Disaster Resilient Optical Core Networks

Zaid Hasan Ali Nasralla

Submitted in accordance with the requirements for the degree of

Doctor of Philosophy

The University of Leeds

School of Electronic and Electrical Engineering

November 2017

The candidate confirms that the work submitted is his own, except where work which has formed part of jointly-authored publications has been included. The contribution of the candidate and the other authors to this work has been explicitly indicated below. The candidate confirms that appropriate credit has been given within the thesis where reference has been made to the work of others.

The work in Chapter 3 of the thesis has appeared in publications as follows:

[1] Z. Nasralla, T. El-Gorashi, M. Musa, and J. Elmirghani, “Routing Post-Disaster Traffic Floods in Optical Core Networks,” in 20th International Conference on Optical Network Design and Modelling, May 2016.

My contribution: literature review, pinpoint the new issue of post-disaster traffic floods in core networks. Proposing five mitigation scenarios and developing the mixed Integer Linear Programming model and run the performance analysis.

Professor Elmirghani: originator of idea of traffic floods during disasters and helped with the preparation of paper.

Dr. Taisir Elgorashi: assisted with developing the idea, the scenarios and paper preparation.

Mohammed Musa: assisted with developing the models, the scenarios and paper preparation.

[2] Z. Nasralla, T. El-Gorashi, M. Musa, and J. Elmirghani, “Routing post-disaster traffic floods heuristics,” in Transparent Optical Networks (ICTON), 2016 18th International Conference on, July 2016.

My contribution: literature review, building the heuristic for post-disaster traffic floods in core networks. Proposing three mitigation scenarios and run the performance analysis.

Professor Elmirghani: originator of idea of traffic floods during disasters and helped with the preparation of paper.

Dr. Taisir Elgorashi: assisted with developing the idea, the scenarios and paper preparation.

Mohammed Musa: assisted with developing the idea, the scenarios and paper preparation.

The work in Chapter 4 of the thesis has appeared in publications as follows:

[3] Z. Nasralla, T. El-Gorashi, M. Musa, and J. Elmirghani, “Energy-Efficient Traffic Scheduling in IP over WDM Networks” International Conference on Next Generation Mobile Applications, Services and Technologies, September 2015.

My contribution: literature review, developed the new idea of using traffic scheduling in advance reservation demands to improve energy efficiency in IP over WDM core networks. Developed the mixed integer linear programming model and ran the performance analysis

Professor Elmirghani: originator of the idea of using traffic scheduling in advance reservation to improve energy efficiency in IP over WDM core networks and helped with the preparation of paper.

Dr. Taisir Elgorashi: assisted with developing the idea and paper preparation.

Mohammed Musa: assisted with developing the idea and paper preparation.

My contribution: literature review, developed the idea of building blackout resilient networks. Developed the mixed integer linear programming model and ran the performance analysis.

Professor Elmirghani: originator of the idea of power outages during disasters in optical networks and helped with the preparation of the paper.

Dr. Taisir Elgorashi: assisted with the development of the idea, validating the results and the production of the paper.

Acknowledgements

First, I would like to sincerely acknowledge my supervisor, Professor Jaafar Elmirghani for his guidance, patience, support and assistance through my PhD journey.

Also I would like to acknowledge Dr. Taisir Elgorashi, my academic co-supervisor for her effort throughout the journey of my PhD, for her useful discussion and advice.

I am very grateful and thankful to my beloved family my wife and my children (Roaa, Yousof and Reema), my mother, my father. I don't have enough words to thank them for supporting me in all possible ways. I hope I made them proud.

My gratitude goes to my sponsor the Higher Committee for Education Development in Iraq for fully funding my PhD. I was very fortunate to be awarded this scholarship.

Finally, Many thanks to my colleagues in the ICaPNet group in the School of Electrical and Electronic Engineering. I was very fortunate to have the opportunity to meet and collaborate with many outstanding students.

Zaid Nasralla

Abstract

During the past few years, the number of catastrophic disasters has increased and its impact sometimes incapacitates the infrastructures within a region. The communication network infrastructure is one of the affected systems during these events. Thus, building a resilient network backbone is essential due to the big role of networks during disaster recovery operations. In this thesis, the research efforts in building a disaster-resilient network are reviewed and open issues related to building disaster-resilient networks are discussed. Large size disasters not necessarily impact the communication networks, but instead it can stimulate events that cause network performance degradation. In this regard, two open challenges that arise after disasters are considered one is the short-term capacity exhaustion and the second is the power outage.

First, the post-disaster traffic floods phenomena is considered. The impact of the traffic floods on the optical core network performance is studied. Five mitigation approaches are proposed to serve these floods and minimise the incurred blocking. The proposed approaches explore different technologies such as excess or overprovisioned capacity exploitation, traffic filtering, protection paths rerouting, rerouting all traffic and finally using the degrees of freedom offered by differentiated services. The mitigation approaches succeeded in reducing the disaster induced traffic blocking.

Second, advance reservation provisioning in an energy-efficient approach is developed. Four scenarios are considered to minimise power consumption. The scenarios exploit the flexibility provided by the sliding-window advance reservation requests. This flexibility is studied through scheduling and

rescheduling scenarios. The proposed scenarios succeeded in minimising the consumed power.

Third, the sliding-window flexibility is exploited for the objective of minimising network blocking during post-disaster traffic floods. The scheduling and rescheduling scenarios are extended to overcome the capacity exhaustion and improve the network blocking. The proposed schemes minimised the incurred blocking during traffic floods by exploiting sliding window.

Fourth, building blackout resilient networks is proposed. The network performance during power outages is evaluated. A remedy approach is suggested for maximising network life time during blackouts. The approach attempts to reduce the required backup power supply while minimising network outages due to limited energy production. The results show that the mitigation approach succeeds in keeping the network alive during blackout while minimising the required backup power.

Table of Contents

Abstract vi

Table of Contents viii

List of Figures xii

List of Tables xvi

List of Abbreviation xvii

1 Introduction 1

1.1 Research objectives 3

1.2 Original contributions 4

1.3 Related publications 5

1.4 Organisation of the thesis 6

2 Background and Related Work 7

2.1 Introduction 7

2.2 IP over WDM Networks 8

2.2.1 IP over WDM Components 8

2.2.3 Routing and Wavelength Assignment in WDM Networks 12

2.3 Disaster Resilient Networks 16

2.3.1 Disaster Risk Evaluation 18

2.3.2 Disaster Mitigation Approaches 19

2.4 Linear Programming and Heuristic Approaches 31

2.5 Disaster-Related Open Issues 34

2.6 Summary.. 35

3 Post-Disaster Traffic Flood Mitigation in IP over WDM networks 36

3.1 Introduction 36

3.2 Post-Disaster Traffic Floods 36

3.3 Post-Disaster Traffic Floods Mitigation Approaches......................... 39

3.3.1 Floods with Fixed Routing (FFR).. 39

3.3.2 Floods with Selective Traffic Filtering (FSTF).............................. 40

3.3.3 Floods with Protection Paths Rerouting (FPPR) 40

3.3.4 Floods with Working and Protection Paths Rerouting (FWPPR) . 41

3.3.5 Floods with Rerouting and Differentiated Services (FRDS) 42

3.4 Network Design MILP Models 42

3.4.1 Dimensioning Model... 42

3.4.2 Floods MILP Model 46

3.5 Post-Disaster Traffic Floods Heuristic 50

3.6 Network Performance Evaluation under Post-Disaster Traffic Floods 58

3.7 Summary.. 66

4 Energy-Efficient Advance Reservation Scheduling and Rescheduling in IP over Optical Networks... 68

4.1 Introduction 68

4.2 Advance Reservation 68

4.3 Reservation Scenarios 70
4.2.1 Immediate and Fixed Advance Reservation (IFAR) 71
4.2.2 Immediate, Fixed and Sliding-window Advance Reservation (IFSAR) 71
4.2.3 Re-Scheduling and Rerouting AR Reserved Requests (RSRR) . 71
4.2.4 Rerouting and Rescheduling Active and Reserved Request (RARR) 73
4.4 MILP Model for Energy Efficient Traffic Scheduling in IP over Optical Networks 74
4.5 Energy Efficient Traffic Scheduling (EETS) Heuristics 78
4.6 Network Performance Evaluation 85
4.7 Summary 92
5 Mitigating Post-Disaster Traffic Floods using Advance Reservation Scheduling in IP over Optical Networks 94
5.1 Introduction 94
5.2 Related Work 94
5.3 AR requests with Floods Approaches 95
5.3.1 Floods with Traffic Scheduling (FTS) 95
This is the baseline approach where AR requests are provisioned on their arrival and their flexibility is not exploited, i.e. they are not rerouted or rescheduled to allow floods to be accommodated. 95
5.3.2 Floods with Traffic Re-Scheduling (FTRS) 95

5.3.3 Floods with Traffic Rerouting and Rescheduling of Active and Reserved Request (FTRR) 96
5.4 Floods with AR Scheduling MILP model 96
5.5 Floods with AR scheduling Heuristic 99
5.6 Network Performance Evaluation 107
5.7 Summary 114
6 Blackout Resilient Network 116
6.1 Introduction 116
6.2 Blackout Disaster 116
6.3 MILP for Blackout Resilient Scenarios 117
6.4 Network Performance Evaluation 121
6.5 Summary 134
7 Conclusions and future directions 135
7.1 Conclusions 135
7.2 Future work 138
References 142

List of Figures

Figure 1-1 Society, Network and Datacentre... 1

Figure 2-1 IP over WDM two node architecture and interconnection 9

Figure 2-2 Protection classification 21

Figure 3-1 Protection Paths Rerouting to accommodate floods at node 2 .. 41

Figure 3-2 FWPPR scenario 42

Figure 3-3 FFR heuristic... 51

Figure 3-4 FSTF heuristic... 52

Figure 3-5 FPPR heuristic 54

Figure 3-6 Routing function 55

Figure 3-7 FWPPR heuristic.. 56

Figure 3-8 FRDS heuristic 57

Figure 3-9 NSFNET network topology.. 58

Figure 3-10 Number of wavelengths per link... 59

Figure 3-11 The percentage of blocked floods for FFR scenario a) MILP b) Heuristic 60

Figure 3-12 The percentage of blocked floods for FSTF scenario a) MILP b) Heuristic 62

Figure 3-13 The percentage of blocked floods for FPPR scenario a) MILP b) Heuristic 63

Figure 3-14 The percentage of blocked floods for FWPPR scenario a) MILP b) Heuristic 64

Figure 3-15 The percentage of blocked floods for FRDS scenario a) MILP b) Heuristic 65

Figure 4-1 Space-time packing a) No packing b) Packing........ 80

Figure 4-2 EETS flowchart 81

Figure 4-3 EER heuristic 82

Figure 4-4 EETRS flowchart........ 84

Figure 4-5 EETRR heuristic 85

Figure 4-6 Sample network 86

Figure 4-7 Traffic Profile........ 86

Figure 4-8 SAR requests arrival distribution........ 86

Figure 4-9 The power saving percentage for IFSAR and RSRR scenarios. 88

Figure 4-10 The power saving for IFSAR and RSRR with different traffic volumes........ 88

Figure 4-11 the power saving for IFSAR and RSRR for 12 and 24 hours sliding window 89

Figure 4-12 the power consumption for MILP models and heuristic for IFAR, IFSAR and RSRR........ 90

Figure 4-13 COST 239 network with distances in kilometers 91

Figure 5-1 FTS heuristic.. 102

Figure 5-2 MBR heuristic... 103

Figure 5-3 FTRS heuristic 104

Figure 5-4 FPR heuristic 105

Figure 5-5 FTRR heuristic 106

Figure 5-6 The floods blocking percentage for node 1 108

Figure 5-7 The floods blocking percentage for node 4 108

Figure 5-8 No. of started SAR requests for FTS and FTRS 110

Figure 5-9 The blocking percentage for node 1.. 111

Figure 5-10 The blocking percentage for node 4...................................... 111

Figure 5-11 The floods blocking percentage under the 12 hours flooding scenario.. 113

Figure 5-12 The floods blocking percentage under the 4 hours flooding scenario.. 114

Figure 6-1 Italian Network 122

Figure 6-2 Average traffic request... 123

Figure 6-3 Solar cells output power at each node 123

Figure 6-4 Node 14 power consumption and battery residual energy under blocking minimisation scenario.. 125

Figure 6-5 Node 14 power consumption and battery residual energy under WESO 1 126

Figure 6-6 Node 14 power consumption and battery residual energy under WESO 2 127

Figure 6-7 Node 14 power consumption and battery residual energy under WESO 3 128

Figure 6-8 Node carried traffic through the day 129

Figure 6-9 The blocking probability for nodes a) 12 b) 13 c) 14 131

Figure 6-10 Number of hops 132

Figure 6-11 The blocking probability for nodes a) 7 b) 9 133

List of Tables

Table 3-1 Sets, parameters and variables for the MILP 43

Table 3-2 Parameters and variables definition for the floods MILP 46

Table 3-3 Input Data for the dimensioning MILP Model [83] 58

Table 3-4 Floods Mitigation Approaches Comparison................................. 67

Table 4-1 a comparison between RSRR and RARR scenarios................... 73

Table 4-2 Sets, variables and parameters for the scheduling MILP 74

Table 4-3 Input Data for the MILP model and heuristics 87

Table 4-4 Reservation Scenarios Comparison.. 93

Table 5-1 scenarios comparison 101

Table 5-2 Reservation Scenarios Comparison.. 115

Table 6-1 Sets, parameters and variables for the blackout MILP.............. 118

Table 6-2 Input Data for the dimensioning MILP Model 122

Table 6-3 Weighing Coefficients 124

List of Abbreviation

AR	Advance Reservation
ASIC	Application Specific Integrated Circuit
BCP	Business Continuity Plan
CAPEX	Capital Expenditure
CO	Central Office
DC	Data Centre
DLE	Dynamic Lightpath Establishment
DRP	Disaster Recovery Plan
EDFA	Erbium Doped Fibre Amplifier
EER	Energy-Efficient Routing
EETRR	Energy-Efficient Traffic Rescheduling and Rerouting
EETRS	Energy-Efficient Traffic Re-Scheduling
EETS	Energy Efficient Traffic Scheduling
FFR	Floods with Fixed Routing
FPPR	Floods with Protection Paths Rerouting
FRDS	Floods with Rerouting and Differentiated Services
FSTF	Floods with Selective Traffic Filtering
FTRS	Floods with Traffic Re-Scheduling
FTS	Floods with Traffic Scheduling
FWPPR	Floods with Working and Protection Paths Rerouting
GMPLS	Generalised Multi-Protocol Label Switching
IFAR	Immediate and Fixed Advance Reservation
IFSAR	Immediate, Fixed and Sliding-window Advance Reservation

ILP	Integer Linear Programming
IR	Immediate Reservation
ISP	Internet Service Provider
LCP	Least Congested Path
LRR	Lightpath ReRouting
NLP	Non-Linear Programming
MILP	Mixed Integer Linear Programming
MLR	Multi-link Rate
OADM	Optical Add Drop Multiplexers
OEO	Optical-Electronic-Optical
OPEX	Operational Expenditure
OXC	Optical Cross Connect
QoP	Quality of Protection
QoR	Quality of Resilience
QoS	Quality of Service
RARR	Rescheduling Active and Reserved Request
RSRR	Rerouting AR Reserved Requests
RWA	Routing and Wavelength Assignment
SDN	Software Defined Network
SLA	Service Level Agreement
SCADA	Supervisory Control And Data Acquisition
SLE	Static Lightpath Establishment
SRG	Shared Risk Group
SRLG	Shared-Risk Link Group
TF	Time frame

TV	Time video
VM	Virtual Machine
VoD	Video on Demand
VoIP	Voice over IP
WDM	Wavelength Division Multiplexing
WESO	Weighted Energy Sources Optimisation
WMD	Weapon of Mass Destruction
WRR	Wavelength ReRouting

1 Introduction

Nowadays networks have an essential job in our daily life because of the increased amount of digital information they handle. The networks are responsible for delivering these digital services between the society (people and businesses) and Data Centres (DCs). DCs provide diverse services such as web traffic, social networks, cloud computing, video-on-demand, and other services. The importance of DCs has increased with the increasing popularity of cloud computing services with most of the organisations moving their IT services and computing resources to the cloud. Thus, networks are playing an integral part in this chain (as shown in Figure 1-1) demanding a reliable high bandwidth network infrastructure.

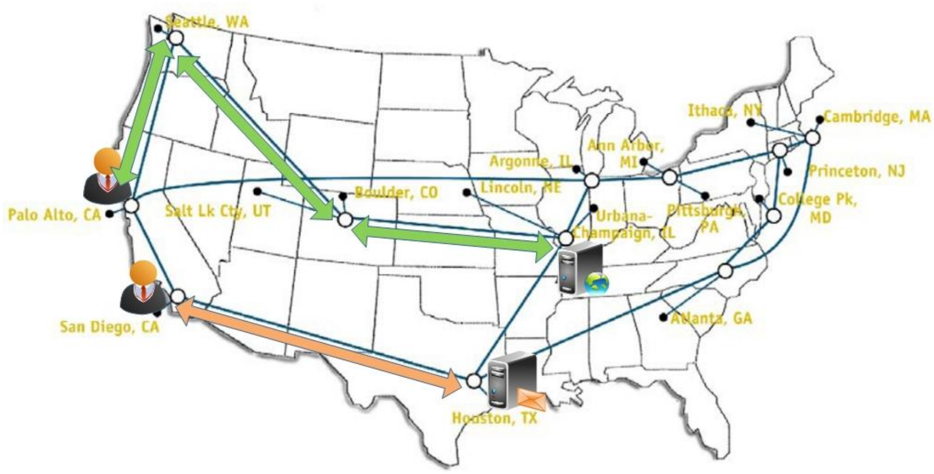


Figure 1-1 Society, Network and Datacentre

Recent years have witnessed a rise in the number of disasters whether natural, technological or man-made that impact the infrastructures. This rise has triggered research efforts to build disaster resilient technologies. The aim of these technologies is to reduce the risk of disasters and mitigate its disruption consequences. One of the growing research fields is disaster-resilient networks. Building a disaster-resilient network is a crucial requirement for network operators to avoid or minimise network outages during and after disasters, as communication networks are essential in the rescue and evacuation process and to ensure business continuity.

Disasters have a direct and indirect impacts that affect networks. The direct impacts can be represented by hardware failures such as link cuts or equipment destruction in central offices or DCs due to building destruction. This type has been studied thoroughly covering link failures, nodes outages and DCs isolation. On the other hand, the indirect impacts can be represented by the impacts of power outages at some nodes and the increased post disaster traffic as customers use of the network surges to share information, which are both less investigated.

The indirect consequences can have a similar impact as the direct ones. For example, during disasters network congestion can happen due to network degradation or due to high levels of generated traffic. The recent data usage trends predict that an early network exhaustion can happen due to excessive access to viral (for example video) content and applications. Although, network operators usually work on resource upgrades for the long term traffic growth to avoid such an exhaustion, this short term congestion might happen due to unpredictable and unprecedented circumstances.

National grid disruption is one of the expected consequences during catastrophic disasters such as earthquakes, Electromagnetic Pulses (EMP) and flooding. Power outages consequently lead to network operations disruption, similar to what happened in Japan during the 2011 Earthquake that left 1500 telecommunication switching offices without power [1].

In this work, the main focus on large size disasters that have an impact on the nationwide, but without network infrastructure degradation. For example, when ISIS invaded Iraq in 2014, the networks was fully functional but the event was a catastrophe for the whole Iraq. In Italy in 2003, a substation failure led to communication network switch shut down [2]. Consequently this shut down causes a failure in the SCADA power control system which causes more substations failure and led to a total blackout.

This thesis addresses two disaster related issues which are the short-term capacity exhaustion and power outages. Mitigation approaches are proposed to reduce the consequences of such events. MILP models and real time heuristics are developed to evaluate the network performance under these approaches.

1.1 Research objectives

The primary research objectives of this thesis are as follows:

- Study the optical network performance under short-term capacity exhaustion which happens after disasters due to the increase in traffic.
- Propose mitigation approaches to reduce the short-term capacity exhaustion.
- Study energy savings that can be achieved in optical core networks in such disaster scenarios by exploiting the flexibility provided by sliding-window advance reservation requests.

- Propose rescheduling and rerouting mechanisms to improve the power savings. Evaluate the network performance and power consumption using the proposed scenarios. Explore the impact of traffic utilisation and sliding-window sizes on power saving.
- Exploit the flexibility of AR requests in post-disaster times to mitigate the short-term capacity exhaustion. Use the AR reprovisioing approaches to accommodate the traffic increase and improve the network blocking.
- Investigate the network performance during power outages with limited alternative power supply and propose mitigation approaches to extend the network life time during the blackout.

1.2 Original contributions

The research main contributions are summarised as follows:

1. Investigated the issue of network short-term capacity exhaustion due to the surge of post-disaster traffic floods. Five mitigation approaches are proposed to absorb the floods and reduce the network blocking probability. MILP models and heuristics are developed to optimise and evaluate the approaches. The approaches were evaluated on a realistic network topology to show how the mitigation approaches perform to reduce the blocking.
2. Proposed two approaches to reduce the network power consumption during provisioning of the advance reservation requests in IP over optical networks. The approaches are based on reschedulling and rerouting the advance reservation requests. MILP model and heuristic approaches are developed to optimise the network performance under

the proposed approaches. The MILP model is used to optimise a sample network while the heuristics are used for small and larger network topologies.

3. Developed a mathematical optimisation model along with a heuristic for mitigating post-disaster traffic floods using the developed reschedulling approaches. The approaches are used to exploit the advance reservation flexibility for serving the post-disaster traffic floods while minimising blocking. The proposed approaches are evaluted using a sample network and a large network topology.
4. Designed a blackout resilient core network and developed a mathematical model to optimise the power (grid, renewable and backup batteries) usage in the optical core network during power outages to extend the network life time and minimise the network outage.

1.3 Related publications

1. Z. Nasralla, T. El-Gorashi, M. Musa, and J. Elmirghani, “Routing Post-Disaster Traffic Floods in Optical Core Networks,” in 20th IEEE International Conference on Optical Network Design and Modelling, May 2016.
2. Z. Nasralla, T. El-Gorashi, M. Musa, and J. Elmirghani, “Routing post-disaster traffic floods heuristics,” in IEEE Transparent Optical Networks (ICTON), 2016 18th International Conference on, July 2016.
3. Z. Nasralla, T. El-Gorashi, M. Musa, and J. Elmirghani, “Energy-Efficient Traffic Scheduling in IP over WDM Networks” IEEE International Conference on Next Generation Mobile Applications, Services and Technologies, September 2015.

1.4 Organisation of the thesis

Following the introduction in Chapter 1, the remaining parts of this thesis are organised as follows:

Chapter 2 provides a review of IP over WDM networks and building disaster-resilient optical core networks.

Chapter 3, studies the issue of post-disaster traffic floods and their impact on the core network. Five mitigation approaches are suggested to alleviate the floods. Mathematical models and heuristics are presented to evaluate the network performance under the proposed approaches.

Chapter 4, studies advance reservation requests in optical core networks and proposes two scenarios for rescheduling and rerouting the advance reservation requests to achieve higher power savings. Mathematical MILP model and heuristics are presented to evaluate the network performance under the proposed scenarios.

Chapter 5, uses the developed scheduling approaches to mitigate post-disaster traffic floods. MILP model and heuristic approaches are developed to minimise blocking during post-disaster floods.

Chapter 6, Studies the blackout impact of blackouts optical core network and develop a blackout resilient optical network. A mathematical MILP model is developed to optimise the power usage during blackout

Finally, Chapter 7 concludes the thesis with a summary and tentative future research topics.

2 Background and Related Work

2.1 Introduction

The optical core network is an intermediate (core) section in the network that interconnects the different access networks and DCs throughout a country. This role is important in handling traffic which in most cases traverses the core network. Therefore, building a resilient core network is essential in maintaining this connectivity and ensuring Quality of Service (QoS).

Resilient technologies can be added in different network layers starting from the physical connectivity to the content availability. Building resilient networks can be studied against a single failure at a time, multiple uncorrelated failures or disaster failures which are multiple correlated failures [3]. Each of these failure scenarios requires specific mitigation approaches but obviously combating disasters is the most challenging failure.

Most of the research in building disaster resilient networks focuses on studying network infrastructure failures due to hardware failures. Power outages have never been considered although it causes a similar impact. High traffic injection that stimulated by disaster events is less considered although it degrades the network performance.

This chapter provides an overview of the IP over WDM network architectures. In addition, a literature survey of the work done in building disaster-resilient optical networks is presented. Finally, open challenges are discussed in building disaster-resilient networks.

2.2 IP over WDM Networks

IP-based traffic is the dominant traffic in ubiquitous internet services so that networks and applications have become very IP-centric. The IP layer is the layer responsible for connecting the heterogeneous networks by solving the addressing and routing problems. While the WDM layer is currently the only underlying technology that provides enormous bandwidths for such applications and traffic. The mixture of these two layers means a powerful, reliable, cost-effective, and scalable system.

Integrating WDM with IP, involves adding a layer to control and manage the optical devices such as the Optical Add Drop Multiplexers (OADM) and Optical Cross Connects (OXC) and interface with IP layer [4]. The optical layer offers a service to upper layers in the form of fixed bandwidth transport pipes (optical paths). The control layer has received substantial research and development attention to realise more intelligent, flexible, survivable and controllable architectures. There are three different control mechanisms which place control in the IP domain or in the optical domain. These control planes are Multi-protocol Label Switching (MPLS)-based which was introduced in MPLmS and Generalised Multi-Protocol Label switching (GMPLS); and more recently control through Software Defined Networking (SDN).

