) then begin ;
                          outFix(60000*totaltimedown(1) ,1,10); outFix( switchtime(1) ,1,13);
                          outImage;
             !end;
         Noreport;
         REPLICATE;
         end;

         !************* END ***** REPLICATE STARTING ****************;
         !************* END ***** REPLICATE STARTING ****************;

  end;
end;
```

Appendix C

AWK script

The Awk script used to filter the UNINETT transmission data log and obtain the downtimes in the network:

```
Awk code:
To extract the ID number, Sequence number, Transmission time, Receiving time from UNINETT log
awk 'BEGIN{FS = "[=, " "]"}{if($2 == "43"){print $2, $4, $10, $12}}'


 Filtering the file where the sequence number difference is greater than 2 or the delay is greater than 0.5s.
awk 'NR > 1 {if(($2 - old2) > 2 || ($3 - old3) > 0.15){print $2, $2 - old2, $3, $4, $3 - old3, $3 -old4}} {old2 = $2; old3 = $3; old4 = $4}' 01-04_Extract2043 > 01-04_SEQ_ArrivalDiff2043.txt

 Filtering accumulated downtime greater than 315000
awk 'Begin{FS = " "}{if($1 > 315000) {print $1, $1-315000}

 Finding Min, Max and Average/Mean of Accumulated Downtime
awk 'BEGIN{FS = " "; OS = ":"}{if(min == "") {min=max=$2}; if($2>max) {max=$2}; if($2< min) {min=$2}; total+=$2; count+=1} END {print total/count, min, max}'
```

Appendix D

List of Terms

D.1 List of Definitions

- **Accumulated downtime:** The total sum of all downtimes in the network connection during the SLA contract.
- **Backup path:** An alternative path of a network.
- **Dedicated backup path:** A backup path which corresponds to one particular working path.
- **Downtime budget:** The remaining maximum allowed accumulated downtimes in SLA.
- **Failure log:** The logs collected from UNINETT's backbone network where all the down events are registered.
- **Maximum allowed accumulated downtime:** It is the threshold of accumulated downtimes that is allowed before the provider violates the SLA and pays the penalty.
- **Network connection:** A group of interconnected links and routers which provide end-to-end service [12]. In this case, an end-to-end connection in a backbone network.
- **Network provider and customer:** A network provider owns a network infrastructure providing connectivity among different points. A customer pays for the provided connectivity. Both parties negotiate the limits and obligations of the service to be provided and define an SLA.
- **Service Level Agreement:** A contract between the provider and receiver of the services where the stipulation of the availability to be guaranteed is established for a given period.

- **Single downtime:** When a network connection is down.
- **SLA risk:** The probability of failing the SLA over the SLA contract period.
- **SLA risk assessment**:The evaluation of the probability of failing or succeeding the SLA requirement over the contracted period.
- **SLA risk target:** The probability of failing the SLA, however the provider can tune the risk target by using an advanced network recovery mechanism (e.g Protection) for more or less time.
- **Switching time:**The period of time where only DBPP is utilized.
- **Transition line:** The line that provides information about when the connection should switch between the Protection and the Restoration mechanisms by knowing the status of its current accumulated downtime and the remaining SLA time.
- **Working path:** A primary path of a network.

D.2 List of Symbols

Notations	Explanation
$\omega_{PR}(\tau, t)$	PDF of connection downtime with PR[1]
$\omega_{DBPP}(\tau, t)$	PDF of connection downtime with DBPP with perfect condition
ω_c	PDF of connection downtime with DBPP whwn both condition applied
$\Omega_{PR}(\tau, t)$	CDF of connection downtime with PR
$\Omega_c(\tau, t)$	CDF of connection downtime with DBPP when both condition applied
PS	Probability for flawed condition (simultaneous failure
τ	SLA duration
t	Time
$D(t)$	Accumulated downtime
$h(t)$	PDF of single downtime
$g(t)$	PDF of uptime
$A(\tau)$	interval availability over an SLA duration
$\Omega(\tau, t)$	CDF of accumulated downtime
$\omega(\tau, t)$	PDF of accumulated downtime
$G(t)$	CDF of uptime
$H(t)$	CDF of single downtime
α	SLA availability guarantee
$S(\tau, \alpha)$	SLA success probability
β	Weibull shape parameter
θ	Weibull scale parameter
$Simulation_{total}$	The total number of simulation replication
$P_{penalty}$	Penalty price per each penalty
$D_{voilation}$	The downtime duration that went above the risk target

Table D.1: Notations used in this thesis with its explanation.