2.2.1 IP over WDM Components

The IP over WDM core network node shown in Figure 2-1 usually consists of the following equipment:

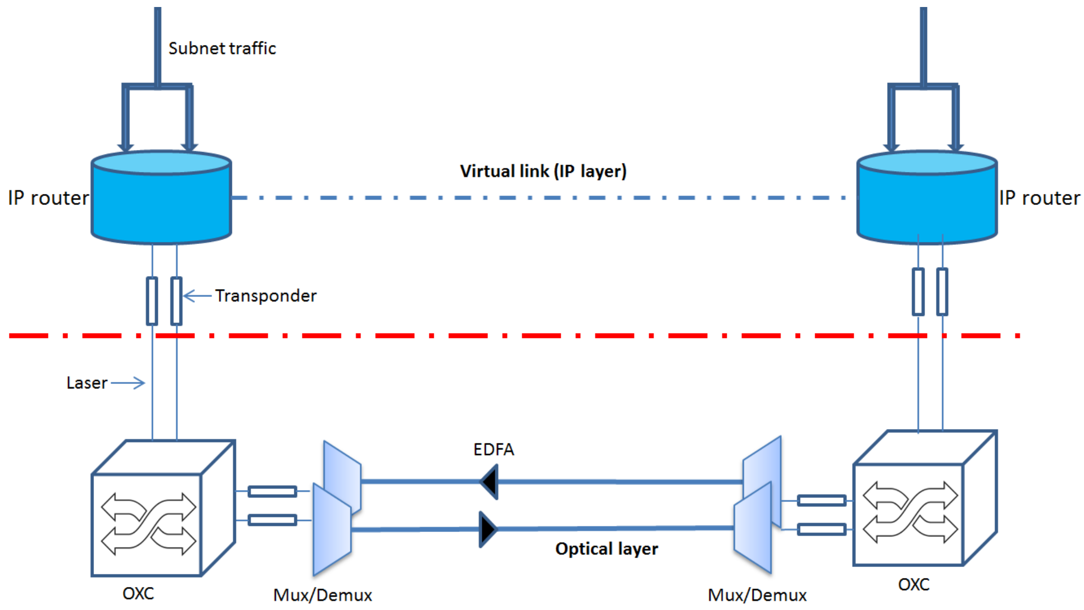


Figure 2-1 IP over WDM two node architecture and interconnection

IP routers

The IP routers represent the only electronic part of the core node. They act as an interface for traffic aggregation from the metro networks to the core optical networks. They are also responsible for routing decisions. The IP router is connected to the optical switch (OXC) via short reach optical interconnects.

Optical Cross Connect (OXC)

OXC is the most important part in the WDM layer. It acts as the interface between the edge router and the optical network. The OXCs work as a cross-connect which means connecting input (*i*) with output (*j*) by using preconfigured cross-connect tables. When establishing a lightpath through the core network, all the OXCs which are ingress, egress and intermediate should be configured according to the cross-connect table to allow the lightpath to pass physically through them. In general an OXC has the ability to wavelength convert an incoming optical signal to facilitate routing or remove OXC blocking.

Multiplexers/Demultiplexers

Multiplexers**/**Demultiplexers are used to combine/separate the multiple wavelengths carried in the fibre to be switched inside the OXC.

Transponders

The optical transponders are used for electronic to optical or optical to electronic signal conversion and for long distance transmission between core network nodes. These transponders connect the node with the optical transport networks.

Erbium Doped Fibre Amplifier (EDFA) and Regenerators

An EDFA is an optical amplifier that represents the key component for enabling the WDM system to efficiently transmit signals for long distances with the span between EDFAs typically reaching up to 80 km. The gain of the EDFA reaches to 30dB, but the amplification does not provide reshaping of the digital stream or re-timing the digital bit stream. EDFAs are however data rate transparent with no need for upgrade when the data rates are increased provided the signals are able to fit within their 30 nm (approximately 3 THz) bandwidth. The EDFA solves the problem of attenuation, but to overcome the distortion problems regenerators should be used.

2.2.2 IP over WDM Architectures

Basically, there are three different core architectures to interconnect the IP networks with WDM networks from physical architecture point of view. These architectures differ in the way they deal with the pass through traffic for the intermediate nodes and the degree of agility provided in the optical network. OXCs are able to handle large data volumes, but only in circuit switching configurations. IP routers have comparable capacities to OXCs, but handle packet routing, thus operate at a finer granularity. In addition, the footprint occupied by the OXC is less than that occupied by the IP router, and the cost per router port for the OXCs is less than that for the IP routers.

In the basic configuration, the IP router is connected directly to the optical fibres through transponders. In this model, no optical switching available and all the decisions are made by the IP router after converting the optical signal to electronic signal which is then processed by the router and finally converted back to optical to be sent to the next node [5].

In the opaque configuration, the OXC is connected to the IP router through short-reach interfaces. All the traffic should be converted by transponders from optical to electronic and then back to optical. The traffic is either sent to the router for termination or grooming or if no grooming is required, the traffic is switched by the OXC directly.

In the transparent configuration, the OEO conversion is required only when grooming or regeneration is needed. Otherwise, the signal can bypass the electronic part of the node directly and is switched by the OXC. This model is considered less complex than the others. It saves power by bypassing the electronic functions in the node, but equally does not get access to the electronic layer at intermediate nodes, so cannot perform deep packet inspection of implement firewalls at intermediate nodes.

The last configuration is the translucent configuration. It is similar to the transparent configuration except that each node is equipped with 3R regenerators that are connected to the OXC. This means that if regeneration is required at the intermediate nodes, then there is no need to terminate the traffic in the IP router. While grooming still should be performed at the IP router.

Regarding the manner in which traffic passes through a nodes, there are two approaches. These are the bypass and non-bypass architectures [6]. In the bypass model, the optical domain is responsible for traffic forwarding at the intermediate nodes, while in non-bypass approach, the traffic should be terminated at the IP router and then converted to optical and forwarded again based on the routing table and this approach is similar to the basic IP-over-WDM network architecture [7].

2.2.3 Routing and Wavelength Assignment in WDM Networks

In WDM networks, the end users can communicate via all-optical channels which called lightpaths [8]. To establish a lightpath, first must select a path or physical link to pass over and this problem is called routing problem, as well as allocating the available wavelengths for this lightpath which is wavelength assignment problem. The lightpath can span one fibre link or more along the end-to-end connection and using the same wavelength. This property of is called wavelength-continuity constraints. In heavy loaded networks, it is difficult to ensure that the used wavelength is not used by other connection on the same fibre link, which causes blocking. Hence, to overcome this problem, the lightpath should change its wavelength according to the available wavelengths on that fibre [4]. The problem of setting up a lightpath by routing and assigning a wavelength to each connection is called Routing and Wavelength Assignment Problem (RWA).

There are three types of connection requests: static, incremental, and dynamic [9]. With the first type, the complete set of connections is known in advance, and the problem is then to setup lightpaths for these connections in an overall manner and attempt to minimize network resources such as the number of wavelengths or the number of fibres in the network. Otherwise, one may attempt to setup as many of these connections as possible for a predetermined fixed number of wavelengths. This problem for static traffic is known as the Static Lightpath Establishment (SLE) problem. The SLE problem consists from two sub-problems the routing and wavelength assignment and each one solved individually. In the incremental-traffic case, connection requests arrive sequentially, a lightpath is established for each connection, and the lightpath remains in the network indefinitely.

For the case of dynamic traffic, a lightpath is setup for each connection request as it arrives, and the lightpath is released after some finite amount of time. The objective in the incremental and dynamic traffic cases is to setup lightpaths and assign wavelengths in a manner that minimizes the amount of connection blocking, or that maximizes the number of connections that are established in the network at any time. This problem is referred to as the Dynamic Lightpath Establishment (DLE) problem. The DLE problem is more difficult to be solved; therefore heuristic methods had been proposed to solve it for both the routing and wavelength assignment. For the routing there are three basic strategies which are fixed routing, fixed-alternate routing and adaptive routing. For wavelength assignment problem there are ten heuristic algorithms [10] which are random wavelength assignment, first-fit, least-used, most-used, min-product, least loaded, MAX-SUM, relative capacity loss, wavelength reservation, and protection threshold.

2.2.3.1 Routing Types

As mentioned earlier there are three types of routing which are:

A) Fixed Routing

The most straightforward strategy is to route a connection on a fixed route for a given source-destination pair. The shortest path is one of these approaches. This approach could be implemented using Dijkstra algorithm or Bellman-Ford algorithm to calculate the shortest-path offline for each source-destination pair and store these predetermined routes. This approach could be used for static case only; otherwise, it can lead to high blocking probability in the dynamic case. Furthermore, in link faults it is difficult to change the route.

B) Fixed-Alternate Routing

This approach is similar to the first one but with enhancement. The enhancement is by calculating multiple routes between the source-destination connections and stores these routes in a routing table; whenever there is a problem in the primary route, there should be alternatives routes to it in the routing table. The routing table contains the shortest path, the second, third, etc. The alternative routes should be link-disjoint from the primary route. This approach reduces the blocking probability of the fixed routing, but if the number of alternative routes less than three it can increase the blocking probability as compared with full wavelength conversion and fixed routing.

C) Adaptive Routing

Using this approach will dynamically choose the route between the source and destination based on the current network state. The shortest-cost path routing is one of the adaptive routing algorithms. In this algorithm, the link cost is considered when calculating the shortest path. The link cost depends on whether the link is used or unused and the availability of wavelength conversion on it. This algorithm requires extensive support from management and control protocols. The blocking probability is lower than the previous approaches. The Least Congested Path (LCP) routing is another example of adaptive routing [11]. It is similar to fixed- alternate routing, there are pre-computed fixed alternative routes and chosen based on the least congested. The congestion is measured by the number of wavelengths currently handled by the link. The disadvantage of LCP is the complex computation required.

2.2.3.2 Wavelength Rerouting Approaches

In fixed routing approach, it is not straight forwards to reroute a lightpath on the run, unless there is a backup path already configured. To reroute the optical path there are two approaches and it depends mainly on whether wavelength conversion is used in the network or not. If wavelength conversion deployed, then Wavelength ReRouting (WRR) should be used [12]. In this approach, the lightpath should be rerouted first then wavelengths should be reassigned on the new path. This approach requires partial rearranging. The second approach where wavelength continuity constraint used, then the whole lightpath should be rerouted and it is called the Lightpath ReRouting (LRR) [13]. In this approach the lightpath should be rerouted and a new wavelength should be assigned to it. This approach requires full rearranging and it is also referred to as non-blocking rearrangement.

Although rerouting improves the network utilisation, but it has a drawback which is to shut down the original route of the rerouted path till configuring the new route. This disruption is higher in LRR as it requires full rearrangement and it is lower in WRR [14].

There are a number of research papers that have proposed solutions for both rerouting techniques, for example [15–17] developed algorithms to do the wavelength rerouting. While in [14], [18–20], the lightpath rerouting approach considered. All the proposed solutions considered using algorithm for both the rerouting and the new wavelength assignment.

The authors in [21], [22–24] have considered a passive rerouting, that means a rerouting would take place whenever a new lightpath demand is to be blocked. While in [24], the authors considered rerouting to improve the resources allocation. On the other hand, the authors in [25] have considered an online rerouting scheme to adapt to the current traffic load. In [26], the authors proposed a new hybrid approach that mixes both passive and active rerouting approach, as they did active rerouting for the lightpaths while passive rerouting for the wavelengths.

2.3 Disaster Resilient Networks

Communication networks have become an essential part of our daily life due to the number applications and services they provide. Network outages represent substantial economic and social disruption. In addition, these outages can have a great influence on the Internet Service Providers (ISPs) reputation and revenue. Such an outage can mainly happen during disasters, so building disaster-resilient networks is essential to avoid such a consequences.

Disasters are events which may cause a significant, adverse or disruptive impact on humans, assets or the economy. Disasters can be classified into three types according to their cause: natural disasters, technological or man-made disasters [3]. The natural disasters include earthquakes, hurricanes, volcanos and floods. The technological disasters include system malfunctions, blackouts, nuclear meltdown and construction collapse. While man-made (deliberate or accidental) disasters include Weapon of Mass Destruction (WMD) or Electromagnetic Pulses (EMP).

Generally, disasters evolve through three phases which are pre-impact, trans-impact, and post impact [27]. In the first phase, the hazard vulnerability and emergency preparedness is studied. The second phase is a complete paralysis period where the disaster impact is growing and spreading so the effect of the disaster is still unknown whether superficial or severe. The last phase is the post-disaster period where the recovery process starts.

For communication networks, there are three scenarios for studying expected failures: single failure at a time, multiple uncorrelated failures, and multi-correlated failures (disasters) [3]. The third type is the main concern for the surveyed literature.

Building disaster-resilient networks has attracted research efforts recently. Avoiding or reducing the effect of disasters is very important because of two aspects: economic impact as a result of the loss of revenue due to service disruption and humanitarian issues [28]. Disaster evacuation operations rely on communication networks.

2.3.1 Disaster Risk Evaluation

The disasters are risky events where risky means probable and uncertain. The uncertainty could mean any negative-effect event such as earthquakes, hurricanes, tsunamis, Weapon of Mass Destruction (WMD) and others. All these events may happen and may not which means they have probable occurrence. Dealing with these probable events can be based on probabilistic or deterministic approaches [27].

In the deterministic approach, the probability of disaster occurrence is 1, and mitigating the disaster should be done without caring about the probability of hazard occurrence [29]. This type disregards the cost as a design constraint and focuses on building a reliable system. For example, choosing a location for building a DC. Such a location should be a risk-free/low risk location even if it is expensive, as the risk should be minimised.

The probabilistic approach deals with hazards based on their risk value. Basically, the risk is the product of hazard impact by its occurrence probability [30]. There are two schemes for evaluating probabilistic risk: qualitative and quantitative. In the qualitative approach, the procedure includes identifying all the expected hazards, estimating the impact of each hazard (1-10 for example), likelihood (1-10), and the recovery time. After finding the risk value for each hazard, the hazards are sorted in descending order and the cost of each downtime scenario is identified. The cost and risk value are determined to identify the hazards to be mitigated. The cost can be noticeable (such as revenue) or hidden (reputation). This scheme is adopted for example by companies in preparing their Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) [31].

The quantitative approach is the second type of the probabilistic models. This approach uses mathematical and economical approaches for evaluating the risk value, and it is more complicated than the qualitative approach. In this type, the disaster risk is used as an objective that should be minimised. The risk here could be represented by lost data, SLA, risk cost or outage time. However; there are more variables related to disasters that could be considered to make the calculations more realistic such as disaster type, how long it takes, the time of occurrence and the impact likelihood such as that used in [28]. As an example of impact likelihood, an earthquake has different occurrence likelihood but also the probability of the earthquake with 3 Richter severity is different from an earthquake with a magnitude of 7 on the Richter scale.

2.3.2 Disaster Mitigation Approaches

Being risk-averse reduces the disruptive consequences of disasters. Generally, there are four ways to manage risks which are: accept it, transfer it, eliminate it or mitigate it [27]. Accepting the risk means the impact of the disaster is not harmful. Transferring the risk is done either by insurance or hedging. Eliminating the risk can be very difficult and expensive to achieve, hence it is not preferred. The mitigation approach can be the most practical approach. There are two mitigation strategies either reducing the impact of a disaster or reducing the likelihood of a disaster.

The recovery mechanisms for building risk-aware networks have been classified into five categories according to domain, layer, sharing, set-up and scope [27]. Here, the classification that identifies when the recovery resources are set-up is adopted. Generally, there are two approaches under this classification: the re-active and pro-active recovery processes. The reactive approach is based on a restoration process which adapts the situation after the disaster, while the pro-active approach is based on a protection process. The first approach is cheaper, slow and flexible, whereas the second approach is robust, faster and expensive [32].

The optical network consists of physical and virtual entities as shown in Figure 2-2. The virtual entities are represented by the connection (lightpath) that traverses physical nodes and links, and the data stored in servers. The disaster can result in complete or partial failures of physical equipment (links and nodes) which can lead to a complete disconnection and consequently leads to lightpath failure.

The protection approach requires deploying redundant resources which can be either physical or virtual entities. The physical entities means extra hardware is installed, while virtual entities mean virtual copies of the entity to be protected are created and embedded into different hardware resources.

The restoration technique attempts to serve the maximum traffic requests by fulfilling the available resources with minimum blocking probability. These techniques seeks to restore the connectivity by rerouting the traffic on either pre-planned restoration routes or on-line through dynamically-computed restoration routes.

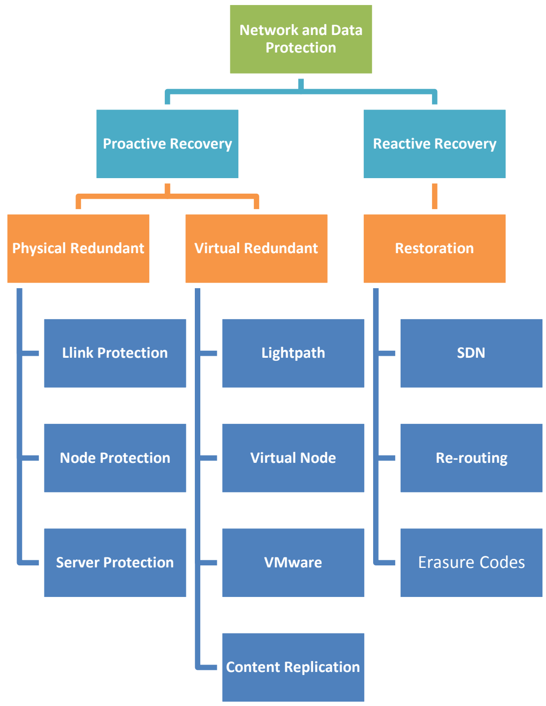


Figure 2-2 Protection classification

In resilient network design, there are a number of variables that can be constrained or unconstrained depending on the designer objectives. These objectives can be the cost of protection, blocking probability, latency (recovery time), Service Level Agreement (SLA), and reliability/risk. The optimization of resilient networks can have the minimisation/maximisation of one or more of these variables as its objective depending on the operator requirements.

If the operator is looking for a risk-free network then the cost will increase by building a backup(s) network to eliminate the risk, but this is not a realistic approach. On the other hand, one of the possible scenarios is to build a reliable network, which means evaluating the hazard vulnerability based on its impact, occurrence probability and location, and then provide Differentiated Quality of Protection (DQoP) depending on the hazard risk value.

Depending on the different SLA liabilities, the ISPs can use different mitigation strategies to meet the needs of the different traffic classes. Each strategy means adding extra cost (in terms of CAPEX and OPEX) for example adding redundant backup resources (storage, links or ports) will increase the resource cost and its operational cost. Thus; these strategies can be used to provide multiple degrees of resilience for different customer classes and this is known as differentiated Quality of Resilience (QoR) [33]. For example, BT provides redundant cloud service for extra fees on outsourced DCs.

Most of the design considerations focus on reliability, fast recovery, and low blocking probability after recovery while the power consumption has not received enough attention. Meeting energy efficiency and resilience simultaneously can be challenging, because building resilient networks means in many cases more cost to provide backup network resources which consume power (if not set in sleep / low power modes for fast wake up on disaster). Furthermore, resilient networks may choose long reliable paths to avoid high-risk areas instead of shortest paths [34].

2.3.2.1 Pro-active Disaster Recovery Approaches

There are a number of strategies that can be used to prepare the network to face a disaster with minimal effect. These solutions attempt to prepare the network to continue to function when disasters materialise. The proactive preparations mainly focus on putting redundant resources as backup that can be used in case of failure in the primary equipment.

A) Physical Redundancy

The concept of protection is designed for combating path/link failures by allocating additional backup resources on a disjoint path/link, so in case of a main link failure, the traffic is switched over to the redundant path/link immediately. The concept of protection is mainly based on offline routing. In optical networks, the protection routes are pre-computed to allocate wavelengths to each lightpath.

Schemes for protection against dual link failures are difficult to extend and use for multi correlated failures. Protection against correlated failures is difficult to achieve using a deterministic approach as finding alternative routes becomes difficult, thus using a probabilistic approach is more realistic [34].

Building a disaster resilient network by assessing the vulnerability of different disaster zones based on geographic location based probability of occurrence can be done using the concept of Shared-Risk Link Group (SRLG) [35]. This approach attempts to identify the shared risk zones and the collocated links within these regions and then provision the primaries and backups to be SRLG-disjoint. This problem is NP-complete as proven by [36] and should be implemented in a real time fashion through heuristics, so the authors addressed the problem of finding diverse routes with minimum joint failure probability (maximum reliability) by using the concept of probabilistic failures for SRLG. They built an Integer Non-Linear Programming (INLP) model to solve the problem of diverse routing. In [37], the author extended the concept of [36] by taking into consideration traffic engineering issues after the probabilistic multiple link failures.

In [38], the authors evaluated the risk associated with the NSFNET network topology based on the US seismic hazard map. They used the US seismic hazard map and evaluated the disaster zones, as the nodes and links collocated within these zones would be affected. The authors used two probabilities to evaluate the risk of disasters, which are the probability of disaster and the probability of damage from that disaster. They used minimising the risk (i.e. penalty of link outage) as the objective function and provided 1+1 protection.

The work in [28] takes the broad picture of the seismic map for the city as a whole, while the work in [38] finds the appropriate geographical routes for network links under a cost constraint to maximise the robustness of the network. Their findings show that the shortest-path is often the lowest risk path, but sometimes long detours might bypass high risk areas resulting in more resilience against disasters.

One of the most essential design considerations is building the data centres in a safe place, whereby a location is not vulnerable to man-made attacks or natural hazards and is located as far as possible from such risky geographic areas. Another important point is to locate DCs in areas close to renewable energy sources such as hydro power sources, wind power farms or solar energy farms because the alternative power solutions are essential in case of normal power failure [39] and furthermore such sources reduce the carbon foot print of data centres. Any failure in DCs can potentially cause loss of large amounts of data and might lead to service disruption. Thus; the first step is to identify the best-nominated candidate’s areas for building the DC.

Traffic engineering wise, the selection of DC locations mainly concentrates on building DCs near hot nodes which are highly connected nodes that other nodes can reach with minimum distance/hops [39]. This aspect is essential in terms of latency, blocking, energy-efficiency and reliability. The reliability is also improved by reducing the path hops/distances, the shorter paths are less vulnerable to failures compared to longer paths in general.

After building a reliable DC, the content also should be handled. One strategy to minimise the impact of DC failure on service delivery, such as by being isolated from the core network, is by optimally locating replicas of content across DCs in multiple locations to guarantee that the content is not lost if any of the replicas becomes unreachable. Synchronisation time (replication time) should be optimised (within the day) to reduce the data loss due to the replicas being not updated [40].

In [40], the authors addressed the problem of disaster survivability by optimising content replication across data centres and providing disaster-survivable routing. They built an Integer Linear Programing (ILP) model and heuristics that provide path and content protection. They provide content protection through content placement and replication. They used the concept of Disaster Zone, which is similar to Shared Risk Group (SRG), where a disaster zone is defined to have a maximum radius of 160 km. In case of severe disasters, all the nodes and links will fail within this disaster zone. They evaluated the model with fixed DC locations while optimizing the content placement and replication. They have also checked the effect of increasing the number of DCs and the number of content replicas. In [41], the authors proposed a green and low risk content placement by using inter-DC content fragmentation instead of replication. The proposed approach was implemented by an ILP model, and the results showed that the content fragmentation outperforms the content replication in reducing both the power consumption and risk.

In [42], the authors attempted to minimise the probabilistic risk of WMD on DCs in proximity to military locations. As they are evaluating military content, they have used two metrics to replicate the content: popularity of the content, which is defined as the frequency of content access, and the importance of the content. They introduced two terms in evaluating the losses, which are the availability of content and reachability, as they differentiate between the content being not available and not reachable due to a disaster. They used the risk as an objective in building the network and proposed two approaches which are the disaster-aware and unaware designs. The results showed enhancement in survivability of 62% in disaster-aware design compared to unaware design.

B) Virtual Redundant

One of the most powerful techniques which save the network and servers after a disaster is virtualisation. Virtualisation in this context means realising computation and network functions in virtual servers, nodes and links and embedding such requests in different physical infrastructure. There are three techniques of interest: server virtualisation, network virtualisation and infrastructure virtualisation.

The concept of Virtual Machines (VMs) is widely used in virtualising servers; this technique can be useful mainly in resource efficiency, and also in keeping virtual backup of a server on different storage resources. This advantage can be deployed in fast disaster recovery, by optimally distributing the VMs in different DCs. The system should assign each VM two storage resources one local and the other remote to guarantee the availability of the application data [43]. Delay here is a critical parameter that should be addressed because VMware applications are generally delay sensitive. The second issue is distributing the VMs in different nodes. This should care about the distance between the two copies of the VMs because putting them far increases the delay and consumes more bandwidth. The number of hop between the two VM copies should be optimised by minimising the maximum hop count for a reliable path.

In [43] the authors studied off-site data replication and virtual machine migration. They attempted to optimise the distribution of storage resources and computing resources among network nodes to support disaster recovery. They used four different optimisation approaches to assign the virtual machine into storage resources. The first approach limits the maximum delay between the VM and remote disk by optimising the bandwidth utilisation of the network. The second approach limits the number of hop count between the VM and the disk. The third approach deals with VM migration by limiting the number of working VMs on one site. The fourth appraoch limits both the hop and the number of VMs on a single site. The results of the fourth approach show the best compromise between bandwidth utilisation and disaster recovery time.

VM migration is another issue related to disaster recovery that should be addressed. It is crucial to optimally implement the migration process due to the large bandwidth requirement and delay-sensitivity. In [44], [45], the authors studied two optimisation scenarios for VM migration, the first scenario considers the availability of renewable energy and the second scenario considers bandwidth and routing optimisation.

The second approach in virtualisation is the Virtual Network Mapping. This approach should ensure that the virtual entity is replicated on different hardware. Second, identifying the shared risk groups, so mapping virtual entities should be not allocated in the same SRG. Finally, risk assessment of the disaster zones should be carried out to map the resources in a way that minimise the risk [46]. This approach ensures maximum network survivability after a disaster because the optimisation model identifies the probabilistic vulnerability and embed the virtual network based on disaster zone isolation.

The infrastructure (servers, nodes, and links) might be virtualised altogether, by considering the bandwidth (which represents network resources) and processing (which represents server resources) as virtual requirements. This joint model can map both aspects when building resilient systems and evaluating the survivability against regional disaster using probabilistic approach. The authors in [47], used the concept of building survivable virtual infrastructure mapping in federated computing and networking by assuming single regional failure. First, they developed a minimum cost MILP to embed the virtual infrastructure (which is represented by computing capacity and networking bandwidth) into the physical topology. They then simulated single regional failure at a time and attempted to provision the resources by embedding redundant virtual infrastructure into another physical node. The migration of a virtual network consumes resources from the host node, however, they built two heuristics. The first assumes the resources are unconstrained and then uses incremental optimisation with constrained mapping. These two approaches differ in cost and blocking probability after a disaster. But the results showed that the unconstrained heuristic has better failure recovery probability while the constrained approach provides cost-efficient solutions.

2.3.2.2 Re-active Disaster Recovery Approaches

In the post-disaster phase, the network topology might be modified due to the loss of network parts (i.e. link cuts or node(s) failures). Even with this reformed topology, the network should maintain its performance using a reactive approach. These approaches can work automatically without the need for manual reconfiguration.

Unlike the protection approach, restoration is similar to IP routing (best-effort) technology which means when a failure happens on the primary path, the network should search for an alternative path to use. This rerouting can be done in GMPLS networks using the RSVP-TE and OSPFF-TE protocols [48]. This technique is dynamic, flexible and unguaranteed; because there are no dedicated extra resources for re-provisioning.

Two important aspects affect the performance of fixed protection. Firstly, sometimes fixed protection cannot provision the demands if multiple failures that are not considered at the design phase occur [9]. Secondly, in failure cases, to make better use of network capacity, all the connections need to be rerouted to reutilise the network, because rerouting single failed demand might unbalance the links utilisation [13]. Using a mixture of the two strategies (protection and restoration) can provide better reliability but this is not cost-effective.

The reprovisioning of a primary path or backup path can be done online after a failure scenario. There are a number of approaches that have been introduced to solve this issue, although these approaches are not specific to disaster scenarios but can be used to any failure scenario. In [49], the authors built an algorithm for reprovisioning optical backup paths against multiple link failures using two scenarios either by reprovisioning failed backup path or rearranging the backups for the whole connections. In [50], the authors introduced the reprovisioning of temporarily unprotected connections for shared backup protection. They considered three scenarios: the first when the working paths fail and they are rerouted on the backup, the second when the working and backup path fail and finally when the connection is working while the shared backup is used by another failed connection.

Software Defined Networks (SDN) is one of the emerging techniques that provide a standardised open interface to the forwarding plane of a network device [51]. In SDN, the control plane is separated from the forwarding plane. The complexity of the forwarding plane is reduced as the responsibility of route updating (adding/deleting) is migrated to the control plane. The transport OpenFlow protocol is used for the communication between these planes.

The authors in [52] talks about SDN scalability due to its centralised operation, but this centralisation approach increases the load on the controller which requires high processing resources to handle the increased amount of requests.

SDN is considered to be more resilient to disasters, but there are three possible attacks that may cause harm and affect the network performance. The problem is that if a physical separation happens between the control and forwarding planes this in turn can cause packet loss and performance degradation. This problem can be solved by increasing the number of controllers or by using a distributed platform for the control plane which will reduce the latency [53]. In disaster recovery, updating the network topology can be done using proactive and reactive scenarios through programmed rules at the controller. SDN supports advanced techniques that can support disaster recovery such as source routing and live migration. In the source routing, the packet routing is performed based on data link layer using the ingress port. In the case of catastrophic disasters that affect the DC itself, the servers require fast recovery. The fast responded can be either by deploying virtual servers on different physical servers or by installing new servers in the same location and migrating the content to the new servers using SDN live migration techniques [54].

2.4 Linear Programming and Heuristic Approaches

Mathematical programming is a mathematical optimisation approach that used for modelling the planning or scheduling of a system by mathematical description. The purpose of using this type of modelling is to minimise or maximise an objective function considering some constraints [55]. This problem is solved by finding out the best solution from all feasible solutions.

Mathematical programming is classified according to linearity to two types which are either linear or nonlinear depending on constrains and objective operators. If the operators exhibit linearity then the model is linear model or otherwise it will be nonlinear model. If the variables are restricted integers then the model is called Integer Linear Programming (ILP), while if the variables are binary then the model is Binary Linear Programming (BLP). If the model has continuous, binary and integer variables then the model is called Mixed Integer Linear Programming (MILP). In linear programming, the variables are continuous and it could be solved in polynomial time while if they are integers then it will be NP-hard which means nondeterministic polynomial time hard [56].

The mathematical programming is one of the tools that can be used to design and control communication networks. The communication network is a multi-commodity flow problem where multiple traffic requests flow between the different source and destination nodes. The solution should find the optimum set of routes that the traffic request should follow from the source node to the destination node. Optimum can be based on different objectives such as minimum cost paths, shortest paths or minimum blocking paths [57].

The network operators starts the network design in practical environment by formulating it as an optimisation problem. First the network should be modelled in directed or undirected graph with two sets G = (V, E) as V represents the vertices (network nodes) and connected by edges (E) which represents the links. The objective function in network design may vary depending on the operator’s objective, such as:

1- Reliability: to design a reliable network, the objective function should maximise the availability by considering the vulnerability as a constraint.

2- Blocking: to design a network with low blocking probability then the objective should maximise capacity to accommodate traffic demands.
3- Cost: design a low cost network could be done by using minimise cost objective function and considering the operational and capital expenditures or one of them in the constraints and objective.
4- Power consumption: to design an energy-efficient network the objective should minimise the number of used devices by considering the consumed power in each part of the network.
5- SLA: satisfying the service level agreement and avoid its violation can be an objective to design a network for different SLAs at the same time.

Added to single objective demand there are also multi-objective function such as minimising both the cost and power consumption, or blocking with cost, different combinations can be made, and these objectives each one can have different weight. These weights can be adjusted using the coefficients in the objective function. When deign requires two different objectives at the same time, such as maximise capacity and minimise power, this is called duality problem.

In some cases where the LP approach fails to produce an optimal solution in polynomial time for large complex problems, it can be evaluated using a small data set, and then a sequential iterative algorithm can be used to mimic the LP performance [55]. The iterative algorithm is a computational procedure to find the solution for every instance of a problem in an iterative manner by checking each feasible solution whether it is optimal or not. This procedure stops when it finds out the optimal solution [57].

The algorithm should have a valid procedure and the produced results should converge from the LP results. The validity can be proved by checking whether the procedure satisfies the design problem. The convergence can be verified through the results, as the algorithm results should be as closer as possible to the LP results.

2.5 Disaster-Related Open Issues

There are several aspects that should be considered during the aftermath period of a disaster. Depending on the disaster impact and the affected portion of the network, the recovery plan should be selected. This plan should consider time schedule for the recovery process, the increased traffic request as compared with the residual resources (consequently the high congestion and high blocking probability). Also the power outages should be addressed to avoid early network die out.

2.5.1 Power System

For large size disasters which cause the shutdown or disconnection of the normal power system, thus an alternatives power solution should be available for powering the network infrastructure (Central Office and fibre repeaters). These alternatives include diesel generators, solar cells, wind power generators and backup batteries.

However; building a post-disaster energy-efficient network is essential due to limited renewable energy sources or battery charge. Energy-efficiency means using energy-efficient traffic engineering techniques whose objective is to minimise the resources used (consequently minimise the consumed power).

The renewable power (solar cells and wind power) should be installed outdoor, which might be affected by catastrophic disasters while the batteries are almost kept safe indoor. In [58], the authors suggested to build intelligent routing protocol that distributes traffic according to the remaining charge in batteries. In other words, building an intelligent system that controls the network traffic by assigning the light traffic to nodes with low remaining charge and avoiding network nodes that are about to shut off.

2.5.2 Congestion and Blocking

In post-disaster phase, the traffic requests are unpredictable, with traffic increase as a result of high requests or reduction caused by large access network outages, but however the traffic varies, it requires online traffic engineering techniques. These techniques should provide load balancing and better traffic utilisation, to reduce the congestion and blocking ratio. As explained previously, re-provisioning lightpaths (working and protection) is a prime solution to better utilise network resources and reduce blocking. Using traffic reduction techniques could enhance network performance such as compression, network coding technique or traffic filtration.

2.6 Summary

This chapter has provided a summary of the IP over WDM network architectures, disaster-resilient network technologies optical networks. Finally, it provided an outline of some open challenges for disaster related consequences that should be addressed in building optical core networks.

3 Post-Disaster Traffic Flood Mitigation in IP over WDM networks

3.1 Introduction

One of the issues that arise after disasters is the increased amount of traffic that contains voice calls, video and social media content. This traffic spark can cause a short-term capacity exhaustion. In this chapter, the impact of Post-Disaster Traffic Flood on the optical core network is studied. Five approaches are considered to improve the network performance during the flooding and MILP models are developed to optimise the network performance. Real time heuristics corresponding to the five approaches are also designed to mimic the MILP models performance. The MILP models and heuristics are evaluated using an example network topology.

3.2 Post-Disaster Traffic Floods

Large size terrorist attacks focused attention on a new issue of temporary capacity exhaustion that might affect communication networks. This issue is relatively different from the previous studied scenarios in building disaster-resilient networks as, in this case, the infrastructure is not affected physically but the heavy traffic on the network causes capacity exhaustion. This problem is a result of the increasing popularity of new applications such as social media applications that most people tend to use to get and share news and information during disasters [59–62].

Traffic tolerance as defined by Sterbenz in [2], "is the ability of a system to tolerate unpredictable offered load without a significant drop in carried load". The unpredictable traffic can come from two scenarios the first is legitimate which is like a content, video or an application going viral, the other is the malicious attacks such as the Distributed Denial of Service (DDoS). The DDoS attacks have a similar impact on network resources although it can be prevented. The legitimate one needs resolution because network operators should commit to SLA.

In [63], the authors show that two-thirds of people use social media during disasters and post-disasters, and that social media is used mostly during disasters to generate data such as tweets, posts, blogs, and videos. Another important aspect is that due to failures of mobile networks to accommodate the large number of voice calls [64], people tend to use social networks or VOIP applications to contact relatives and get in touch. In [65], the authors conducted a survey on the user behaviour during large size disasters and found that 95% of users make phone calls and 76% post information in social media. Added to social media, the news agencies and governmental websites issuing warnings and precautions also produces traffic. In [66], the authors showed a sharp rise in the popularity of video traffic of both types: real-time video streaming (TV breaking news) and video streaming (user-generated videos) after the Great East Japan Earth Quake and Tsunami.

This sudden traffic increase starts in the post-disaster phase. The shape of this increase is similar to the floods wave shape; it has a sharp surge in traffic and after a while it slowly starts decreasing until it returns back to usual traffic levels. This phenomenon could be called Post-Disaster Traffic Flood.

This flood can cause capacity exhaustion in the different parts of the network starting from access networks, to core and DC networks. The core network is the main concern of this study as it is responsible for delivering the traffic between the access networks and DCs and between cities.

Although the network capacity is already overprovisioned [67], this overprovisioning is not enough to serve the increased traffic, and installing new fibres is not feasible within few hours to accommodate the traffic changes [68]. This means traffic engineering approaches are required to adapt these changes.

The operator has to ensure service availability of 99.999% with good QoS [69], but in emergency times rules can be abandoned. And the operator can prioritise traffic types to accommodate as much traffic as possible and filter out traffic with lower priority. For example, entertainment services can be blocked while disaster-related information is served. As an example, online gaming traffic can be temporarily blocked to free capacity for the VOIP traffic to be served.

As shown in chapter two, most of the disaster-related work focuses on maximising availability during network failures. Limited research efforts have been dedicated to study the short-term capacity exhaustion that takes place after disaster. The authors in [70] and [71] have considered traffic anomalies caused by the short-term traffic increase and developed an algorithm for anomaly detection based on traffic monitoring at core nodes. After detecting traffic increase, the network is reconfigured to accommodate the traffic increase.

The authors in [72–75] exploited the excess capacity to improve network robustness by developing a MILP and a heuristic for new connection pre-provisioning and backup reprovisioning. During traffic fluctuation and growth, the algorithm frees protection resources to be used by the newly arrived connection request and then re-provisions protection paths with less availability protection schemes. During disasters, as the network suffers from resources degradation, it is efficient to use such an algorithm to serve more traffic.

3.3 Post-Disaster Traffic Floods Mitigation Approaches

At the post-disaster phase, the flooded node does not have a global view of the network, therefore it attempts to route floods using the already predetermined paths. The failure of this routing due to lack of enough capacity causes long traffic queuing and potential blocking, causing drop of traffic and long delays for the end user. Five approaches are proposed to minimise post-disaster traffic flood based on excess capacity exploitation, traffic filtering, rerouting and differentiated services.

3.3.1 Floods with Fixed Routing (FFR)

The routing table of the optical core network is predetermined for the working and protection paths and in case of an expected traffic increase, new wavelength is configured over the pre-computed path. Any traffic exceeding the capacity of the links of the pre-computed path is dropped.

However; exhausting the capacities of the configured pre-computed path does not necessarily mean the physical capacity has been exhausted as the network is designed with overprovisioned capacity. Exploiting the excess capacity by configuring new paths can absorb the excess traffic. This is considered the baseline approach.

3.3.2 Floods with Selective Traffic Filtering (FSTF)

In case the FFR approach fails to absorb the post-disaster traffic floods, then the operators can filter out less critical traffic temporarily to allow serving more disaster related traffic. Less critical traffic, such as file sharing, gaming and VoD, can be filtered out using port filtering [76] and deep packet inspection [77].

3.3.3 Floods with Protection Paths Rerouting (FPPR)

Although using the FSTF produces some improvements in terms of lowering the blocking of post-disaster traffic, it comes at the cost of dropping less critical traffic. One approach to accommodate post-disaster traffic while minimising the impact on other traffic is through the rerouting of protection paths away from flooded nodes to create capacity on the links around these nodes. The reprovisioning will not disrupt the traffic unless a failure happens during the reprovisioning operation.

Figure 3-1 shows an example of how FPPR works. Node 2 represents a flooded node. Rerouting the protection traffic away from its original path that passes through node 2 allows it to accommodate the flood traffic instead.

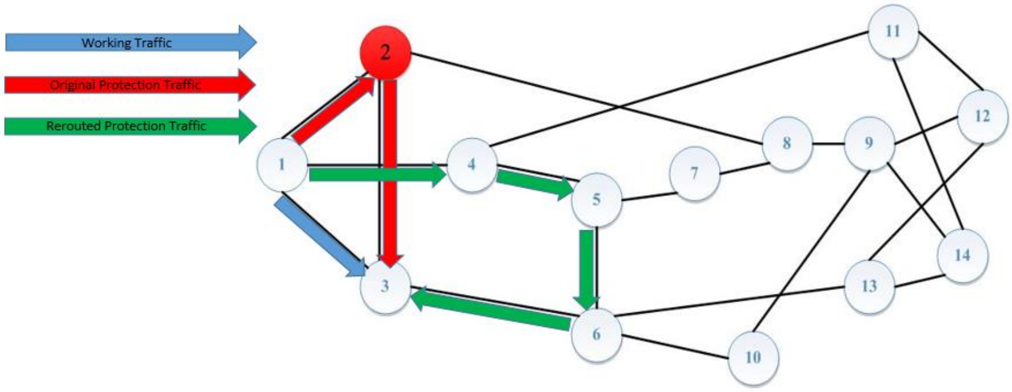


Figure 3-1 Protection Paths Rerouting to accommodate floods at node 2

3.3.4 Floods with Working and Protection Paths Rerouting (FWPPR)

In this approach, the working paths, in addition to the protection paths, are also rerouted. If the improvement as a result of rerouting both the working and protection is small compared to rerouting protection paths only, then a recommendation is made to the network operator that rerouting the protection paths is sufficient without the need to disrupt the traffic on the working paths, and if the blocking probability reduction is large, then a recommendation can be given to the operator to consider the potential of using dynamic networks.

Figure 3-2 shows an example of how FWPPR work. This example demonstrates how working paths rerouting can be beneficial for the flooded node. There are two concerns with this approach; the first one is that everything is disrupted until rerouting and reprovisioning is completed, unless an online routing technique is used such as SDN. The second is that some traffic requests get longer paths than the original ones and this might impact the non-delay-tolerant requests.

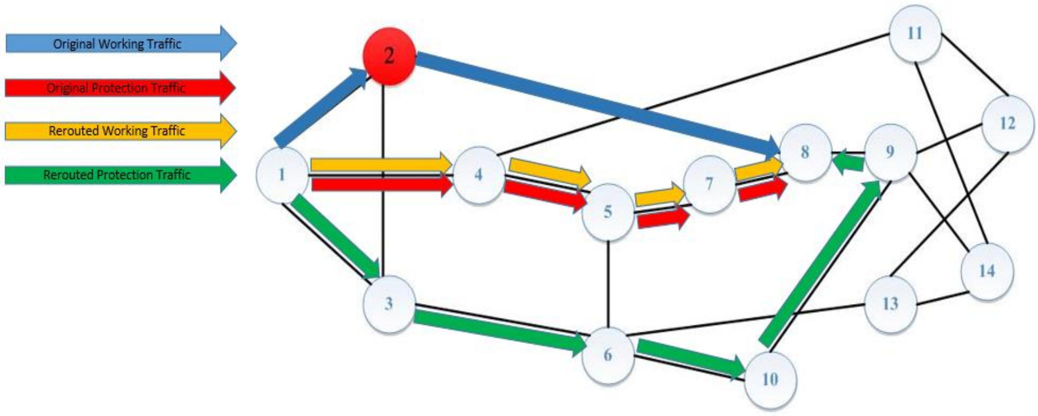


Figure 3-2 FWPPR scenario

3.3.5 Floods with Rerouting and Differentiated Services (FRDS)

In this approach, a hybrid approach is used that mixes the rerouting approach with Differentiated Services (Diff-Serv). In Diff-Serv, the traffic is classifieds into protected and best-effort requests [78]. For the protected type which represents critical traffic, the 1+1 protection is kept, while for less critical traffic it is canceled.

3.4 Network Design MILP Models

In this section two MILP models are presented. The first model is for dimensioning the network and determining the routing paths and the second is for evaluating the network performance under the different approaches introduced to deal with flooding.

3.4.1 Dimensioning Model

First, the network dimensions should be set in terms of capacities. A model was built to provision the working and protection paths for traffic requests at the busy hour to get the maximum capacity for the network links and build the routing table. The architecture used in is the non-bypass IP over WDM network architecture which is the most widely used core network architecture.

Protection was considered in the modelling and was implemented as 1+1 protecction which is the form of protection used in core networks [79]. The model objective is to build energy minimised network. Before introducing the model, the notations used are defined in Table 3-1.

Table 3-1 Sets, parameters and variables for the MILP

Notation	Description
N	Set of nodes
N_m	Set of neighbouring nodes of node m
s and d	Denote source and destination points of traffic request between two nodes
m and n	Denote end points of a physical link
λ^{sd}	Traffic request from node s to node d
P_r	Power Consumption of router ports (W)
P_t	Power Consumption of a transponder (W)
P_g	Power Consumption of a regenerator (W)
P_o	Power Consumption of optical switch (W)
P_e	Power Consumption of an EDFA (W)
B	Capacity of each wavelength in Gbps
W	Capacity of each fiber in number of wavelengths
RG_{mn}	Number of regenerators on physical link (m,n)
A_{mn}	Number of EDFAs on physical link (m,n) Typically, $A_{mn} = \left(\frac{L_{mn}}{s} - 1\right) + 2$, where s the distance between two neighbouring EDFAs and L_{mn} is the distance between (m,n)
α, β, M and U	Weighing coefficients
W_{mn}^{sd}	The number of primary wavelength channels in the virtual link (i , j) that traverse link (m,n)
$W_{mn_b}^{sd}$	Binary equivalent of W_{mn}^{sd} , equals 1 if W_{mn}^{sd} has a value greater than zero.
Wp_{mn}^{sd}	The number of protection wavelength channels in that traverse link (m,n)
$Wp_{mn_b}^{sd}$	Binary equivalent of Wp_{mn}^{sd} , equals 1 if Wp_{mn}^{sd} has a value greater than zero.
W_{mn}	The number of primary wavelength channels that traverse link (m,n)

Wp_{mn}	The number of backup wavelength channels that traverse link (m, n)
Wt_{mn}	The total number of wavelength channels that traverse link (m, n)
F_{mn}	Number of fibres in link (m, n)

Under the non-bypass approach, the total network power consumption is composed of:

1- Total power consumption of router ports

$$\sum_{m \in N} \sum_{n \in N_m} P_r \, W_{mn}$$

2- The power consumption of transponders

$$\sum_{m \in N} \sum_{n \in N_m} P_t \, W_{mn}$$

3- The power consumption of regenerators

$$\sum_{m \in N} \sum_{n \in N_m} P_g \, RG_{mn} W_{mn}$$

4- The power consumption of EDFAs

$$\sum_{m \in N} \sum_{n \in N_m} P_e \, F_{mn} A_{mn}$$

5- The power consumption of optical switches

$$\sum_{m \in N} P_o$$

The MILP model is defined as follows:

$\boldsymbol{Objective}$: $Minimise$

$$\propto \left(\sum_{m \in N} \sum_{n \in N_m} P_r \, W_{mn} + \sum_{m \in N} \sum_{n \in N_m} P_t \, W_{mn} + \sum_{m \in N} \sum_{n \in N_m} P_g \, RG_{mn} W_{mn} \right) + \beta \left(\sum_{m \in N} \sum_{n \in N_m} P_r \, Wp_{mn} + \sum_{m \in N} \sum_{n \in N_m} P_t \, Wp_{mn} + \sum_{m \in N} \sum_{n \in N_m} P_g \, RG_{mn} W_{mn} \right) + \sum_{m \in N} P_o + \sum_{m \in N} \sum_{n \in N_m} P_e \, F_{mn} A_{mn} \quad (3\text{-}1)$$

The objective function (3-1) aims to minimise the total network power consumption. Coefficients $\propto$ and β are used to select the best route for working path and for protection path respectively, where best means energy minimised path whether min-hop or shortest path.

Subject to:

$$\sum_{n\in N_m} W_{mn}^{sd} - \sum_{n\in N_m} W_{mn}^{sd} = \begin{cases} \lambda^{sd}/B & m = s \\ -\lambda^{sd}/B & m = d \\ 0 & otherwise \end{cases} \quad (3\text{-}2)$$

$$\forall s, d, m \in N : s \neq d,$$

$$\sum_{n\in N_m} Wp_{mn}^{sd} - \sum_{n\in N_m} Wp_{mn}^{sd} = \begin{cases} \lambda^{sd}/B & m = s \\ -\lambda^{sd}/B & m = d \\ 0 & otherwise \end{cases} \quad (3\text{-}3)$$

$$\forall s, d, m \in N : s \neq d,$$

Constraints (3-2) and (3-3) represent the flow conservation constraints for the working and protection traffic. These constraints ensure that the total outgoing traffic is equal to the total incoming traffic except for the source and destination nodes.

$$\sum_{s\in N} \sum_{d\in N: s\neq d} W_{mn}^{sd} = W_{mn} \quad (3\text{-}4)$$

$$\forall m \in N, n \in N_m,$$

$$\sum_{s\in N} \sum_{d\in N: s\neq d} Wp_{mn}^{sd} = Wp_{mn} \quad (3\text{-}5)$$

$$\forall m \in N, n \in N_m,$$

$$W_{mn} + Wp_{mn} \leq Wt_{mn} \quad (3\text{-}6)$$

$$\forall m \in N, n \in N_m,$$

$$Wt_{mn} \leq W\, F_{mn} \quad (3\text{-}7)$$

$$\forall m \in N, n \in N_m,$$

Constraints (3-4) and (3-5) calculate the total number of working and protection wavelengths in each link. Constraint (3-7) ensures that the total number of wavelengths in a physical link does not exceed the capacity of the fibres in the physical link.

$$M\ W_{mn}^{sd} \geq W_{mn_b}^{sd} \qquad \forall s,d,m \in N, \forall n \in N_m, \qquad (3\text{-}8)$$

$$W_{mn}^{sd} \leq U W_{mn_b}^{sd} \qquad \forall s,d,m \in N, \forall n \in N_m, \qquad (3\text{-}9)$$

$$M\ Wp_{mn}^{sd} \geq Wp_{mn_b}^{sd} \qquad \forall s,d,m \in N, \forall n \in N_m, \qquad (3\text{-}10)$$

$$Wp_{mn}^{sd} \leq U Wp_{mn_b}^{sd} \qquad \forall s,d,m \in N, \forall n \in N_m, \qquad (3\text{-}11)$$

$$W_{mn_b}^{sd} + Wp_{mn_b}^{sd} \leq 1 \qquad \forall s,d,m \in N, \forall n \in N_m, \qquad (3\text{-}12)$$

Constraints (3-8)-(3-11) are used to get the binary variable for the working and protection wavelengths channels that traverses a physical link. Constraint (3-12) ensures that the working and protection paths for each request (s,d) are link disjoint and overall also path disjoint.

3.4.2 Floods MILP Model

In this section, the MILP model for post-disaster traffic floods is presented. As discussed in the previous section, the network capacity (F_{mn}) and routing tables ($W_{mn_b}^{sd}$ and $Wp_{mn_b}^{sd}$) for this model are defined as parameters that are imported from the dimensioning model. In addition to the parameters and variable defined in the dimensioning model above, the following parameters and variables are defined in Table 3-2.

Table 3-2 Parameters and variables definition for the floods MILP

F_{mn}	Number of fibers in link (m,n)
F^{sd}	Multiplier that represents the increase in traffic volume between node s and node d as a result of a flood
$W_{mn_b}^{sd}$	Binary variable indicator, set to 1 when request (s,d) is routed through link (m,n), 0 otherwise
$Wp_{mn_b}^{sd}$	Binary variable indicator, set to 1 when the protection path of request (s,d) is routed through link (m,n), 0 otherwise

Δ^{sd}	The total traffic request between node s and d
$\widetilde{\Delta^{sd}}$	The total protection traffic of request Δ^{sd}
Wt_{mn}	The total number of wavelengths on a physical link (m,n) including working and protection wavelengths
δ^{sd}	Binary variable indicates whether the request λ^{sd} is served ($\delta^{sd}=1$) or not ($\delta^{sd}=0$)
γ^{sd}	Binary variable indicate whether the protection path for request λ^{sd} is provisioned ($\gamma^{sd}=1$) or not ($\gamma^{sd}=0$)

The model is defined as follows:

$\boldsymbol{Objective}$: $Maximise$

$$\sum_{s\in N}\sum_{d\in N:s\neq d}\delta^{sd}+\sum_{s\in N}\sum_{d\in N:s\neq d}\gamma^{sd}-\sum_{m\in N}\sum_{n\in N_m}Wt_{mn} \tag{3-13}$$

The objective maximises the number of requests served (first term) and the number of protection paths provisioned (second term) while minimising the number of hops traversed by the working and protection paths (third term).

Subject to:

$$\sum_{n\in N_m}W_{mn}^{sd}-\sum_{n\in N_m}W_{mn}^{sd}=\begin{cases}\Delta^{sd} & m=s\\ -\Delta^{sd} & m=d\\ 0 & otherwise\end{cases} \tag{3-14}$$
$$\forall s,d,m\in N: s\neq d,$$

$$\sum_{n\in N_m}Wp_{mn}^{sd}-\sum_{n\in N_m}Wp_{mn}^{sd}=\begin{cases}\Delta^{sd} & m=s\\ -\Delta^{sd} & m=d\\ 0 & otherwise\end{cases} \tag{3-15}$$
$$\forall s,d,m\in N: s\neq d,$$

Constraints (3-14) and (3-15) represent the flow conservation constraints, where the overall traffic, including the floods, is served between source and destination. The constraint itself accounts for the possibility that some requests can be blocked depending on the overall network situation. This is represented by the total traffic definition that is given by equations (3-16) and (3-17).

$$\Delta^{sd}=\delta^{sd}\lambda^{sd}F^{sd}/B \tag{3-16}$$
$$\forall\ s,d,\in N$$

$$\widetilde{\Delta^{sd}} = \gamma^{sd}\lambda^{sd}F^{sd}/B \quad (3\text{-}17)$$
$$\forall\, s, d, \in N$$

F^{sd} is a multiplier that scales the traffic between source and destination by a certain amount provided the source node is a disaster/non-disaster node, and (3-17) already takes into account the population of the source and destination nodes since λ^{sd} is a function the populations of the two cities.

The request λ^{sd}can be a non-integer and hence given (3-16) and (3-17) with non-integer values of $\Delta^{sd}$and (3-14) and (3-15) results in wavelength grooming being performed in equation (3-18).

$$\sum_{s\in N}\sum_{d\in N:s\neq d} W_{mn}^{sd} + \sum_{s\in N}\sum_{d\in N:s\neq d} Wp_{mn}^{sd} = Wt_{mn} \quad (3\text{-}18)$$
$$\forall m \in N, n \in N_m,$$

$$M\, W_{mn}^{sd} \geq W_{mn_b}^{sd} \qquad \forall s, d, m \in N, \forall n \in N_m, \quad (3\text{-}19)$$

$$W_{mn}^{sd} \leq U W_{mn_b}^{sd} \qquad \forall s, d, m \in N, \forall n \in N_m, \quad (3\text{-}20)$$

$$M\, Wp_{mn}^{sd} \geq Wp_{mn_b}^{sd} \qquad \forall s, d, m \in N, \forall n \in N_m, \quad (3\text{-}21)$$

$$Wp_{mn}^{sd} \leq U Wp_{mn_b}^{sd} \qquad \forall s, d, m \in N, \forall n \in N_m, \quad (3\text{-}22)$$

Constraints (3-19)-(3-22) represent the routing based on the precomputed paths. Setting $W_{mn_b}^{sd}$ and $Wp_{mn_b}^{sd}$as parameters forces the requests to follow the precomputed routes. These constraints are similar to the path-disjoint constraints in the dimensioning model but here the disjoint nature is already given within the precomputed paths.

Capacity constraint (3-7) is used the same way, except the fact that the capacity which is represented by F_{mn} is a parameter in this model and not a variable.

$$\delta^{sd} = \gamma^{sd} \quad (3\text{-}23)$$
$$\forall s, d \in N$$

Constraint (3-23) ensures that if a request is accepted, then its protection path is also accepted.

The floods MILP model is used to evaluate the network performance under FFR approach assumptions without making changes.

To represent the FSTF approach, the blocking variable is redefined as a non-binary variable, as the traffic can be blocked partially. Also, a constraint is added to limit the acceptance variable value such that it does not exceed 1 as in (3-24).

Variables

δ^{sd} A variable indicating the served percentage of a request λ^{sd}

γ^{sd} A variable indicating the percentage of the provisioned protection for request λ^{sd}

$$\delta^{sd} \leq 1$$

$$\forall s, d \in N \quad (3\text{-}24)$$

To allow protection paths rerouting in the FPPR, Wp_{mn}^{sd} is redefined as a variable. So the working path still follows the precomputed path and a protection path that allows accommodating more floods is rerouted.

Variables

$Wp_{mn_b}^{sd}$ Binary equivalent of Wp_{mn}^{sd}, equals 1 if Wp_{mn}^{sd} has a value greater than zero.

To allow the rerouting of working and protection paths in the FWPPR, both $W_{mn_b}^{sd}$ and $Wp_{mn_b}^{sd}$ are changed from parameters into variables.

Variables

$W_{mn_b}^{sd}$ Binary equivalent of Wp_{mn}^{sd}, equals 1 if Wp_{mn}^{sd} has a value greater than zero.

$Wp_{mn_b}^{sd}$ Binary equivalent of Wp_{mn}^{sd}, equals 1 if Wp_{mn}^{sd} has a value greater than zero.

Finally, the FRDS approach is an improved version of FWPPR approach, as it will drop the protection provisioned resources for low-class traffic types. The MILP model for this approach is the same model for FWPPR, apart from changing the protection resources by a fraction. This change is applied to equation (3-17) by adding a new parameter θ^{sd} to the equation, and this parameter represents the fraction of protection resources that is provisioned. Equation (3-17) is redefined as:

$$\widetilde{\Delta^{sd}} = \gamma^{sd}\lambda^{sd}F^{sd}f^{s}\theta^{sd}/B \qquad \forall\, s, d, \in N \tag{3-25}$$

3.5 Post-Disaster Traffic Floods Heuristic

In order to validate the MILP models, five real-time heuristic approaches are developed with the objective of maximally serving post-disaster traffic floods.

The FFR approach uses the predetermined paths to exploit the whole capacity to accommodate the floods. The pseudo-code of this heuristic is shown in Figure 3-3. The algorithm consists of two parts: the first routes the non-flooding requests while the second part routes the flooding traffic. Initially, a pair of disjoint paths between all nodes is given as an input to the heuristic and these paths can be generated using Bhandari algorithm [80]. The flooding and non-flooding requests should follow these precomputed paths. Also, the algorithm maintains the mutual necessity between the working and protection path; they are either accepted together or blocked together.

Algorithm: FFR

Input: Set of nodes in the network (N),

Set of physical links in the network (L),

Set of flooding requests(F),

Set of non-flooding requests (Z)

Predetermined paths for each request given as P1(r), P2(r)

Output: network blocking probability

Sort Z,F in ascending order
/* Routing non-flooding requests (Z)*/
For $\forall r \in Z$
    Route r (working) on P1(r)
    Route r (protection) on P2(r)
End for
/* Routing flooding requests (F) */
For $\forall r \in F$
    Find residual capacity of P1(r), P2(r) given as R1(r), R2(r)
    If Datarate(r) ≤R1(r) & Datarate (r) ≤ R2(r)
        Route r (working) on P1(r)
        Route r (protection) on P2(r)
    Else Block r
End for
Calculate the total blocking probability

Figure 3-3 FFR heuristic

FSTF approach is similar to FFR approach, except that it should filter out less critical traffic using traffic filters. Figure 3-4 shows the FSTF heuristic approach, the only difference from the FFR heuristic is that the traffic matrix should be multiplied by a reduction factor before the routing steps.

In the FPPR, a new degree of freedom is added to exploiting the residual capacity, which is rerouting and reprovisioning the protection paths, while the working paths are left undisrupted.

Algorithm: FSTF

Input: Set of nodes in the network (N),

Set of physical links in the network (L),

Set of requests (D),

Set of flooding requests (F),

Set of non-flooding requests (Z)

Predetermined paths for each request given as P1(r), P2(r)

Percentage of reduction (M)

Output: network blocking probability

```
For ∀ r ∈ D
    Datarate(r)= Datarate(r)* M
End for
Sort Z,F in ascending order
/* Routing non-flooding requests (Z) */
For ∀ r ∈ Z
        Route r (working)    on P1(r)
        Route r (protection) on P2(r)
End for
/* Routing flooding requests (F) */
For ∀ r ∈ F
      Find residual capacity of P1(r), P2(r) given as R1(r), R2(r)
      If  Datarate(r) ≤R1(r) &  Datarate (r)  ≤ R2(r)
          Route r (working)    on P1(r)
          Route r (protection) on P2(r)
      Else Block r
End for
```

Figure 3-4 FSTF heuristic

The pseudo-code heuristic which is shown in Figure 3-5 consists of three steps, which are routing the non-flooding working traffic, then the flooding working traffic and finally the protection paths for both flooding and non-flooding requests. In the preparation phase: a pair of disjoint paths is given as an input to the heuristic. The heuristic then sorts the requests (floods/non-floods) in ascending order based on their data rates. In order not to disrupt the working traffic, it will use one of the disjoint paths to route the working traffic. The first step is to route the non-flooding requests working paths forming an initial routing solution for their corresponding protection paths. In the second step, the flooding requests working paths are routed and provisioned, while their protection paths are routed (but without provisioning) and an initial solution is formed. The third step is to find the best route that can accommodate the protection paths. This includes both the non-flooding and flooding requests. The heuristic checks whether the initial routing solution has enough residual capacity or not, if it still has capacity then it will use it, otherwise it will attempt to route the traffic using the routing function which is shown in Figure 3-6. To get a protection path that is path-disjoint from the working path, the algorithm removes the working path links from the physical topology then searches for the next best path (in terms of residual capacity). If the function fails to route the protection path, its working traffic is blocked.

This routing heuristic objective is to maximally serve the request. It has three possible scenarios: route the request based on a single path by initiating new wavelengths. If it fails to find enough capacity through single path it will do multipath routing otherwise if it fails to route it using single or multipath routing then the request is blocked. First, it searches for all possible non-loop paths between the source and destination. Then it calculates the residual-hop count product. After that, it checks whether the request can be accommodated in a single path. If it fails to find a single path, then it will route it using the widest path, after that it will update capacities and paths residual capacities. Again, it will use the new widest path to accommodate the remaining fraction of the request. It continues this process till it accommodates the whole request or explores all the available paths. Failing to serve the request will return a blocking indicator.

```
Algorithm: FPPR
Input: Set of nodes in the network (N),
Set of physical links in the network (L),
Set of requests(D),
Set of flooding requests(F),
Set of non-flooding requests (Z)
Predetermined paths for each request given as P1(r), P2(r)

Output: network blocking probability
Find a pair of disjoint paths (P1(r), P2(r)) ∀ r ∈ D
Sort D in ascending order
Sort Z in ascending order
Sort F in ascending order
/* Routing Non-flooding Requests' Working Path */
For ∀ r ∈ Z
        Route r on P1(r)
        Form an initial solution by routing r (protection) on P2(r)
End for
/* Routing flooding Requests' Working Path */
For ∀ r ∈ F
     Find residual capacity of P1(r), P2(r) given as R1(r), R2(r)
        If Datarate(r) ≤R1(r)
          Route r on P1(r)
          Form an initial solution by routing r (protection) on P2(r)
        Else Block r
End for
/* Rerouting flooding and non-flooding Requests' Protection Path */
For ∀ r ∈ D
     Find residual capacity of (P2(r)) R2(r)
      If Datarate (r) ≤ R2(r)
            Route r on P2(r)
      Else Reroute r using Routing Function (Topology, Available Capacity, sr, ds, Datarate(r))
      If r blocked
         Delete r on P1(r)
End for
```

Figure 3-5 FPPR heuristic

Figure 3-7 shows the FWPPR heuristic, it consists of two main parts, the first one routes the non-flooding requests while the second part routes the flooding requests. The reason for routing non-flooding requests first is to prevent the floods from occupying the network resources and leads to blocking other nodes requests. The non-flooding requests are routed using Bhandari algorithm, but the function increases the cost of the links that lead to the flooding node to avoid using such links for the pass through traffic. For the floods, the routing function is used to route both working and protection paths.

```
Routing Function (Topology, Available Capacity, sr, ds, datarate)
Output: Available Capacity, Blocking
Get k-paths
Calculate hop count h(k)
For ∀ i ∈ k
    Find residual capacity of all paths R(k)
    Calculate R(k)*H(k) product (residual-hop count product)
     Sort R(k) in descending order
        If R(1) ≥ rate
        Sort remaining paths with R > rate based on R×H ascendingly
          Route on the minimum (top) path
          Update capacities
              Break;
          If R(1) < rate
            Route request on R(1)
            Update request datarate(rate=rate-R(1))
            Update capacities
End for
```

Figure 3-6 Routing function

As depicted earlier in FRDS description, the scenario is similar to FWPPR except it can remove protection resources for a fraction of the requests that cannot be provisioned fully. The FRDS heuristic is shown in Figure 3-8, step 16 does the reduction in protection resources, in case of failing to provision the whole request.

Algorithm: FWPPR

Input: Set of nodes in the network (N),
Set of physical links in the network (L),
Set of requests(D),
Set of flooding requests(F),
Set of non-flooding requests (Z)
Predetermined paths for each request given as P1(r), P2(r)

Output: Network Blocking Probability

```
Sort Z,F in ascending order
Find a pair of disjoint paths (P1(r), P2(r)) ∀ r ∈ D (Bhandari algorithm)
Step 1: Route the Working and Protection Paths for non-flooding requests
For ∀ r ∈ Z
    Route r (working)    on P1(r)
    Route r (protection) on P2(r)
End for
/* Routing flooding requests' Working and Protection Path */
For ∀ r ∈ F
    Route r (working) using Routing Function (Topology, Available Capacity, sr, ds, datarate(r))
    If r blocked
        Break
    Else Delete Working Path Links from physical topology
        Route r (protection)using Routing Function (Topology, Available Capacity, sr, ds, datarate (r))
            If r blocked
                Delete the working path route
End for
```

Figure 3-7 FWPPR heuristic

```
Algorithm: FRDS
Input: Set of Physical Nodes in Network (N),
Set of Physical Links in Network (L),
Set of Flooding Requests(F),
Set of Non-flooding Requests (Z),
Percentage of Reduction (M)

Output: Network Blocking Probability
Sort Z,F ascendingly
Find a pair of disjoint paths (P1(r), P2(r)) ∀ r ∈ D (Bhandari algorithm)
/* Route the Working and Protection Paths for non-flooding requests */
For ∀ r ∈ Z
        Route r (working)    on P1(r)
        Route r (protection) on P2(r)
End for
/* Routing flooding requests' Working and Protection Path */
For ∀ r ∈ F
        Route r (working) using Routing Function (Topology, Available Capacity, sr, ds, datarate(r))
        If r blocked
            Break
        Else Delete Working Path Links from physical topology
            Route r (protection)using Routing Function (Topology, Available Capacity, sr, ds, datarate (r))
                If r blocked
                    r=r * M
                    Route r (protection)using Routing Function (Topology, Available Capacity, sr, ds, datarate (r))
                If r blocked
                    Delete the working path route
End for
```

Figure 3-8 FRDS heuristic

3.6 Network Performance Evaluation under Post-Disaster Traffic Floods

To evaluate the MILP models, the NSFNET network which is shown in Figure 3-9 is considered. The NSFNET covers the US and consists of 14 nodes and 21 bidirectional links. The network contains five data centres located at nodes (2, 3, 7, 8 and 9). These optimised data centre locations are based on the work in [39]. The traffic matrix is based on the gravity modelling that considers the US population [81]. The network accommodates different traffic types as shown in [82].

The first step is to get the network dimensions based on the busy hour traffic using the dimensioning MILP model to obtain the network capacity. The input parameters for the models and heuristics are shown in Table 3-1. After running the model, Figure 3-10 shows the links capacities.

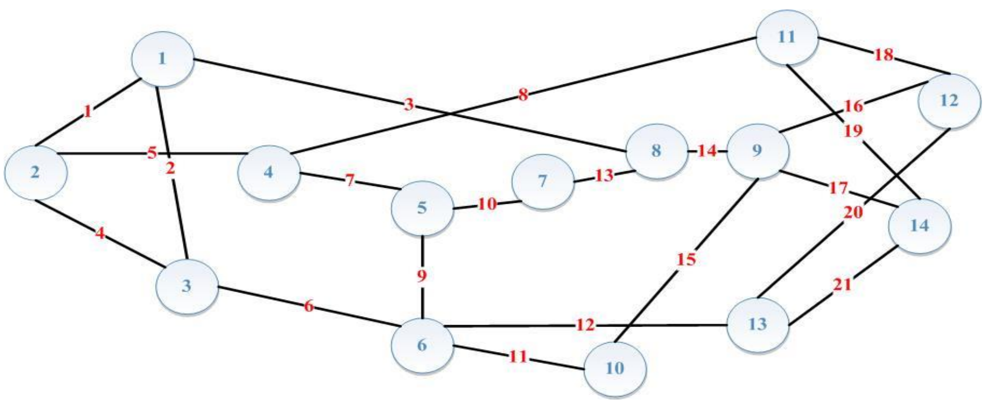


Figure 3-9 NSFNET network topology

Table 3-3 Input Data for the dimensioning MILP Model [83]

Distance between two neighbouring EDFAs (*S*)	80 (km)
Number of wavelengths in a fibre (*W*)	32
Capacity of a wavelength (B)	40 (Gb/s)
Power consumption of a router port (P_r)	825 (W)
Power consumption of a transponder (P_t)	167 (W)
Power consumption of a regenerator (P_g)	334 (W)
Power consumption of an EDFA (P_e)	55 (W)
Power consumption of an optical switch (P_o)	85 (W)

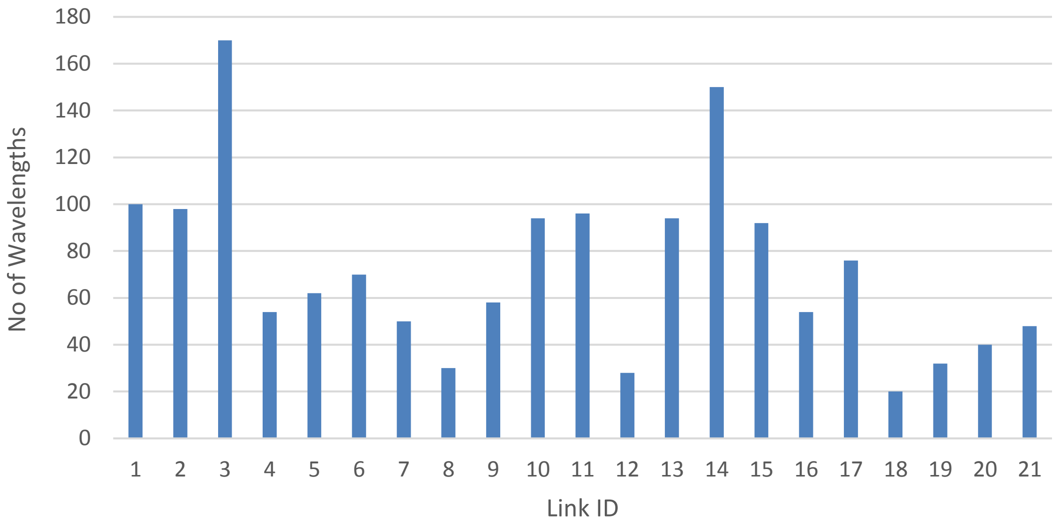
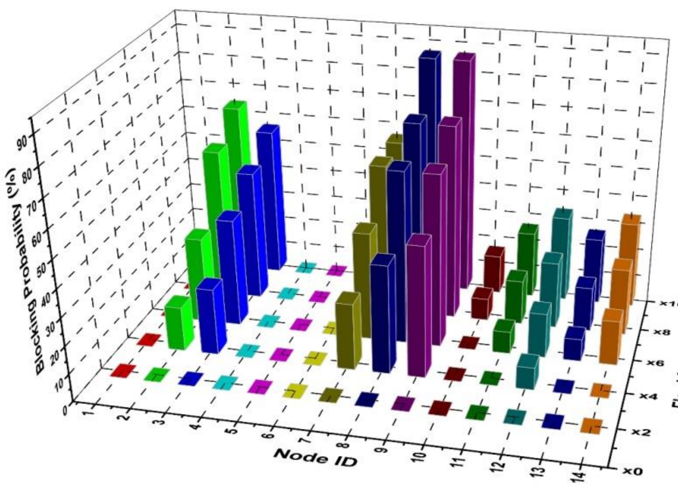


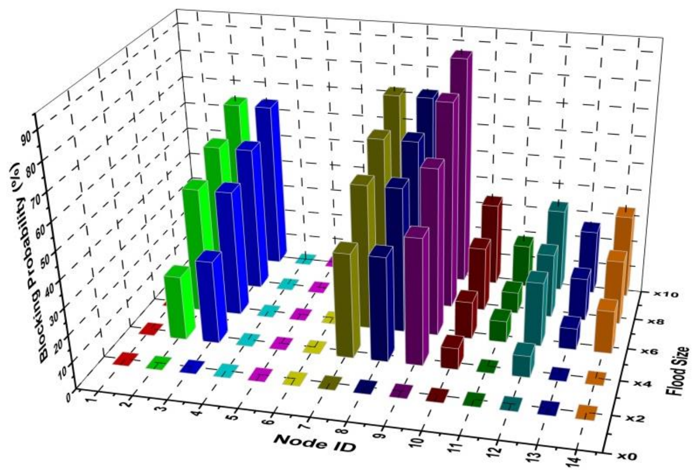
Figure 3-10 Number of wavelengths per link

To investigate the network performance, incremental flood volumes (x2, x4, x6, x8 and x10) were applied on a single node at a time and the percentage of blocked traffic floods for the five proposed scenarios was determined. Note that, x2 means x1 for regular traffic and the other x1 represents the floods.

First, the FFR approach is evaluated by applying floods at each node. Figure 3-11 shows the FFR approach results using both MILP and heuristic approaches. It is can be seen that floods up to double the traffic size can be fully accommodated because of the over-provisioning of network capacity while for larger floods the network starts blocking requests due to capacity exhaustion.



(a)



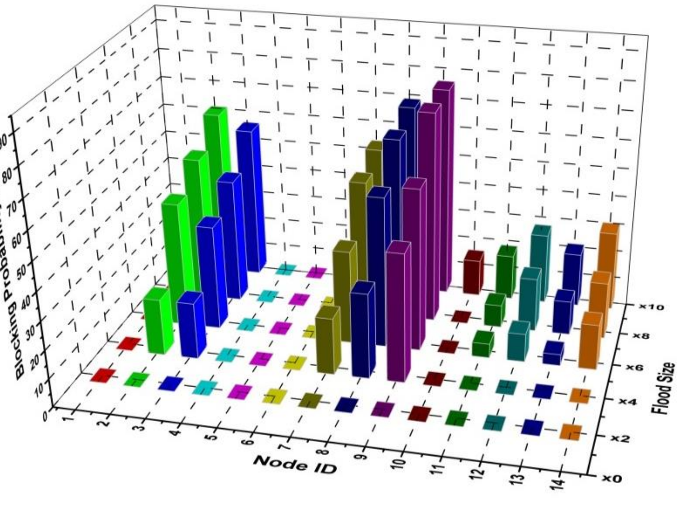
(b)

Figure 3-11 The percentage of blocked floods for FFR scenario a) MILP b) Heuristic

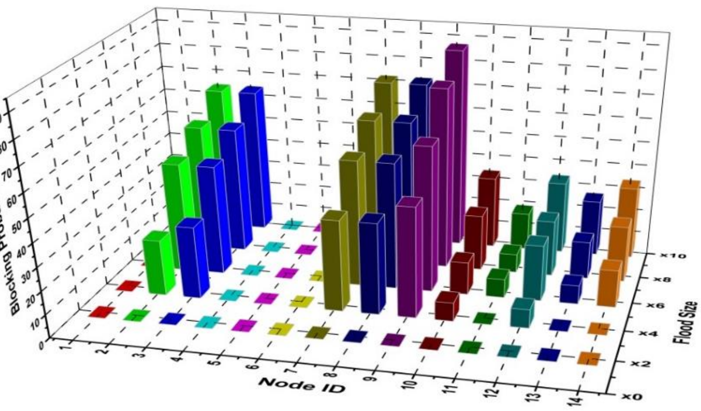
The results show that DC nodes (2, 3, 7, 8 and 9) have the highest blocking probability because their own traffic uses more than 50% of the node resources, so when the floods multiplier exceeds 2, blocking starts. For non-DC nodes, the results show that these nodes can be classified into two groups. The first group, nodes (1, 4, 5 and 6) have the lowest blocking probability. In contrast, nodes (10, 11, 12, 13 and 14) have higher blocking. The non-DC nodes traffic uses less than 30% of the node resources, while the transit traffic is the dominant. The amount of the transit traffic mainly depends on the node location and its nodal degree. Regarding the location, nodes next to DC nodes or in the middle of the topology or nodes that have longer links that interconnect the two ends of the topology have higher transit traffic. Also, nodes with higher nodal degree mean higher connectivity and consequently this increases the transit traffic such nodes handle. The transit traffic includes both working and protection traffic which are usually groomed together. In this sense, the mitigation approaches attempt to deal with these traffic kinds to reduce the blocking.

In the FSTF scenario, the less critical traffic is blocked which accounts for approximately 40% of the total traffic (note that the online gaming, VoD and peer to peer traffic are classified as non-critical traffic)[82]. Figure 3-12 shows the percentage of floods traffic when using the FSTF approach for the MILP model and heuristic. In terms of blocking it is superior to FFR approach, it reduces the percentage blocking under x10 traffic floods for DC by 15%, and for non-DC nodes by 5%. Dropping this less critical traffic will free more resources to be filled by the floods.

FPPR, FWPPR and FRDS approaches introduced further improvement compared with the two previous approaches as they deal with the floods and the transit traffic at the same time.



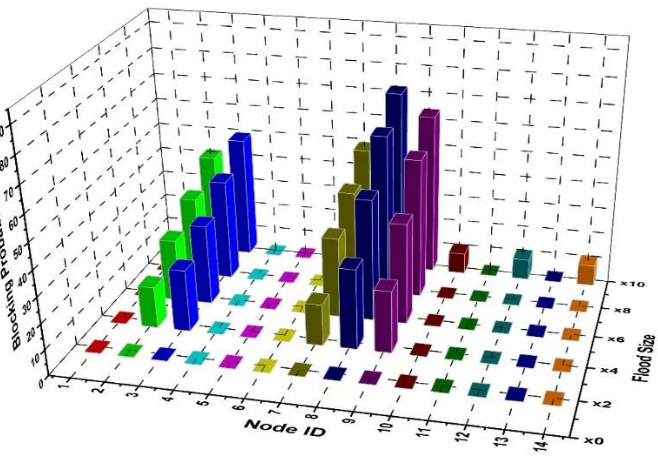
(a)



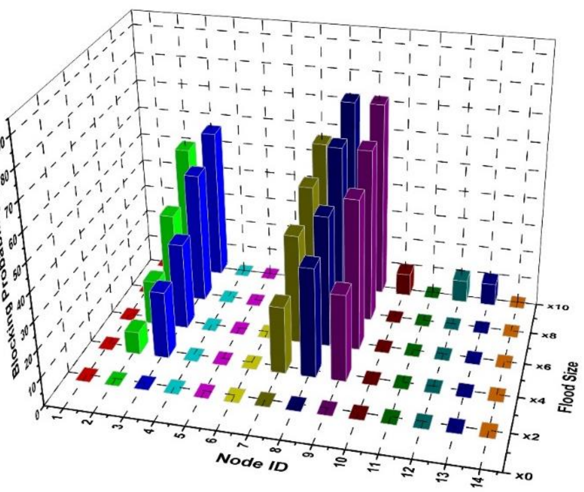
(b)

Figure 3-12 The percentage of blocked floods for FSTF scenario a) MILP b) Heuristic

The results of the FPPR approach is shown in Figure 3-13. The results show that some nodes have better performance compared with FSTF results, while others are worse under this approach. Non-DC nodes blocking percentage is reduced by 24% compared to FFR, because the 30% of the total node resources that is occupied by the transit protection paths is freed. On the other hand, DC nodes slightly improved (percentage blocking reduced by 5% compared to FFR) because the percentage of transit traffic does not contribute to the total node traffic.



(a)

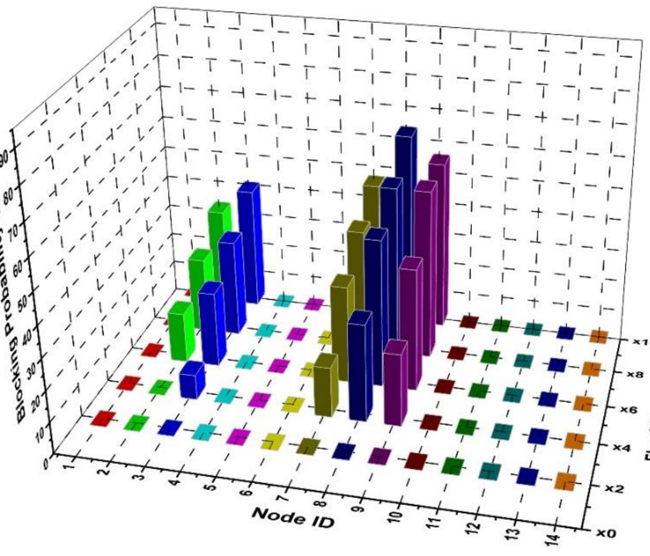


(b)

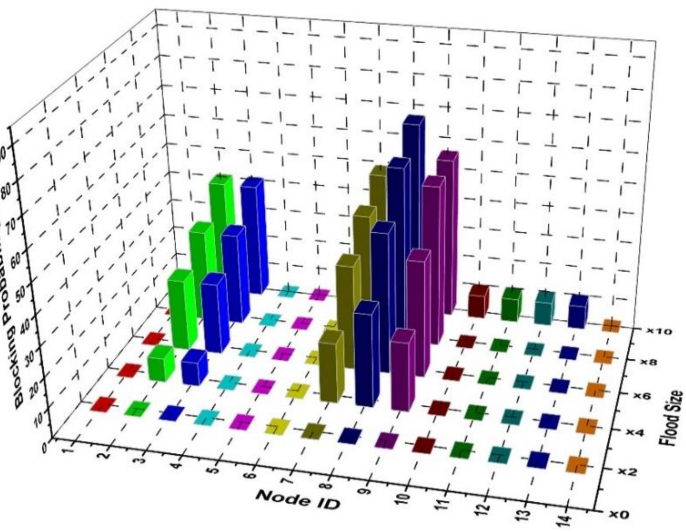
Figure 3-13 The percentage of blocked floods for FPPR scenario a) MILP b) Heuristic

The MILP model is superior to the heuristic approach, because of the sequential operation of the heuristic. For example, under the heuristic, a request of 2 Gbps that can be rerouted over two paths with 4 Gbps and 30 Gbps spare capacity is rerouted over the 4 Gbps path. Then if the next request is 4 Gbps, it is rerouted over the 30 Gbps route, as the 4 Gbps route is half full and wasted.

The FWPPR approach has another degree of freedom because it reroutes the working and protection traffic in the whole network. This advantage means better resource utilisation and less blocking. Figure 3-14 shows the results of the FWPPR approach. The non-datacenter nodes have zero blocking using this approach. On the other hand, datacenter nodes blocking is reduced by 15%-30% compared to FFR.



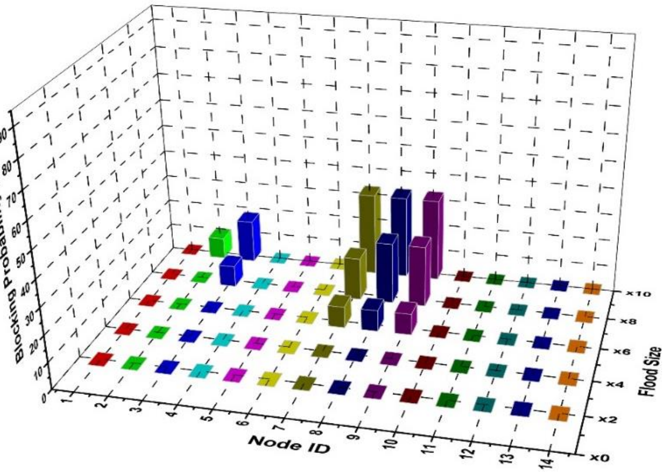
(a)



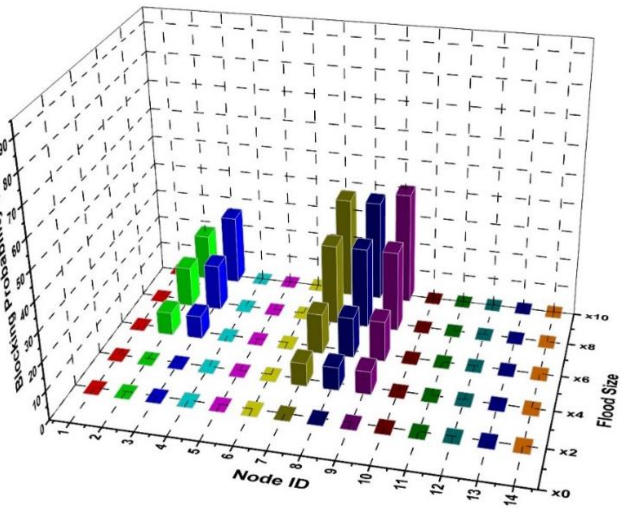
(b)

Figure 3-14 The percentage of blocked floods for FWPPR scenario a) MILP b) Heuristic

In evaluating the FRDS approach, 40% of the floods traffic are assumed to be served as best-effort traffic and are left to the IP layer restoration service while 60% of the traffic is protected. Figure 3-15 shows the MILP and heuristic results for the FRDS approach. Clearly, this approach significantly outperforms the other approaches. DC nodes blocking percentage his lower by 20%-50% compared to the FFR approach.



(a)



(b)

Figure 3-15 The percentage of blocked floods for FRDS scenario a) MILP b) Heuristic

Although, the results showed an improvement in the network performance in terms of blocking but still each approach has pros and cons and the improvement came at a cost or sacrifice. And as stated earlier, deploying these approaches mainly depends on the used network technologies. Table 3-1 summarises the approaches cons and pros.

3.7 Summary

In this chapter, the temporal network capacity exhaustion (due to the increased traffic requests that originate as a disaster consequence) is studied and referred to as Post-Disaster Traffic Floods capacity exhaustion. Five mitigation approaches have been suggested to minimise the blocking. MILP models for the IP over WDM core network were developed to evaluate the network performance under the mitigation approaches and five heuristics have been developed to mimic the MILP models for real time network control and operation. The MILP models and heuristics were evaluated using single node flooding at a time under different flooding volumes for all of the nodes. The results showed a variant performance trends, as these trends depends on the approach scheme. The FFR approach is the worst in performance as it failed to absorb high volume traffic floods, on the other hand it required less cost and efforts to deploy. The FTRS approach is an improved version of FFR but at the cost of dropping traffic. The FPPR approach has a comparable results to FTRS but without traffic dropping. It requires efforts to reprovision the protection paths and add new wavelengths for the working paths. This approach did not require traffic disruption because it dealt with protection paths only. The FWPPR results were better than previous approaches as it managed to reduce blocking significantly, but at the cost of disrupting the whole network traffic till rerouting all paths and reconfigure new lightpaths. The best mitigating approach was the FRDS, which is based on rerouting the whole network traffic and cancelling the protection resources for the less critical traffic. This approach resulted in blocking probability reduction between 20% and 50% in the DC nodes, and eliminated the blocking in other nodes. This improvement comes at the cost of disrupting the traffic until the traffic is rerouted and additionally at the cost of sacrificing the protection paths for some of the traffic requests. Table 3-4 summarises the approaches cons and pros.

Table 3-4 Floods Mitigation Approaches Comparison

Approach	**Traffic disruption**	**Blocking**	**Cost/complexity**	**New technology/features**
FFR	no	Very high	low	Not needed
FSTF	no	high	low	Traffic filters
FPPR	no	high	high	Not needed
FWPPR	yes	low	Very high	Dynamic routing technology
FRDS	yes	Very low	Very high	Dynamic routing technology

4 Energy-Efficient Advance Reservation Scheduling and Rescheduling in IP over Optical Networks

4.1 Introduction

This chapter methods that can introduced to improve the energy efficiency of network resource allocation for advanced reservation requests where large bandwidth connections are required for a certain period of time only. Four approaches to provision resources for advanced reservation requests in optical core networks are proposed. A MILP model is developed to optimize the network resource allocation of IP over optical core networks considering four provisioning scenarios. A heuristic is also developed to optimise network resource allocation in real time. The model is used to compare the four approaches over a small example network (due to the model complexity) and the heuristic is used to validate the model. The heuristic is then used to evaluate the power savings of the provisioning approaches over larger networks, namely the NSFNET [84] and COST239 [85] networks.

4.2 Advance Reservation

Recently, these types of applications became popular and significantly contribute to the total traffic. The VoD services represents 50% of the video traffic in the core network according to Cisco [86]. Also, the growing reliance on cloud services impose new requirements on cloud providers, and one of these requirements is reliability [87]. Reliability is realised by backing the data on different DCs, and this back up should be done several times a day to ensure the different data copies are synchronised.

Traffic requests in e-Science applications, grid networks, cloud-computing and DCs synchronisation often require large bandwidth only for a certain period of time [88]. In addition, some services are highly popular during a short period such as VoD that is popular during the evening for example [89].

These types of requests can be provisioned through advance reservation to guarantee QoS for users and allow operators to better plan their resource usage. Advance reservation has different requirements in terms of the start time, end time, data rate and duration [90], and therefore allows flexible network resource allocation that eventually improves network performance [91–95].

Chen and Jaekel addressed the problem of energy-aware grooming for scheduled traffic requests [96]. They reported savings of 7%-40% by changing the requests overlapping factors to maximise grooming of sub-wavelength requests and maximise the switching off of unused lightpaths. In [97], the authors achieved a power saving of 10% in the sliding-window AR requests scenario as compared with the fixed AR requests scenario in a 6-node network with 4 sub-wavelength requests. Their power saving was achieved by grooming these requests by sliding the start time of the request. In [98], the authors investigated the power savings by traffic grooming in both static and dynamic traffic requests and evaluated the power saving with three types of traffic overlapping scenarios. They achieved a power saving of 10% by increasing the requests overlapping factor.

In [99], the authors suggested a two-step dynamic rerouting approach for the advance reservation connection request before their start time. This rerouting approach considers load balancing between the newly arriving AR requests during the rerouting process. To the best of our knowledge no previous work exploited the flexibility of rescheduling and rerouting sliding-window advance reservation requests which are yet to start.

4.3 Reservation Scenarios

The scheduled traffic requests arriving at the network are classified as: Immediate Reservation (IR) requests and Advance Reservation (AR) requests [100]. An IR request must be established as soon as it arrives whereas an AR request needs to be allocated in the near future. Furthermore, AR requests can be classified into Fixed-window AR (FAR) and Sliding-window AR (SAR). The FAR requests specify a start time while the SAR requests allow more flexibility by specifying a window where the request can be scheduled to start at any time within that window.

The provided flexibility by the AR requests can be beneficial for optical networks to reduce the power consumption by choosing the optimal provisioning solution. To study the impact of reservation and sliding requests on network power consumption, different scenarios were considered to exploit this flexibility to show the impact of scheduling requests on power consumption.

4.2.1 Immediate and Fixed Advance Reservation (IFAR)

This is the baseline scenario where only FAR and IR requests with a fixed start time are considered. In this scenario, no sliding requests are considered, which limits the flexibility that can be achieved.

4.2.2 Immediate, Fixed and Sliding-window Advance Reservation (IFSAR)

In the second scenario, all the three traffic reservation types are considered and the sliding-window advanced reservation (SAR) is included alongside the IR and FAR of the baseline IFAR reservation scenario.

4.2.3 Re-Scheduling and Rerouting AR Reserved Requests (RSRR)

Scheduling is a decision that is taken at the arrival of the request and this decision is based on the network state at that time, but during the day more requests arrive and the network state keeps changing. RSRR is a scenario where the scheduler has the ability to reschedule and reroute the previously scheduled AR requests before their scheduled starting time.

Basically, the scheduler can provision resources for the newly arrived requests with respect to the previously scheduled requests. While in this approach, the scheduler can optimally allocate resources for both the previously scheduled requests and the newly arriving requests, as the scheduler consider all of them as a newly arriving request. Obviously, SAR requests can be rescheduled and rerouted while FAR requests can be rerouted only.

As an example, assume that a network operator has scheduled a lightpath for a DC backup process between Atlanta and Houston (nodes 6 and 10 in NSFNET) at 16:00, for a duration of two hours at a data rate of 20Gbps, but this backup process has a starting time flexibility and can be delayed to start at any time up to 18:00. At 14:00, the operator receives a video conference request between Atlanta and Houston but the conference is required to start at 18:00 for a duration of two hours and a data rate of 20 Gbps. The network is equipped with 40 Gbps transponders only.

In the normal scenario, the scheduler provisions a half utilized wavelength from Atlanta to Houston for four hours from 16:00 to 18:00 for the DC backup and then from 18:00 to 20:00 for the video conference. However, if the operator has the ability to reschedule requests, then after receiving the video conference request the scheduler checks whether there is any request that is already provisioned at 18:00 to groom the new request with, in order to utilize the wavelength fully. If it fails to find any request at that time, then it will look for scheduled requests that have not started yet and can be shifted for an hour or two. So in our example, the operator will reschedule the DC backup process to start at 18:00 instead of 16:00, and groom the two requests in a single 40 Gbps wavelength from 18:00 to 20:00. Therefore, the operator has reduced the power consumed by an operating, partially filled, wavelength for two hours.

In the previous example, rescheduling was shown to be able to save power, and in the same manner, rerouting can achieve the same savings. For example, if a delay tolerant request has been scheduled and provisioned using the shortest path and before the scheduled starting time, another request arrived to the network that passes through the destination node of the provisioned request but using a longer path. In this case, instead of using two paths for the two requests, they can be groomed by rerouting the first request and grooming it with the new request. This way, the power consumption is reduced by switching off the resources on the first route.

4.2.4 Rerouting and Rescheduling Active and Reserved Request (RARR)

In the previous scenario, the network operation is not disrupted as only the AR requests that have not started are rescheduled. In this scenario, a dynamic routing approach is used, where the active requests in the network are disrupted and rerouted, and the AR requests that have not yet started are rescheduled. In this scenario, no previous knowledge is important as long as the requests are delay-tolerant. Added to rerouting, rescheduling is done for the AR requests that have not started yet. A comparison between RSRR and RARR scenarios is shown in Table 4-1.

Table 4-1 a comparison between RSRR and RARR scenarios

Request type	**RSRR**	**RARR**
IR	No capability	If started, it can be rerouted
FAR	If not started, it can be rerouted. If started *can't* do any rerouting or rescheduling	If not started can be rerouted. If started can be rerouted
SAR	If not started can be rerouted and rescheduled. If started *can't* do any rerouting or rescheduling	If not started can be rerouted and rescheduled. If started can be rerouted

4.4 MILP Model for Energy Efficient Traffic Scheduling in IP over Optical Networks

A MILP model is developed for energy efficient advance reservation resource allocation. The model is built based on the non-bypass approach with multi-hop grooming. In multi-hop grooming, the wavelength occupancy is higher [101], because at each intermediate node more sub-wavelength traffic streams can be groomed.

The scheduled traffic request is defined as a tuple $r\ (sr_r, ds_r, dr_r, du_r, at_r, st_r, et_r)$, where sr_r is the source node, ds_r is the destination node, dr_r is the required data rate, du_r is the duration, at_r is the arrival time and, st_r is the start time for the sliding window and et_r is the end time of the sliding-window of the request.

The model optimises the allocation of network resources to meet the requirements of the scheduled requests at each scheduling time slot so that the total network power consumption is minimised while maintaining QoS (in terms of request start time, duration and other requirements). The model sets, parameters and variables are defined in Table 4-2:

Table 4-2 Sets, variables and parameters for the scheduling MILP

Notation	Description
N	Set of nodes in the network
L	Set of links
P	Set of paths
T	Set of time points
D	Set of traffic requests
I	Set of IR traffic requests, $I \in D$
F	Set of FAR traffic requests, $F \in D$
S	Set of SAR traffic requests, $S \in D$

P_r	The power consumption of a router port
P_t	The power consumption of a transponder
P_a	The power consumption of an EDFA amplifier
P_o	The power consumption of an optical switch
P_g	The power consumption of regenerator
sr_r	The source node of request r
ds_r	The destination node of request r
dr_r	The data rate of request r in Gbps
du_r	The duration of request r (number of time slots)
st_r	The start time of request r
et_r	The end time of request r
at_r	The arrival time of request r
F_l	The number of fibers in the physical link (l)
B	The capacity of each wavelength in Gbps
W	Number of wavelengths in a fiber
H	Distance between neighboring EDFAs
L_l	The length of the physical link (l) in km
A_l	The number of EDFAs on link (*l*). Typically $A_l = \lfloor L_l/H - 1 \rfloor + 2$
RG_l	The number of regenerators in link (*l*).
ex_l^t	The number of occupied wavelengths from previous requests on physical link (l) at time t
x_{pt}^r	The amount of traffic of request r traversing path p at time t
W_l^t	The number of wavelength channels that traverse link l at time t
k_l^t	Ceiling variable
β_t^r	Binary variable: $\beta_t^r = 1$ if request r runs at time slot t otherwise $\beta_t^r = 0$. A request can run at multiple time slots depending on its duration
δ_t^r	$\delta_t^r = 1$ when request r starts running at time t, 0 otherwise

The power consumption at time t is composed of:

1- Power consumption of router ports at time t:

$$\sum_{l \in L} P_r \ W_l^t$$

2- Power consumption of transponders at time t:

$$\sum_{l \in L} P_t \, W_l^t$$

3- Power consumption of EDFAs at each time t:

$$\sum_{l \in L} P_a \, A_l \, F_l$$

4- Power consumption of Regenerators at each time t:

$$\sum_{l \in L} P_g \, RG_l \, W_l^t$$

5- Power consumption of optical switches at each time t:

$$\sum_{m \in N} P_o$$

The model is defined as follows:

Objective: *Minimise*:

$$\sum_{t \in T} \left(\sum_{l \in L} P_r \, W_l^t + \sum_{l \in L} P_t \, W_l^t + \sum_{l \in L} P_a \, A_l \, F_l + \sum_{m \in N} P_o + \sum_{l \in L} P_g \, RG_l \, W_l^t \right) \quad (4\text{-}1)$$

The objective function aims to minimise the total network power consumption by minimising the total activated resources.

Subject to:

$$dr_r \, \beta_t^r = \sum_{p \in P} x_{pt}^r \quad (4\text{-}2)$$

$$\forall t \in T, \forall r \in D$$

Constraint (4-2) is the demand constraint where for each request the sum of the traffic on the paths between the source and destination should be equal to the request data rate.

$$W_l^t = \left\lceil \sum_{r \in D} \sum_{p \in P} \frac{x_{pt}^r}{B} + ex_l^t \right\rceil \quad (4\text{-}3)$$

$$\forall t \in \mathrm{T}, \forall l \in L$$

Constraint (4-3) represents the grooming constraint where the total number of wavelengths on link l at time point t equals the summation of the newly arrived requests wavelengths and the previously scheduled requests wavelengths. The ceiling function is non-linear so constraint (4-3) is replaced with two constraints to make the problem feasible.

$$W_l^t = \sum_{r \in D} \sum_{p \in P} \frac{x_{pt}^r}{B} + ex_l^t + k_l^t \quad (4\text{-}4)$$

$$\forall t \in \mathrm{T}, \forall l \in L$$

$$k_l^t < 1 \quad (4\text{-}5)$$

$$\forall t \in \mathrm{T}, \forall l \in L$$

Constraint (4-4**)** replaces the ceiling function by adding a small fraction to the total traffic to make W_l^t an integer value. This ceiling fraction value is bounded by constraint (4-5) to limit its value to less than one.

$$W_l^t \leq W\, F_l \quad (4\text{-}6)$$

$$\forall t \in \mathrm{T}, \forall l \in L$$

Constraint (4-6) ensures that the total number of wavelengths in a physical link does not exceed the maximum capacity of the physical link.

$$\sum_{t=st_r}^{et_r+du_r-1} \beta_t^r = du_r \quad (4\text{-}7)$$

$$\forall r \in D$$

$$\beta_t^r = 0$$

$$\forall r \in D, \forall t \in T : t < st_r \lor t \geq et_r + du_r \quad (4\text{-}8)$$

Constraints (4-7)-(4-8) ensure that the request service time equals the duration of the request within the service window.

$$\delta_0^r = \beta_0^r \quad (4\text{-}9)$$

$$\forall r \in S$$

$$\delta_t^r \geq \beta_t^r - \beta_{t-1}^r \quad (4\text{-}10)$$

$$\forall r \in S, \forall t \in T$$

$$\sum_{t=0}^{T} \delta_t^r \leq 1 \quad (4\text{-}11)$$

$$\forall r \in S$$

$$\left(\sum_{i=0}^{du_r} \beta_{t+i}^r\right) - du_r \geq -M(1 - \delta_t^r) \quad (4\text{-}12)$$

$$\forall r \in S, \forall t \in T: \quad st_r \leq t \leq et_r + du_r - 1$$

Constraints (4-9)-(4-12) ensure that the SAR request service time is contiguous inside the sliding window, by introducing a binary variable δ_t^r that is set for only the request start time. Constraint (4-9) sets the value of δ_t^r equal to β_t^r at t=0. Constraint (4-10) makes sure that whenever a transition happens in the value of β_t^r from 0 to 1, where this transition represents the request start time, then δ_t^r is set to 1. Constraint (4-11) ensures that δ_t^r for each request r should have a single impulse within the entire set of time points, and this impulse occurs at the time point of the request start of service. Constraint (4-12) ensures that if a request starts at time t (i.e. $\delta_t^r = 1$), then β_t^r values are set to 1 for the duration of the request and the β_t^r values that are equal to 1 are contiguous.

The above model does not support the rescheduling and rerouting scenarios, and to do so a modification is required. This modification includes deleting the previously provisioned paths and rerouting them again. To extend the model, a new set and a parameter are introduced.

R	Set of previously scheduled requests $R \in D$
xr_{pt}^r	The amount of traffic of request r traversing path p at time t that have been scheduled before

$$W_l^t = \sum_{r \in \mathbb{D}} \sum_{p \in P} \frac{x_{pt}^r}{B} + ex_l^t - \sum_{r \in R} \sum_{p \in P} \frac{xr_{pt}^r}{B} + k_l^t \qquad (4\text{-}13)$$

$$\forall t \in \mathrm{T}. \forall l \in L$$

Constraint (4-4**)** is replaced by constraint (4-13). This grooming constraint adds the new routing information for the previously scheduled requests to the new received requests and deletes previous routing information for the previously scheduled requests.

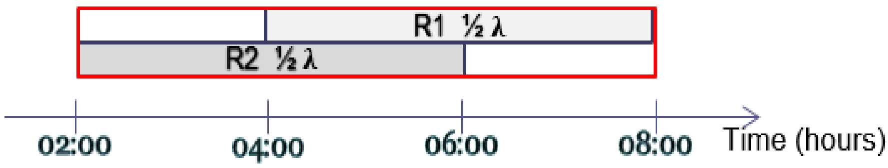
4.5 Energy Efficient Traffic Scheduling (EETS) Heuristics

For real-time implementation of the energy efficient traffic scheduling approach, heuristics are developed to optimise the network resource allocation for the advance reservation requests in real time. Three heuristics are developed to evaluate the different scheduling scenarios.

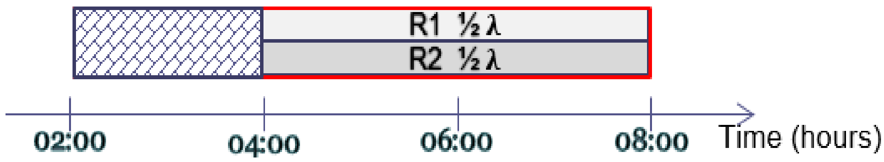
The heuristics aim to do capacity-time domain packing. The capacity is represented by the network state [102]. The heuristics are expected to result in higher power consumption compared to the MILP model as the packing is performed sequentially.

The heuristic starts by routing the IR and FAR requests and then routing and scheduling the SAR request as the SAR request are flexible in terms of their start time. The heuristic contains two elements: firstly, to do the packing it searches for all possible paths that can accommodate the request within the request duration. Secondly, provisioning IR and FAR requests as they do not need scheduling.

Figure 4-1 shows an example that illustrates how packing/scheduling works. Consider two requests passing through same link and each requires half **λ** data rate. Assume that R1 is a FAR request, provisioned from 04:00 to 08:00, while R2 is a SAR request and can start either on 02:00 or at 04:00 and lasts for four hours duration. In Figure 4-1(a), R2 is provisioned at 02:00, while in Figure 4-1(b), R2 is provisioned at 04:00. Obviously, scenario B is better in terms of packing as R1 and R2 are packed on the same **λ** for the same time slots, and eventually **λ** is switched to sleep mode from 02:00 to 04:00.



a)



b)

Figure 4-1 Space-time packing a) No packing b) Packing

Figure 4-2 shows the flowchart of the Energy-Efficient Traffic Scheduling (EETS) heuristic. At the beginning of each time slot, a number of reservation requests arrive in the network. As mentioned above, the IR and FAR are served first. The FAR requests are served based on ascending order of their start time. Both types of requests are routed based on the Energy-Efficient Routing (EER) heuristic shown in Figure 4-3.

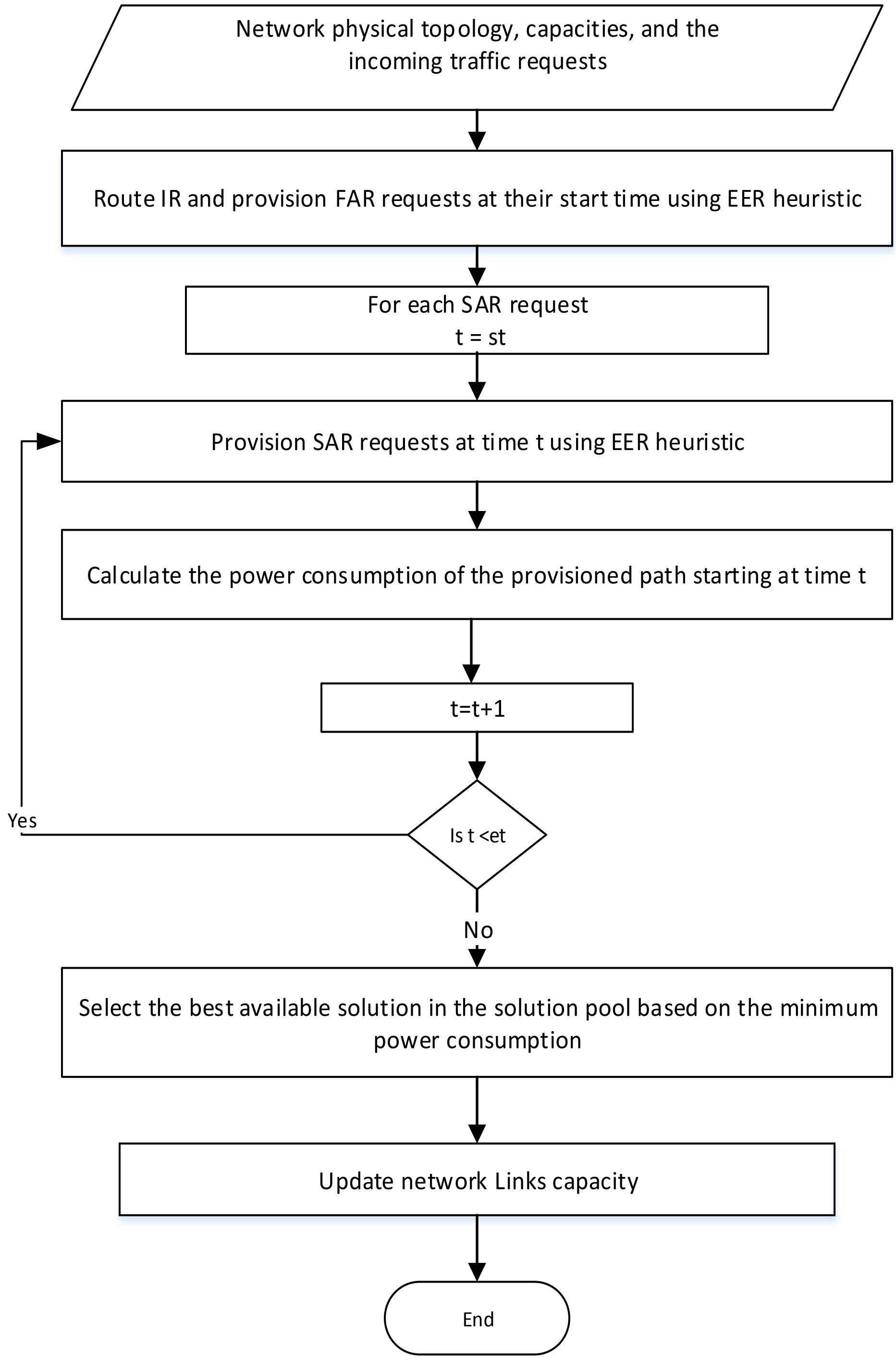


Figure 4-2 EETS flowchart

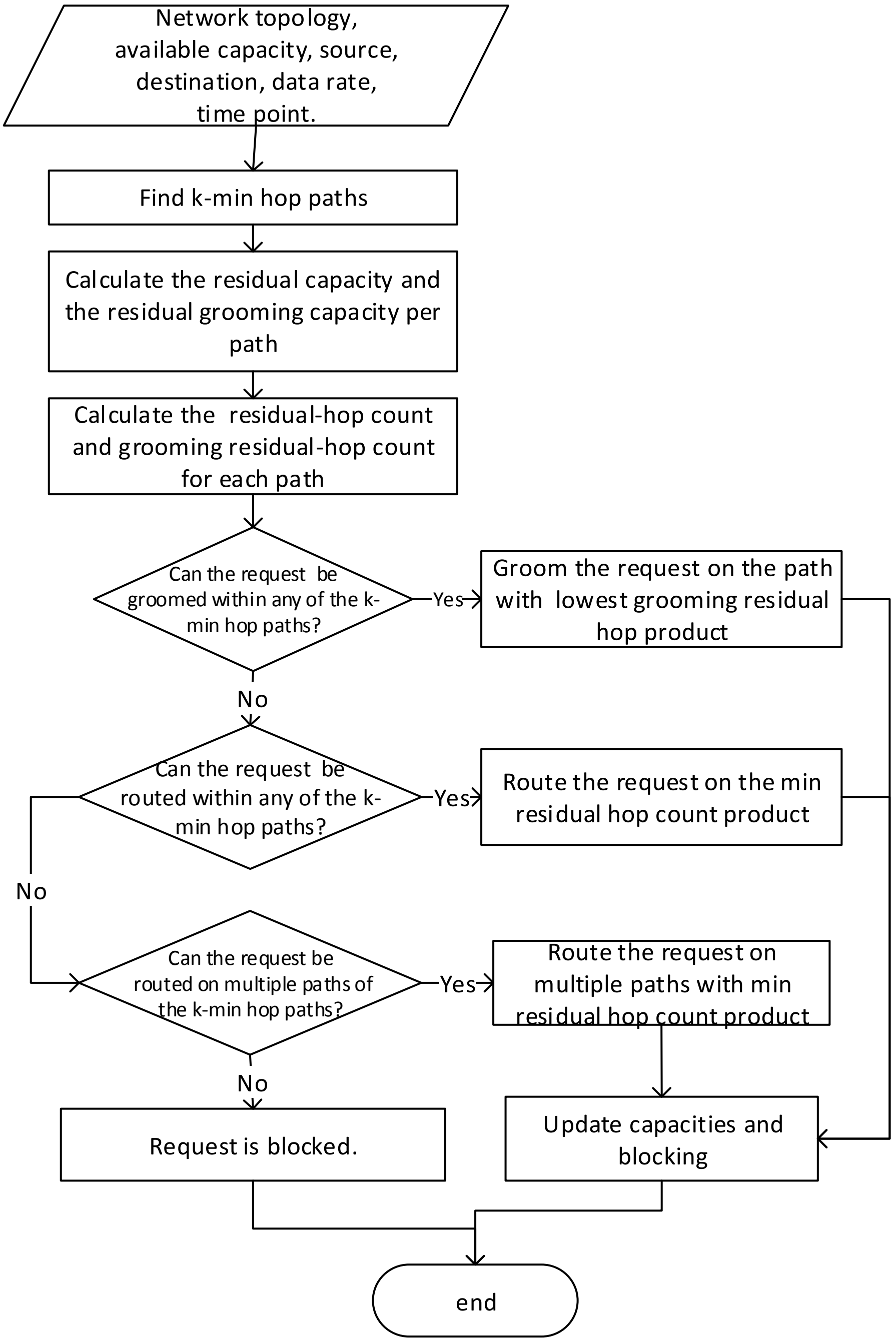


Figure 4-3 EER heuristic

This routing heuristic objective is to find the minimum power consumption path at a specific time point out of the *k-min* hop paths. It has four possible scenarios: the first grooms the request within already established wavelengths, if it fails to groom then it will initiate new wavelengths, if it fails to find enough capacity through single path it will do multipath routing otherwise if it fails to route the request, then the request is blocked. After finding the k-min hop paths, the EER will find the minimum residual capacity and minimum grooming capacity for each one of the k-paths. To find the best path in terms of number of hops, a product of the residuals paths and the number of hops is determined. This product is used in choosing the best path whether for grooming or new wavelengths.

After routing the IR requests and provisioning the FAR requests, the SAR requests are provisioned. For SAR requests there are two dimensions to be optimized which are the start time (scheduling) and the path (routing). The EER routing heuristic selects the best candidate path in terms of power consumption. For optimal start time, the heuristic will use a greedy algorithm by checking the minimum power consumption for each possible start time. If the SAR request occupies more than one time slot, then the EER heuristic might choose different paths for each time point so the total power consumption for the whole request duration is minimum.

Figure 4-4 shows the heuristic for the RSRR approach, which is called Energy-Efficient Traffic Re-Scheduling (EETRS). In this heuristic, the previously scheduled AR requests are deleted, and reprovisioned along with the newly arrived requests. For RARR the corresponding heuristic is shown in Figure 4-5 and called Energy-Efficient Traffic Rescheduling and Rerouting (EETRR). The EETRR is similar to the EETRS heuristic except it can act on the currently active requests not only the not started ones. So it will delete the active traffic paths and reroute them again.

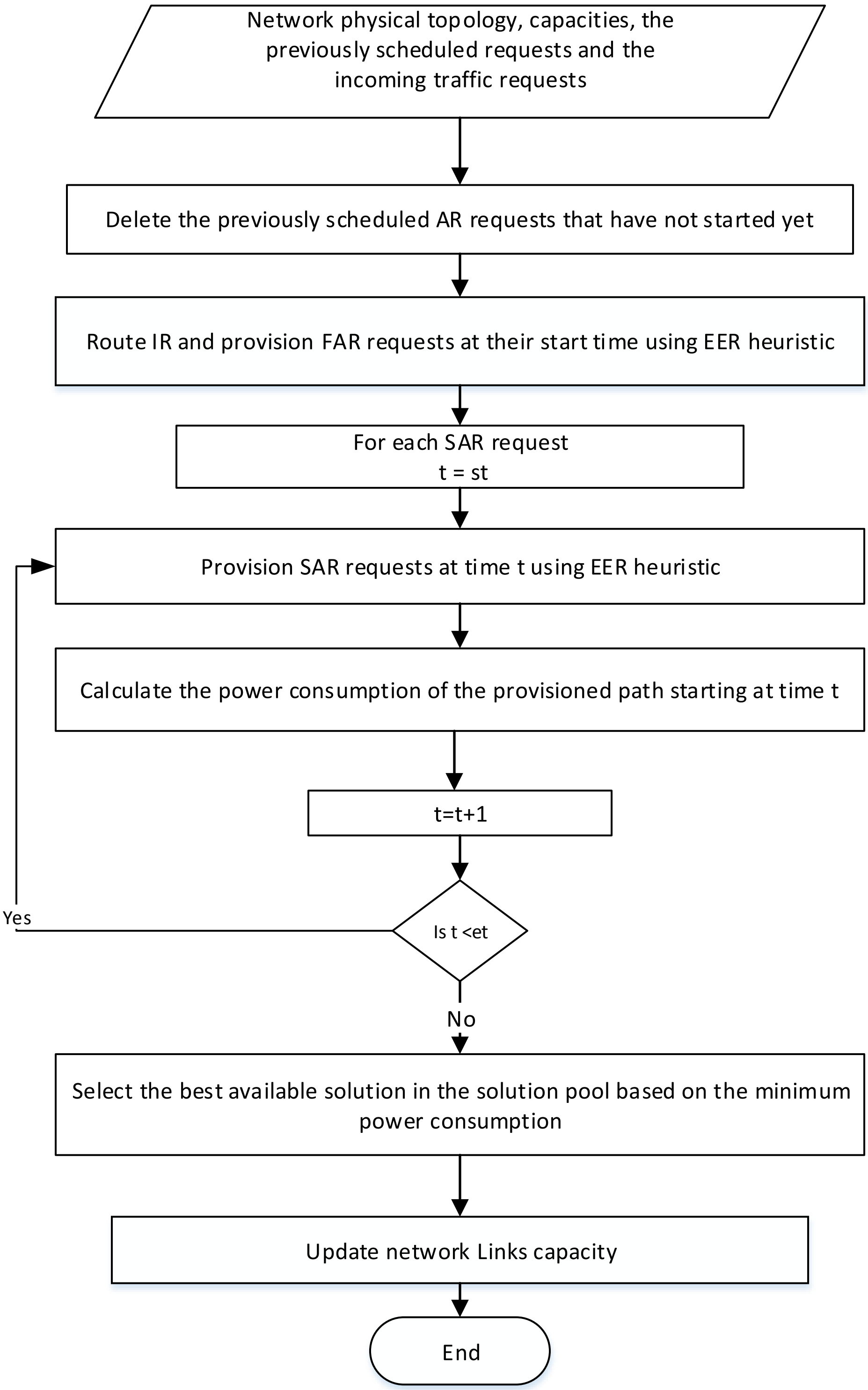


Figure 4-4 EETRS flowchart

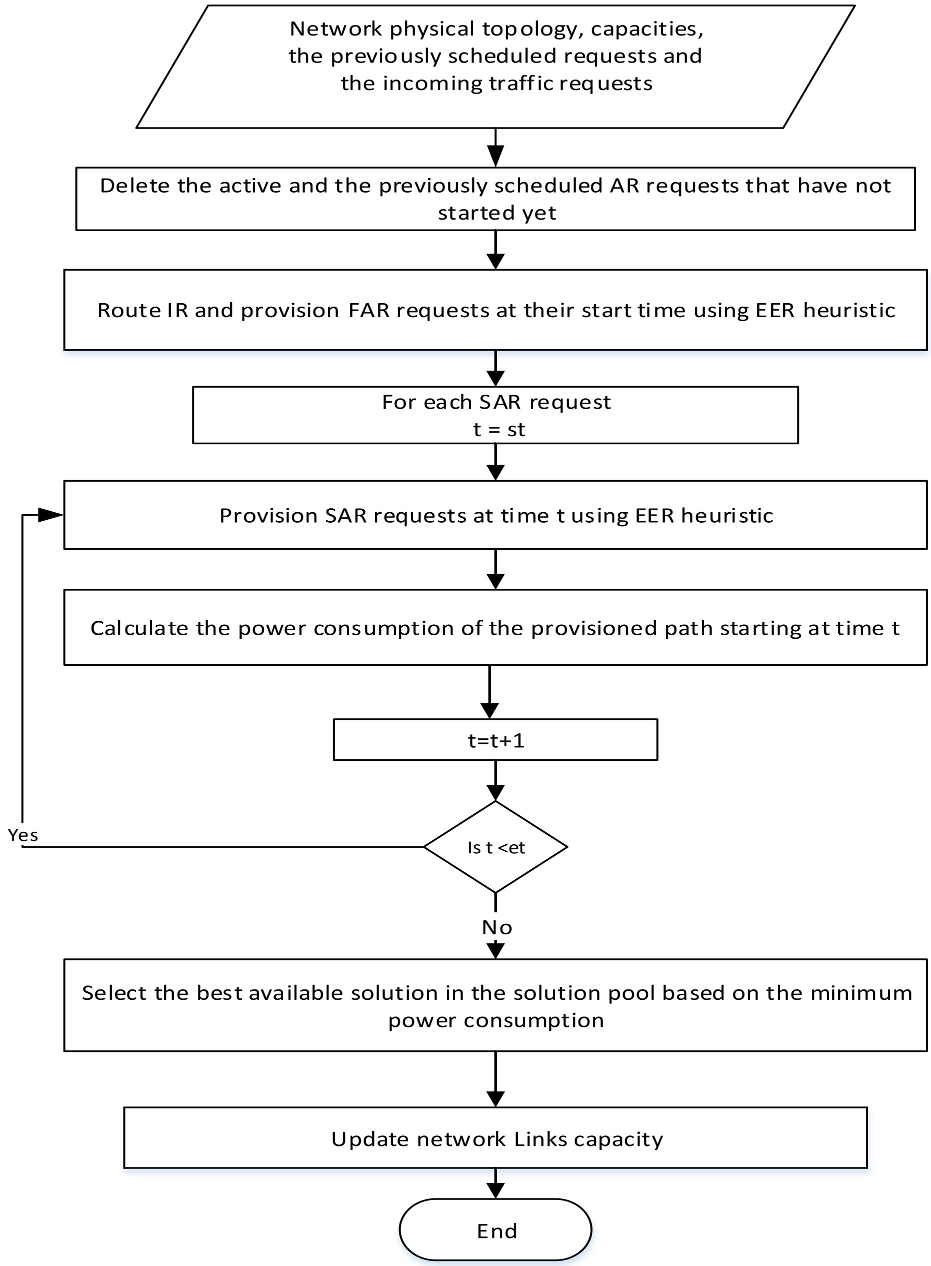


Figure 4-5 EETRR heuristic

4.6 Network Performance Evaluation

The performance of the MILP model and the heuristics was tested on a sample network, depicted in Figure 4-6, is considered. Figure 4-7 shows the average traffic request between each node pair which ranges from 20 Gb/s to 120 Gb/s and the peak occurs at 22:00 [103]. Note that the traffic request of a node pair is uniformly distributed between 10 and 80 Gb/s. The size of the sliding window of SAR requests is uniformly distributed between 2-6 hours and the duration of traffic requests is exponentially distributed with a mean of 4 hours. The number of AR requests arriving to the network throughout the day follows a Poisson distribution [104] as shown in Figure 4-8.

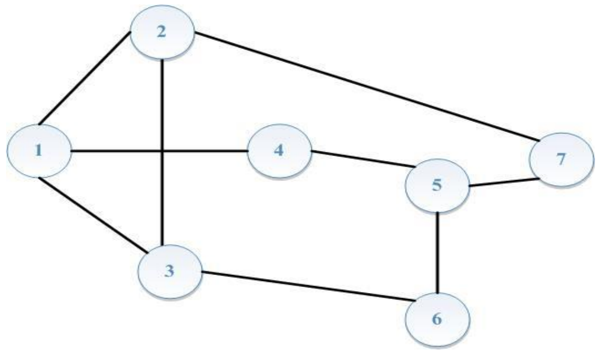


Figure 4-6 Sample network

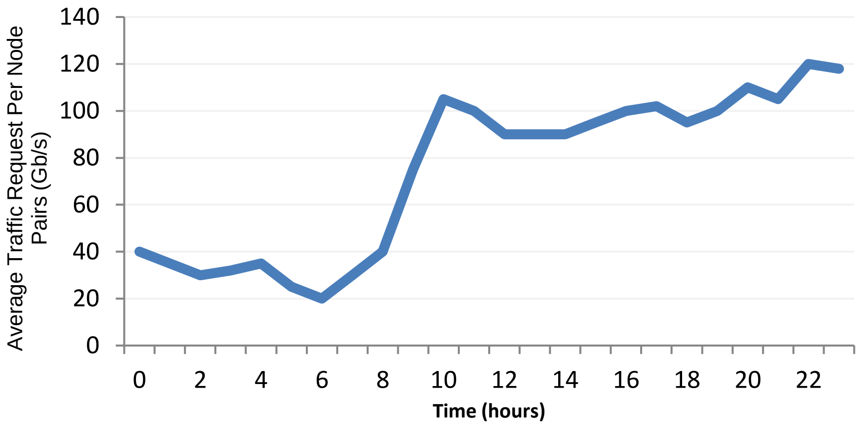


Figure 4-7 Traffic Profile

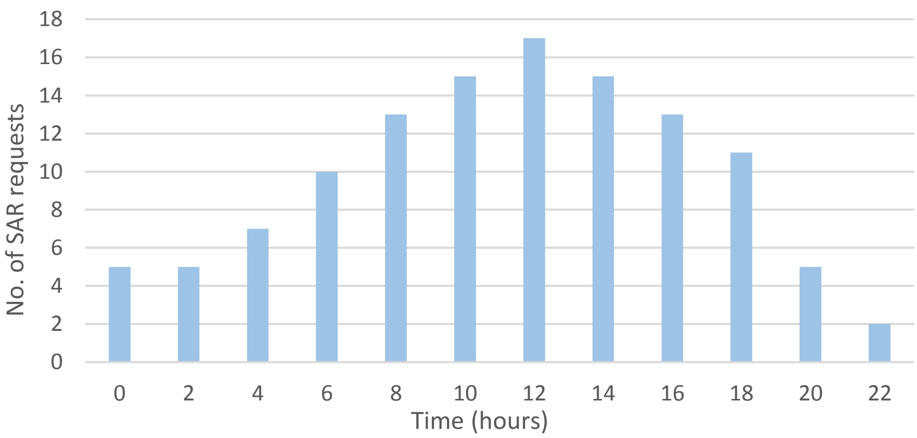


Figure 4-8 SAR requests arrival distribution

In the IFAR scenario, the traffic matrix consists of 60% IR requests and 40% FAR requests. While in IFSAR, RSRR and RARR scenarios, SAR is 20%, FAR is 20% and IR is 60%. These percentages represent the different types of traffic in the network that can be served using these approaches [86]. The VoIP, online gaming, business internet, email, file sharing and consumer web traffic are considered as IR traffic. The VoD and video conferencing are considered as FAR traffic, while the cloud DC to DC synchronization is considered as SAR traffic.

The RARR scenario is evaluated using the heuristic only, as the model fails to produce a result within a reasonable time because of the high number of requests in the input traffic matrix.

The reservation scenarios are evaluated using the traffic profile in Figure 4-7 on a two hour basis. At the beginning of each time slot, the network receives a number of requests and provisions them, with respect to the current network status.

Table 4-3 presents the network parameters including the power consumption of the different network devices and wavelength rate based on the predicted 2020 technologies [83].

Table 4-3 Input Data for the MILP model and heuristics

Power consumption or a router port (p_p)	39.2 W
Power consumption of a transponder (p_t)	86 W
Power consumption of an Optical Switch (p_o)	8.5 W
EDFA's power consumption (p_e)	15.3 W
Distance between neighbouring EDFAs (H)	80 km
Number of wavelengths in a fibre (W)	16
Capacity of each wavelength (B)	1 Tbps

A- Reservation Scenarios

The improvements realised by the sliding requests and rescheduling approaches are compared with IFAR approach. The results in Figure 4-9 show that the IFSAR scenario with 20% of SAR requests can reduce the power consumption by 3% while RSRR approach while the RSRR can save up to 5% as more flexibility is introduced.

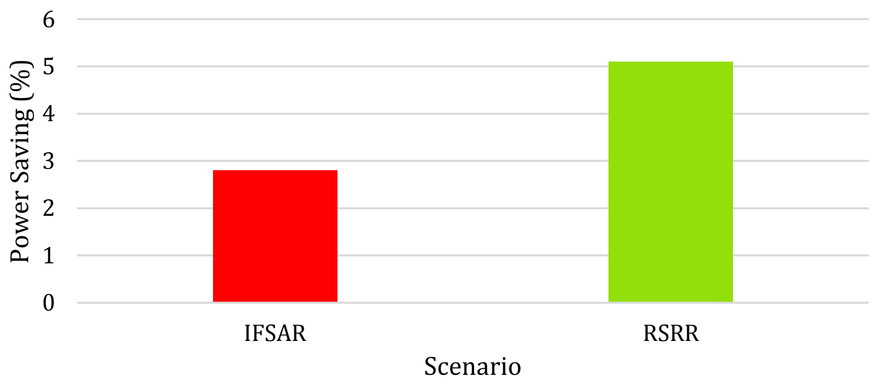


Figure 4-9 The power saving percentage for IFSAR and RSRR scenarios

B- Impact of Traffic Profile

To study the impact of network utilisation on power savings with respect to advance reservation approaches, the power consumption was evaluated under different traffic volumes. Figure 4-10 shows the power saving for different traffic volumes for the two scenarios (IFSAR and RSRR) compared with IFAR. Increasing the network utilisation reduces the power saving because the grooming potential is reduced. The RSRR is less affected by increasing the traffic volumes, because it has the flexibility to select the start time that allows more grooming.

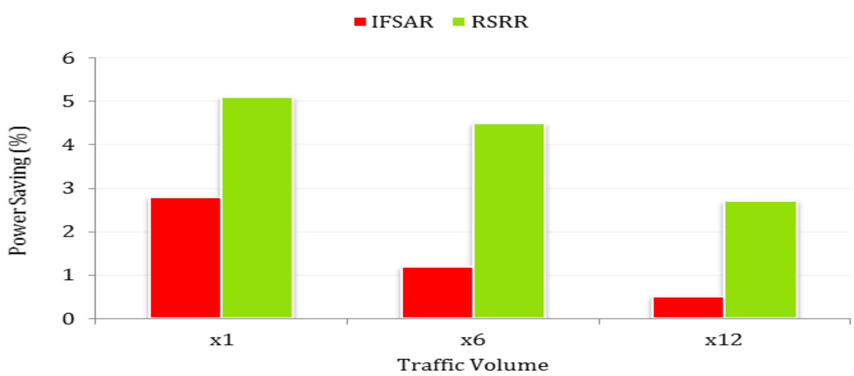


Figure 4-10 The power saving for IFSAR and RSRR with different traffic volumes

C- Impact of sliding window size

To study the impact of increasing the holding time, the sliding window for SAR requests have been increased to 12 and 24 hours. Although 24 hours means shifting some requests to the next day, there are some applications that can accept such a delay. Figure 4-11 shows the network power consumption for three different window sizes (6, 12 and 24 hours).

The larger window means higher degree of freedom and consequently better grooming solution by consolidating the SAR requests within few hours to reduce the active network resources.

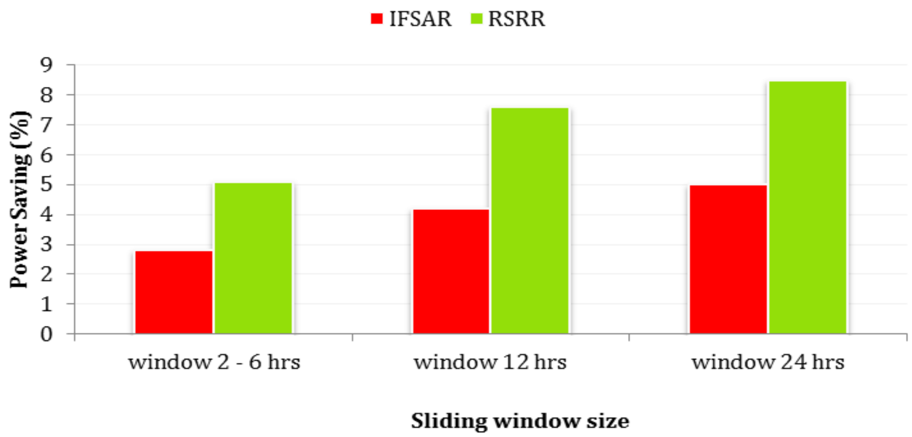


Figure 4-11 the power saving for IFSAR and RSRR for 12 and 24 hours sliding window

D- MILP vs Heuristic for the small network

To validate the model, its results are compared to the results of the heuristics proposed in Section 4.5. The MILP model results of such a network are obtained within a reasonable time. The results in Figure 4-12, show that the different heuristics power consumption are comparable to those of the MILP model.

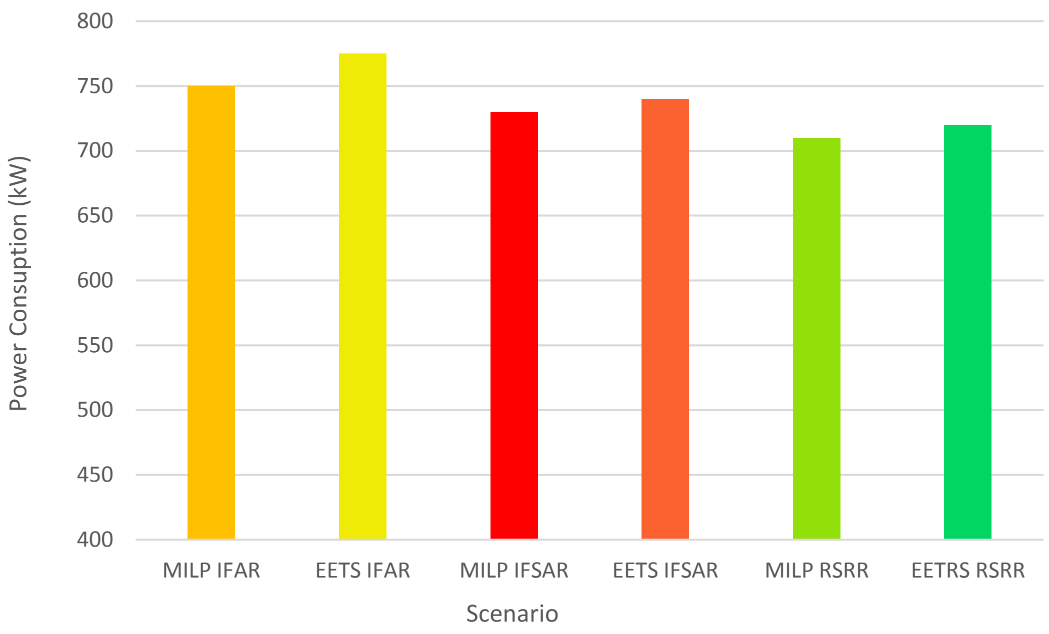


Figure 4-12 the power consumption for MILP models and heuristic for IFAR, IFSAR and RSRR

E- Heuristic results for NSFNET and COST-239

After verifying the heuristics, the heuristics are used to evaluate the different reservation scenarios considering large network topologies, because of the high model complexity at large networks as the grooming problem is an NP-complete [105]. Two topologies are considered which are the NSFNET and COST 239 [85] shown in Figure 3-9 and Figure 4-13, respectively.

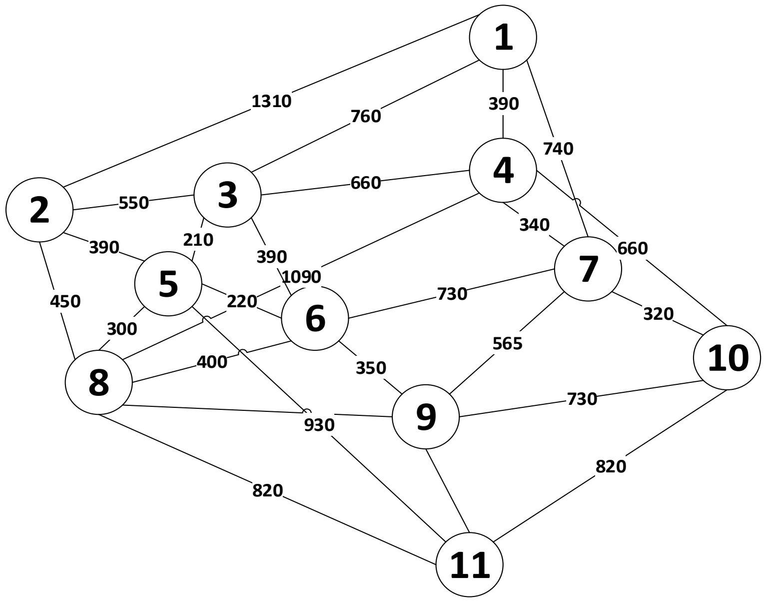


Figure 4-13 COST 239 network with distances in kilometers

Figure 4-14 and Figure 4-15 show the power savings of the IFSAR, RSRR and RARR scenarios for NSFNET and COST 239, respectively. The RARR outperoms the other two scenarios because of its ability to reroute the active requsts (IR, FAR and SAR) in addtion to the yet to start SAR and FAR requets. The higher the traffic volumes the lower the power savings due to reduced grooming possibilities as concluded previously. The COST 239 results show higher power savings as compared with NSFNET, and the reason for that is due to the higher nodal degree in the topology which is 4.7 as comnpared with 2.5 in the NSFNET, and eventaully grooming savings increased.

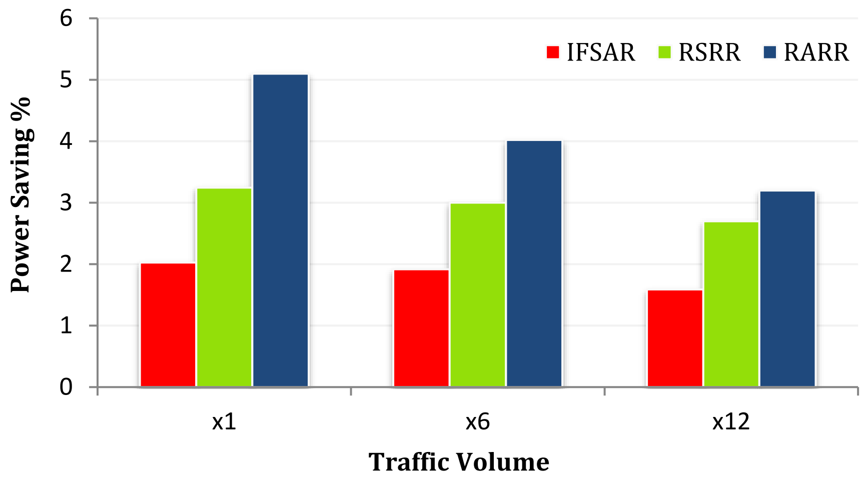


Figure 4-14 The power savings of the NSFNET network

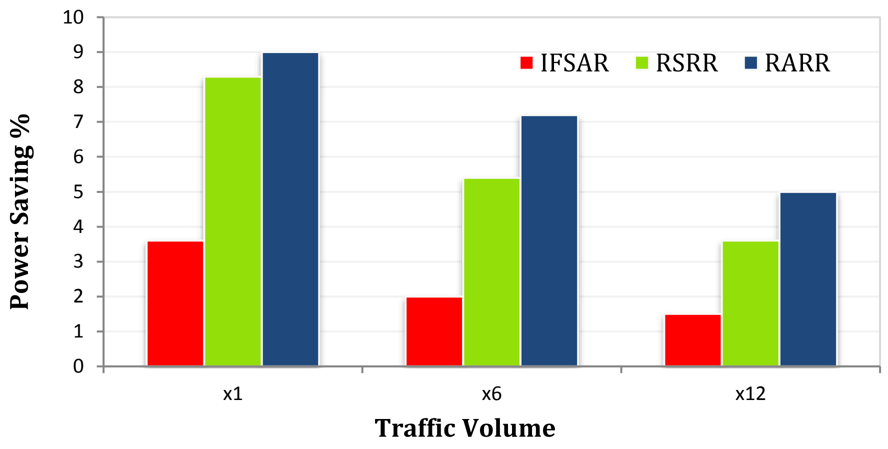


Figure 4-15 The power savings of the COST 239 network

4.7 Summary

In this chapter, the energy-efficiency of advance reservation in optical core network has been considered. The network traffic was classified into three types of reservations, IR, FAR and SAR. Four scenarios have been proposed to study the power savings that can be achieved through advance reservation approaches. The first approach with no sliding-widow AR requests was used, as the baseline approach. The second scenario considers the three types of requests. The third and fourth approaches consider rescheduling and rerouting the not started AR requests. Additionally, the fourth scenario can reroute the active requests. A MILP model and a real time heuristic were developed to optimise the network resource allocation in IP over optical networks considering different classes of scheduled traffic requests. The results show that energy efficient network resource allocation according to the scheduling requirements saves power, 3%; while adding the flexibility of rescheduling and rerouting the reserved traffic requests that have not started saves up to 8% of the network power consumption. The results also show that disrupting the active traffic requests to reroute them increases the power savings to 10%. This limited improvement comes at the cost of a slight increase in the delay experienced by users of the interrupted requests.

Table 4-4 summarises the approaches pros and cons. Also, higher network utilisation reduced the power savings as the grooming savings reduced. Extending the sliding window for delay-tolerant traffic requests for 12 or 24 hours reduced the power consumption, because larger window means scheduling more requests to be groomed together at the same time slots.

Table 4-4 Reservation Scenarios Comparison

Approach	**Traffic disruption**	**Power consumption**	**Cost/Complexity**	**New technology/Features**
IFAR	No	Very high	Very low	Not needed
IFSAR	No	High	Low	Scheduling
RSRR	No	Low	High	Scheduling and rescheduling
RARR	Yes	Very low	Very high	Scheduling, rescheduling and rerouting. Dynamic routing technology.

5 Mitigating Post-Disaster Traffic Floods using Advance Reservation Scheduling in IP over Optical Networks

5.1 Introduction

In Chapter 3, the issue of post-disaster traffic floods has been explored and in Chapter 4 the provisioning problem of AR requests has been addressed. In this chapter the flexibility of AR requests are exploited in post-disaster times to mitigate floods. MILP models and heuristics are developed with the objective of minimising the blocking of post-disaster traffic floods considering the three scheduling approaches that were developed in Chapter 4. The model and heuristics are used to evaluate the network performance for a sample network, while for larger network topologies the heuristics are used.

5.2 Related Work

Most of the discussed literature in chapter four focused on efficient resource provisioning for AR requests. Few research papers have discussed the blocking of IR requests accompanied by AR requests using analytical models. The authors in [106] were the first to propose an analytical model to study resource sharing between IR and AR requests. They have proposed an admission control algorithm in which admission is allowed if the interrupt probability is below a certain threshold. Also [107] proposed an analytical model using discrete time Markov-Chain to show the benefit of book-ahead time compared with immediate reservation. Due to model complexity, the simulation considered a single link only. In [108], the authors overcome this limitation by developing an analytical model that can be run on a whole network with both wavelength conversion and wavelength continuity.

Also, most of the previous work focused on analytical models not linear programming models, and their objective is to analyse the network blocking by provisioning both types of reservations. In this chapter, a MILP model and heuristic approaches are developed to minimise network blocking. However, to the best of our knowledge no previous work considers the sliding-window requests for the objective of optimising network blocking and how to exploit their flexibility to reduce IR blocking.

5.3 AR requests with Floods Approaches

The aforementioned AR scheduling approaches, IFSAR, RSRR and RARR are considered here but in a different context, the post-disaster flooding context. These approaches have two objectives here: the first is resource provisioning in an energy-efficient way, and the second is keeping the blocking as low as possible.

5.3.1 Floods with Traffic Scheduling (FTS)

This is the baseline approach where AR requests are provisioned on their arrival and their flexibility is not exploited, i.e. they are not rerouted or rescheduled to allow floods to be accommodated.

5.3.2 Floods with Traffic Re-Scheduling (FTRS)

In this approach, the operator can reschedule and reroute the reserved AR requests, i.e. not started AR requests. The results in Chapter 4 show that this approach has improved the network energy efficiency due to its ability to reroute and reschedule AR reserved requests to improve network resources efficiency. This flexibility is exploited in the post-disaster traffic flooding scenario to accommodate floods. This approach also aims to maintain the power consumption and blocking to a minimum. Minimising blocking comes from routing the requests both (IR and AR) away from the flooded node, and scheduling the SAR requests far from the flooding time points.

5.3.3 Floods with Traffic Rerouting and Rescheduling of Active and Reserved Request (FTRR)

This approach is an improved version of the FTRS approach where the currently active requests can be rerouted or rescheduled in addition to the reserved AR to allow the maximum flexibility in accommodating traffic floods.

5.4 Floods with AR Scheduling MILP model

The AR scheduling model in Chapter 4 is extended to represent a scenario where one of the nodes becomes flooded after a disaster. The extended model minimises the blocking of traffic floods by optimising the resource allocation for the AR and IR requests. Before constructing the new MILP model, a list for the new parameters and variables are defined. The new model attempts to optimise the resource allocation for the AR and IR requests while minimising the blocking of floods. Below parameter and variable are added to the previous model.

γ and α	Weighing coefficients
Bl_r	Binary blocking variable. If $Bl_r = 1$ then request r is blocked, otherwise it is not blocked.

The model is defined as follows:

Objective: *Minimise*:

$$\gamma \sum_{t \in T} \left(\sum_{l \in L} P_r \; W_l^t + \sum_{l \in L} P_t \; W_l^t + \sum_{l \in L} (P_a \, A_l \, F_l) + \sum_{m \in N} P_o + \sum_{l \in L} (P_g \, RG_l \, W_l^t) \right) + \alpha \sum_{r \in I} Bl_r \tag{5-1}$$

The objective function aims to minimise the total network power consumption by minimising the resources used while minimising the floods blocking.

$$dr_r \, \beta_t^r = \sum_{p \in P} x_{pt}^r \tag{5-2}$$
$$\forall t \in T, \forall r \in F, S$$

$$dr_r F_{sd} \, \beta_t^r = \sum_{p \in P} x_{pt}^r \tag{5-3}$$
$$\forall t \in T, \forall r \in I, \forall s, d \in N: s = sr_r$$

Constraints (5-2) and (5-3**)** are the demand constraints, where for each request the sum of the traffic on the paths between the source and destination is equal to the request data rate. Constraint (5-2) represents the demand constraint for the AR requests while constraint (5-3**)** is for the IR requests. In (5-3**)**, the request data rate is multiplied by the flood multiplier (if the node is not flooded then $F_t^{sd} = 1$).

$$W_l^t = \sum_{r \in D} \sum_{p \in P} \frac{x_{pt}^r}{B} + \; ex_l^t + k_l^t \tag{5-4}$$
$$\forall t \in \mathrm{T}, \forall l \in L$$

$$k_l^t < 1 \tag{5-5}$$
$$\forall t \in \mathrm{T}, \forall l \in L$$

Constraint (5-4) represents the grooming constraint where the total number of wavelengths on link l at time point t equals the summation of the newly arrived requests wavelengths and the previously scheduled requests wavelengths added is a small fraction that helps with ceiling the wavelength value to be an integer value. Constraint (5-5) bounds the ceiling/converting variable to less than 1.

$$\sum_{t=st_r}^{et_r+du_r-1} \beta_t^r = (1 - Bl_r)du_r \qquad \text{(5-6)}$$

$$\forall r \in I$$

$$\sum_{t=st_r}^{et_r+du_r-1} \beta_t^r = du_r \qquad \text{(5-7)}$$

$$\forall r \in F, S$$

$$\beta_t^r = 0 \qquad \text{(5-8)}$$

$$\forall r \in D, \forall t \in T, t < st_r \lor t \geq et_r + du_r$$

Constraints (5-6)-(5-8) ensure that the request service time equals the duration of the request within the service window.

$$W_l^t \leq WF_l \qquad \text{(5-9)}$$

$$\forall l \in L, \forall t \in T,$$

The capacity constraint (5-9) ensures that the total number of wavelengths in a physical link does not exceed the maximum capacity of the physical link.

$$\delta_0^r = \beta_0^r \qquad \text{(5-10)}$$

$$\forall r \in S$$

$$\delta_t^r \geq \beta_t^r - \beta_{t-1}^r \qquad \text{(5-11)}$$

$$\forall r \in S, \forall t \in T$$

$$\sum_{t=0}^{T} \delta_t^r \leq 1 \qquad \text{(5-12)}$$

$$\forall r \in S$$

$$\left(\sum_{i=0}^{du_r} \beta_{t+i}^r\right) - du_r \geq -M(1 - \delta_t^r) \qquad \text{(5-13)}$$

$$\forall r \in S, \forall t \in T: \quad st_r \leq t \leq et_r + du_r - 1$$

Constraints (5-10)-(5-13) are the same as constraints (4-9)-(4-12) as they ensure that the SAR request service time is contiguous inside the sliding window which is explained earlier.

For FRTS and FTRR scenarios, the same model can be used except the grooming constraint (5-4) is replaced by constraint (5-14). This constraint is similar to constraint (4-13) in the previous chapter.

$$W_l^t = \sum_{r\in D}\sum_{p\in P}\frac{x_{pt}^r}{B} + ex_l^t + k_l^t - \sum_{r\in R}\sum_{p\in P}\frac{xr_{pt}^r}{B} \quad (5\text{-}14)$$

$$\forall t \in \mathrm{T}, \forall l \in L$$

5.5 Floods with AR scheduling Heuristic

Due to model complexity, a real time approach is implemented. To verify the model performance and enable real time operation, three real time heuristics have been designed for the three approaches. In the previous two chapters, two types of heuristics were developed. The first for the floods scenario with the objective of minimising blocking and the second is for the scheduling approach where the objective was provisioning the AR requests in an energy-efficient way. The new heuristics are inspired by both objectives, as the aim is to minimise blocking while provisioning the requests using the lowest power consumption.

Basically, the AR is a request that should not be blocked due to its high level of commitment while the IR is a request that can be accepted or blocked, due to its nature of being submitted immediately. These principles considered in the heuristic design. The scheduling heuristic discussed in Section 4.5 starts with serving the IR and FAR requests while leaving the SAR requests to the end so it can find a better solution for grooming. In the current scenario, and due to the increased amount of traffic, AR requests is given a high priority leaving the IR requests to the end in order not to fill the available capacity and avoid violating the AR commitments.

Generally, each heuristic contains four main procedures, three are responsible for provisioning the three types of requests and the fourth is responsible for routing. In the first scenario, the network schedules and route the requests at their arrival time which is the baseline for the scenarios. The algorithm is similar to EETS, except for one change, where the AR is provisioned first then IR requests are provisioned afterwards. The algorithm is called Floods with Traffic Scheduling (FTS) shown in Figure 5-1. The AR requests use the EER heuristic shown previously in Figure 4-3. The IR floods use the MBR heuristic which is shown in Figure 5-2 while the non-flooding IR requests use the ERR heuristic. The MBR heuristic attempts to get lower blocking by searching for the residual capacity in all the possible paths between each source-destination and not only the k-minimum hop paths.

The second algorithm is for the FTRS scenario which is shown in Figure 5-3 and called Floods with Traffic Rescheduling (FTRS). In this algorithm, there are two options. The first represents the normal operation and the second represents when floods take place. It starts by deleting the previously scheduled AR requests and reprovision them again as they have just arrived with the newly arrived requests. The first option objective is to minimise power consumption while the second option aims to minimise blocking during flooding. When floods take place, the criteria for scheduling and routing should take different action to minimise the blocking and improve network utilisation. So for routing/rerouting AR requests and the non-flooding IR requests, it uses the FPR heuristic.

The FPR heuristic is shown in Figure 5-4. It attempts to route these non-flooding requests far away from the flooded node by using a weighted graph that assigns high weights for the links connected to the flooded node. Then based on the minimum cost routing it will choose the lowest cost routes to provision the paths. So for scheduling SAR requests, the algorithm chooses the lowest utilisation time points to schedule the request during low traffic periods.

The FTRR approach, shown in Figure 5-5, is similar to the FTRS heuristic except it can act on the currently running requests plus the not started ones. However, as an algorithm it is similar to the FTRS except that during the deletion of the previously scheduled AR requests, it will disrupt the currently running AR/IR requests and delete their provisioned paths. Obviously, the parameter xr_p^t contains all the previously routed information, so the first step is to delete their paths and route them as they have just arrived.

Table 5-1 scenarios comparison

	FTS	**FTRS**	**FTRR**
Scheduling under normal operation	Schedule SAR requests on their arrival only	Reschedule SAR requests before their start time	Reschedule SAR requests before their start time
Routing under normal operation	Route once at arrival	Reroute AR before their start time	Reroute AR/IR at each time point
Routing/Rerouting under floods	Do nothing	Rerouting: Avoid flooded node during rerouting for the future hours	Rerouting: Avoid flooded node during rerouting for now and the future hours
Scheduling/Rescheduling under floods	Do nothing	Rescheduling: Avoid high utilized network hours	Rescheduling: Avoid high utilized network hours

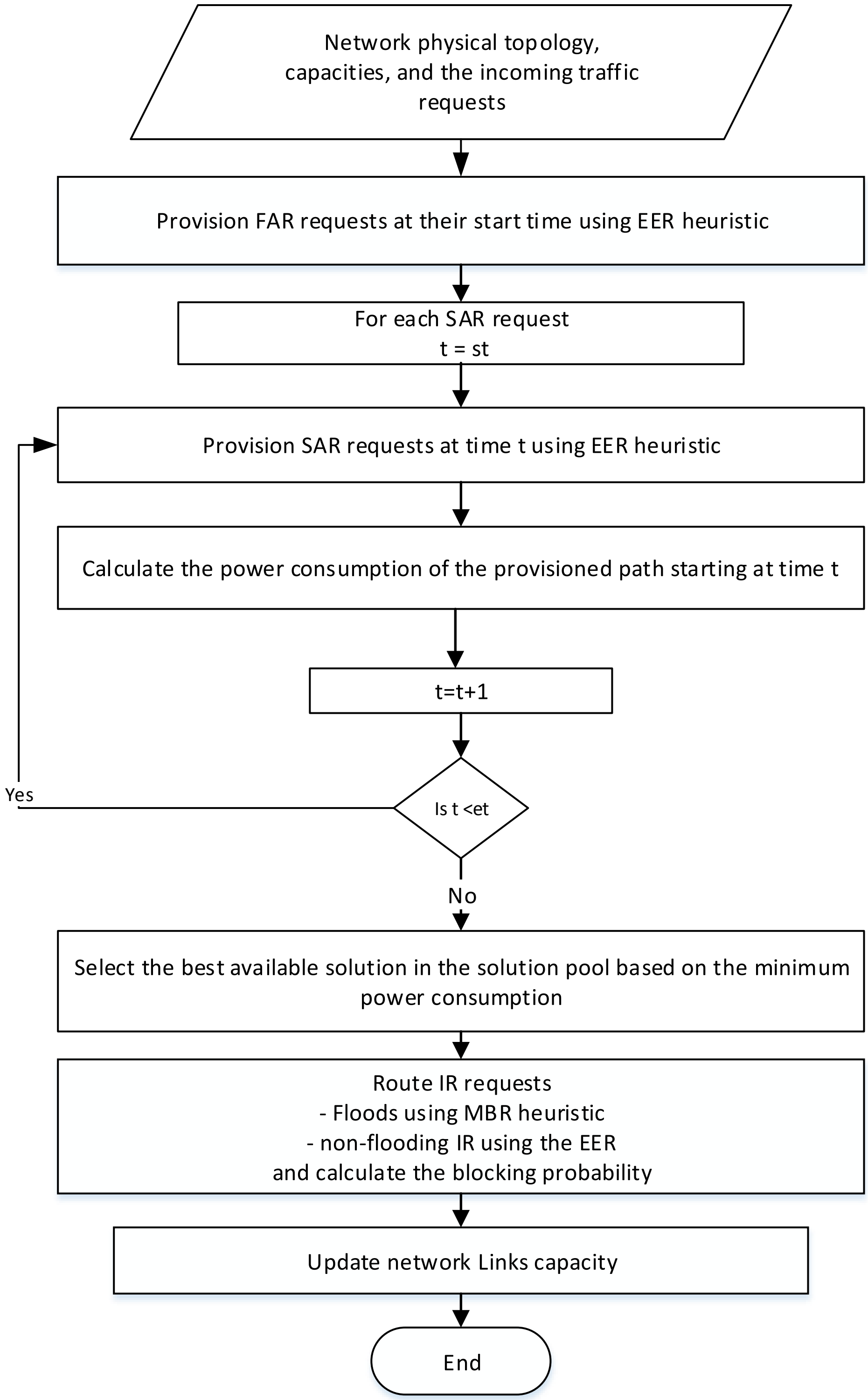


Figure 5-1 FTS heuristic

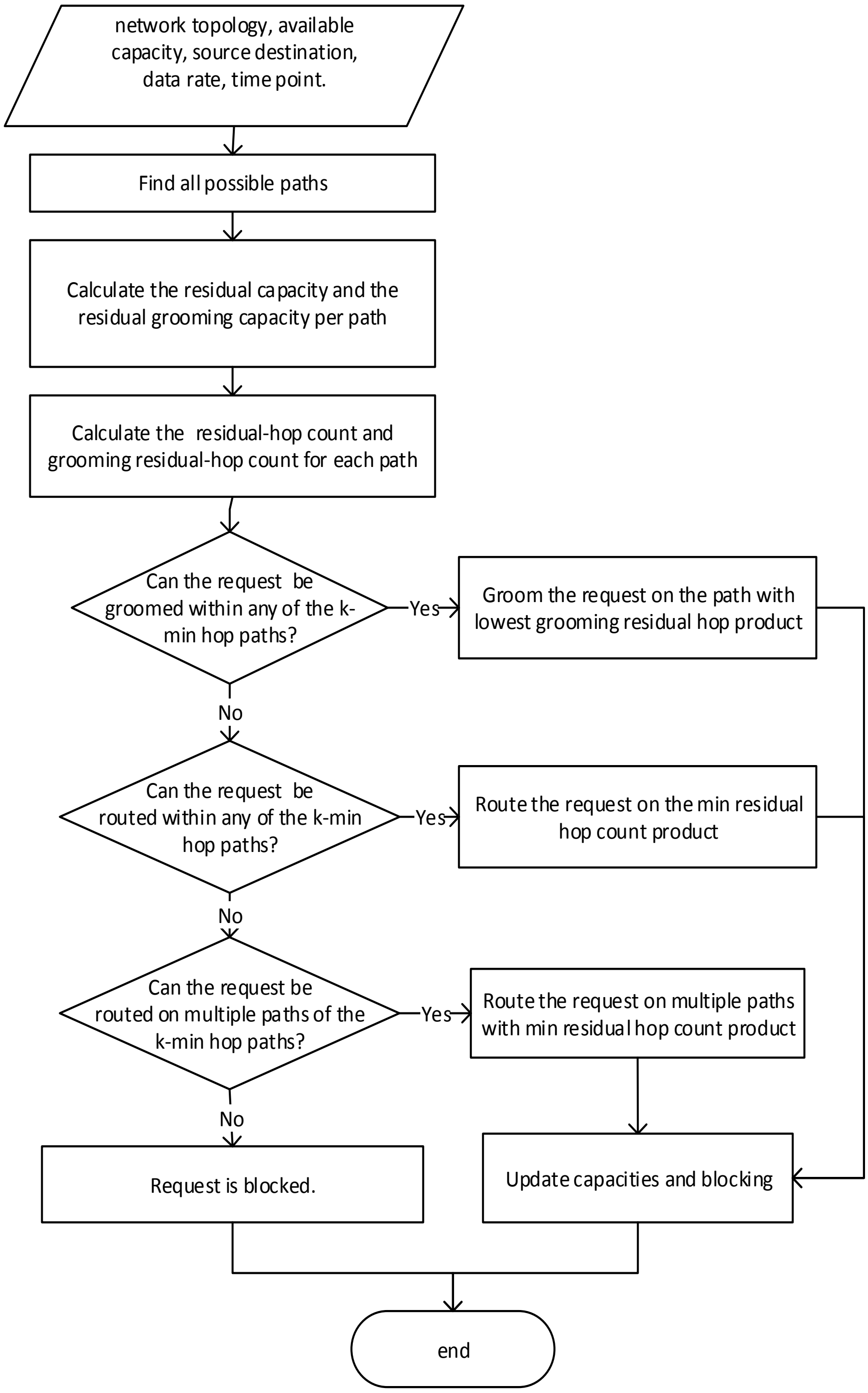


Figure 5-2 MBR heuristic

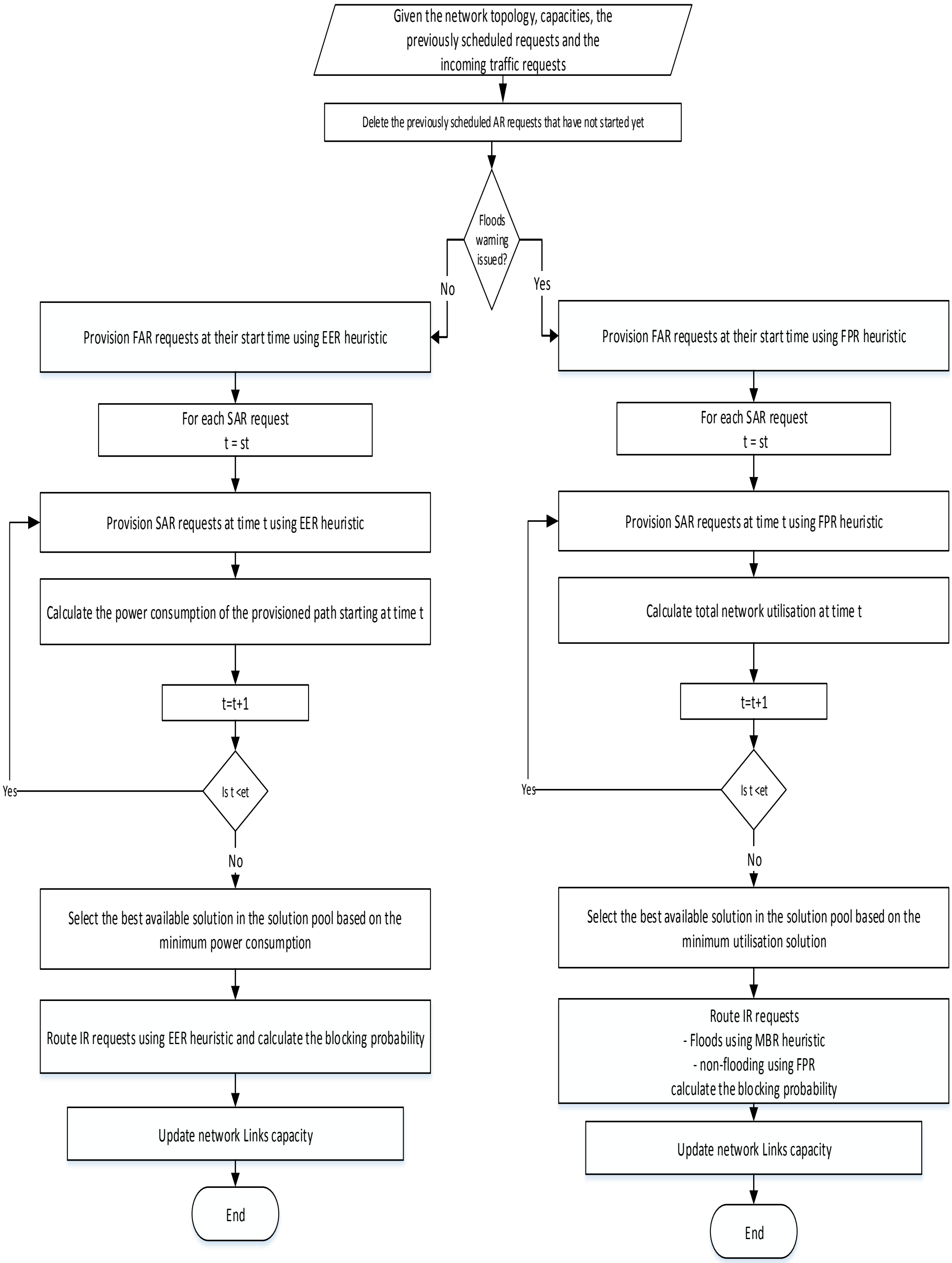


Figure 5-3 FTRS heuristic

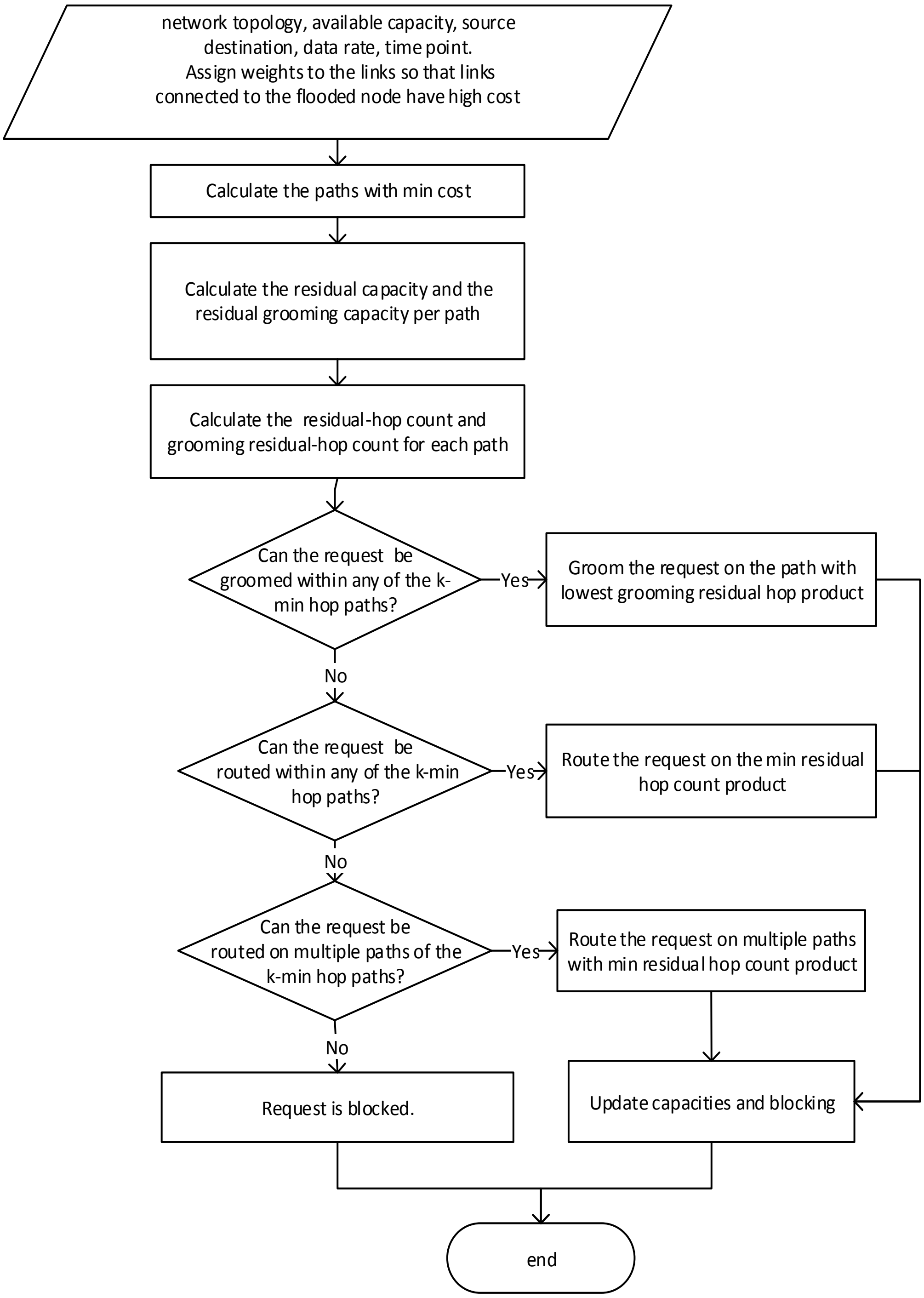


Figure 5-4 FPR heuristic

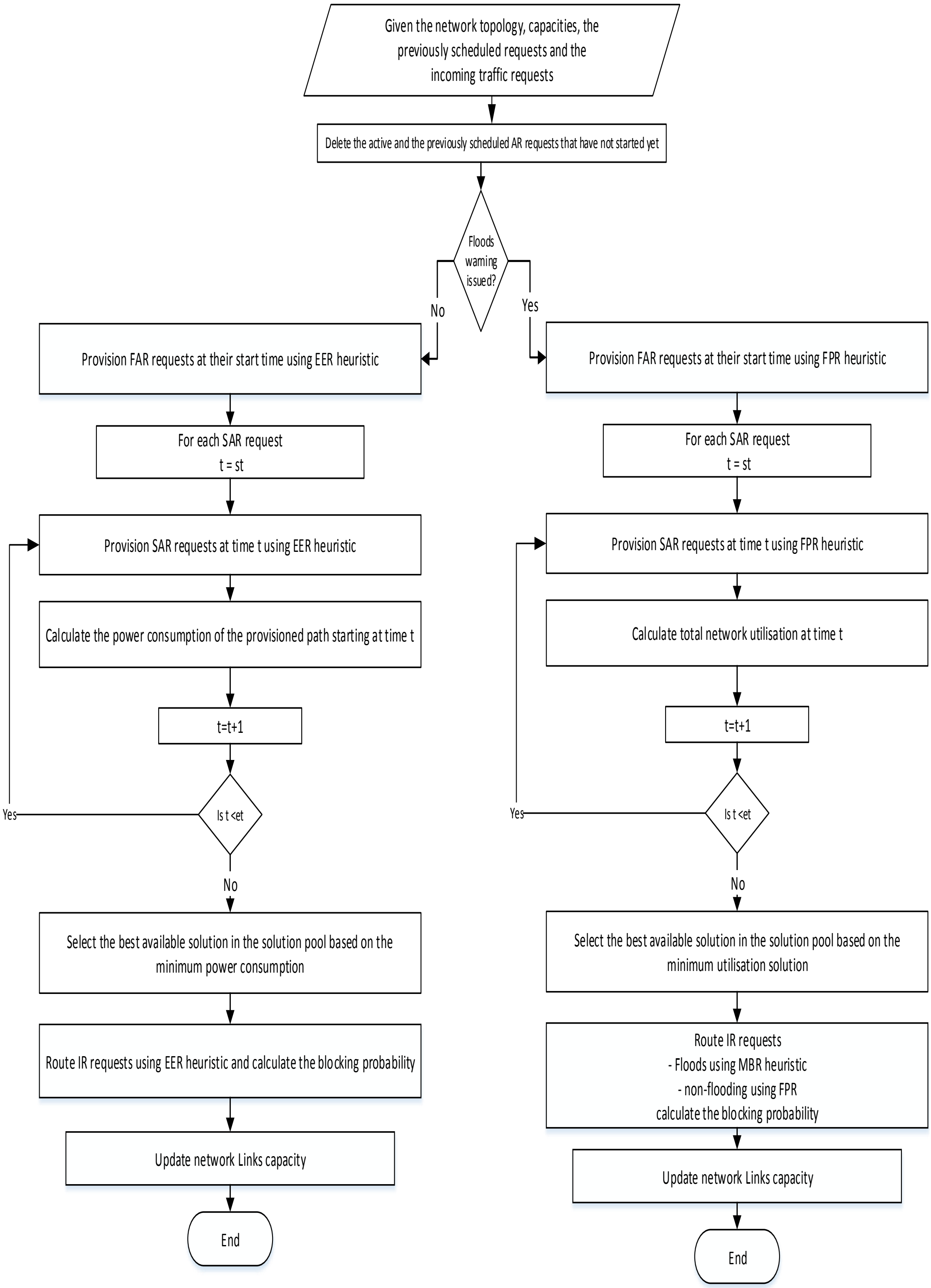


Figure 5-5 FTRR heuristic

5.6 Network Performance Evaluation

Due to the model complexity, the same procedure of the previous chapter is followed, where the MILP model is evaluated on a small example network and it is thus verified by comparing its results to the heuristic. Then the heuristic is used for larger network topologies. The sample network topology with the same traffic profile of the previous chapter was used which is depicted in Figure 4-6 and Figure 4-7, respectively. The traffic consists of 60% IR requests and 40% AR requests. The AR requests consists of 20% SAR and 20% FAR and these percentages are based on [86]. The AR requests arrival follows a Poisson distribution that can be shown in Figure 4-8.

The reservation approaches are evaluated using the traffic profile in Figure 4-7 on a two hour basis. At the beginning of each time slot, the network receives a number of requests and provisions them, with respect to the current network status.

A single node flooding will take place at a time and within specific hours of the day. Two nodes are chosen one with nodal degree of 2 at a middle location (node 4) and the other in the edge with nodal degree of 3 (node 1). The flooding is assumed to take place from midday until midnight. The proposed scenarios are evaluated under these assumptions to check the network behaviour.

Figure 5-6 and Figure 5-7 show the blocking percentage for node 1 and node 4 flooding scenarios respectively, considering the traffic floods to be triple the normal IR traffic for the three proposed approaches for both models and heuristics. For node 1 and node 4, the flooding happens at 12:00, but no blocking happens until 20:00 hours, because the traffic is low compared with busy hour traffic and can be served within the overprovisioned capacity (overprovisioning factor of 2). Node 4 blocking is higher as compared to node 1 because of its location and nodal degree. The higher nodal degree leads to less blocking probability, because higher nodal degree means more freedom in routing.

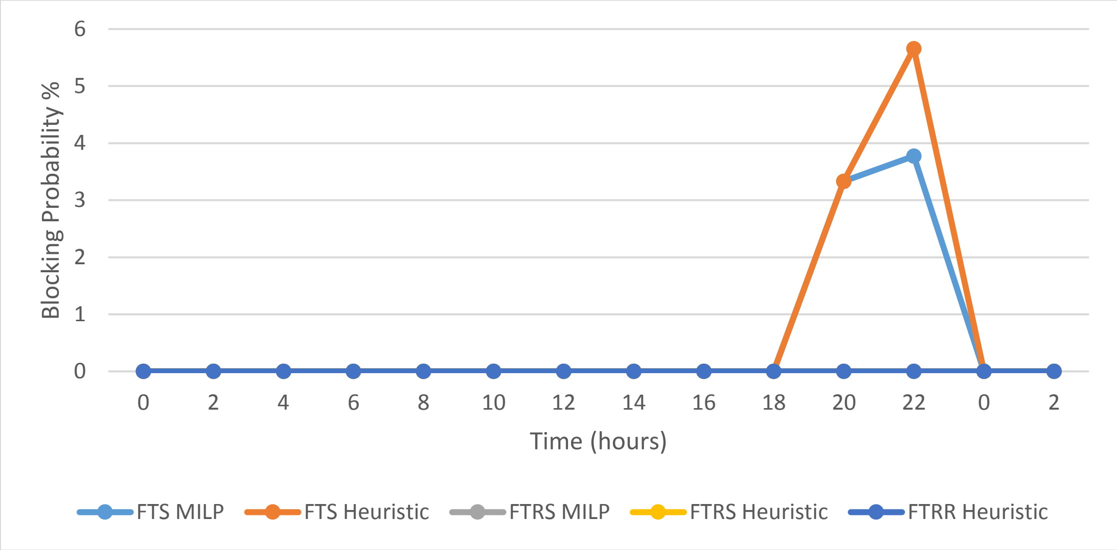


Figure 5-6 The floods blocking percentage for node 1

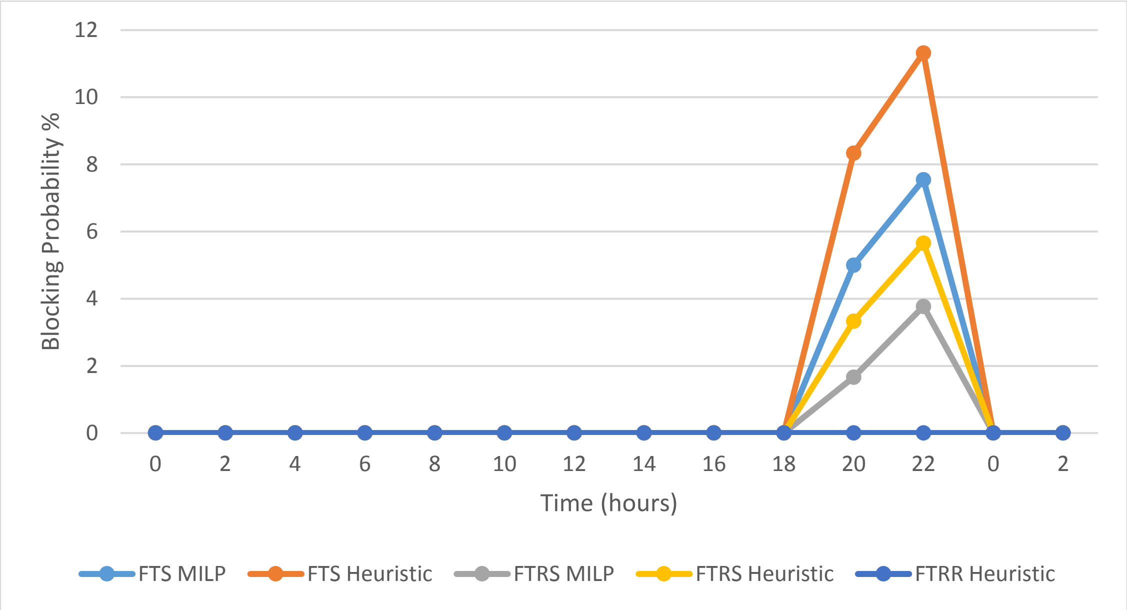


Figure 5-7 The floods blocking percentage for node 4

The FTRS approach outperforms the FTS scenario in terms of blocking, as it manages to reduce the blocking by 4%. This reduction is due to the ability of the FTRS to reprovision the previously provisioned AR requests. The reprovisioning includes rerouting for FAR requests and rerouting and rescheduling for SAR requests. The rerouting allows finding an alternative path for the AR requests routed through the flooded node and therefore allows the flooded node to use its resources to serve its own traffic. The rescheduling can help reschedule the SAR requests to avoid the flooding time by pushing the sliding requests towards the end of the sliding window.

In the heuristic approach, the FTRS heuristics results approach those of the model as the heuristic mimics the model behaviour. In the heuristic approach, the floods warning changes the provisioning process by choosing the lowest utilisation time points instead of lowest power consumption and avoiding flooded nodes instead of using shortest path routing. In the simulation, the floods warning is issued at 12:00, so the routing and scheduling decisions are changed starting at that time.

To determine how the two approaches perform in terms of scheduling Figure 5-8 shows the number of SAR requests scheduled at each time point. The FTS approach attempts to provision the AR requests in an energy-efficient approach which means grooming as many requests as possible during the busy hours, and consequently the FTS has a higher blocking probability. On the other hand the FTRS reschedules SAR demands to avoid the flooding time by pushing them to the end of the sliding window. The FTRS has two objectives in rescheduling the first is to groom more requests and the second to reduce blocking. The grooming can be seen at 14:00 hours where the number of groomed SARs for the FTRS is higher than FTS approach. This improved grooming is a result that benefits from the flexibility of the sliding window size that ranges between 2 and 6 hours. Thus, FTRS reschedules as much SAR requests as possible to start at the end of the sliding window. Reduced blocking can be seen at time 00:00 hours of the next day. This is attributed to the FTRS approach which rescheduled the SARs that should start at the busy hours towards the next day. This rescheduling means freeing more resources during the busy hours that can be used by the floods. On the other hand, the FTS approach scheduled a large number of SAR requests at 20:00 and 22:00 hour, and that leads to higher blocking.

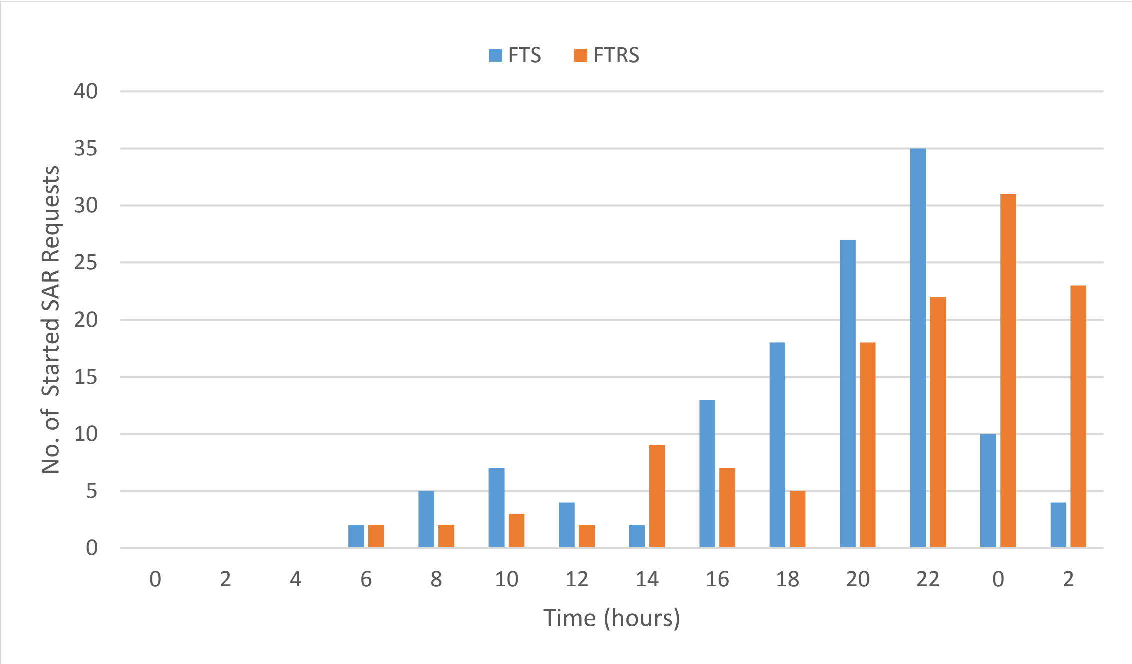


Figure 5-8 No. of started SAR requests for FTS and FTRS

A flooding multiplier of x5 is considered for node 1 and node 4. The floods blocking percentage is shown in Figure 5-9 and Figure 5-10, respectively. Clearly the blocking probability increases with the increase of the floods.

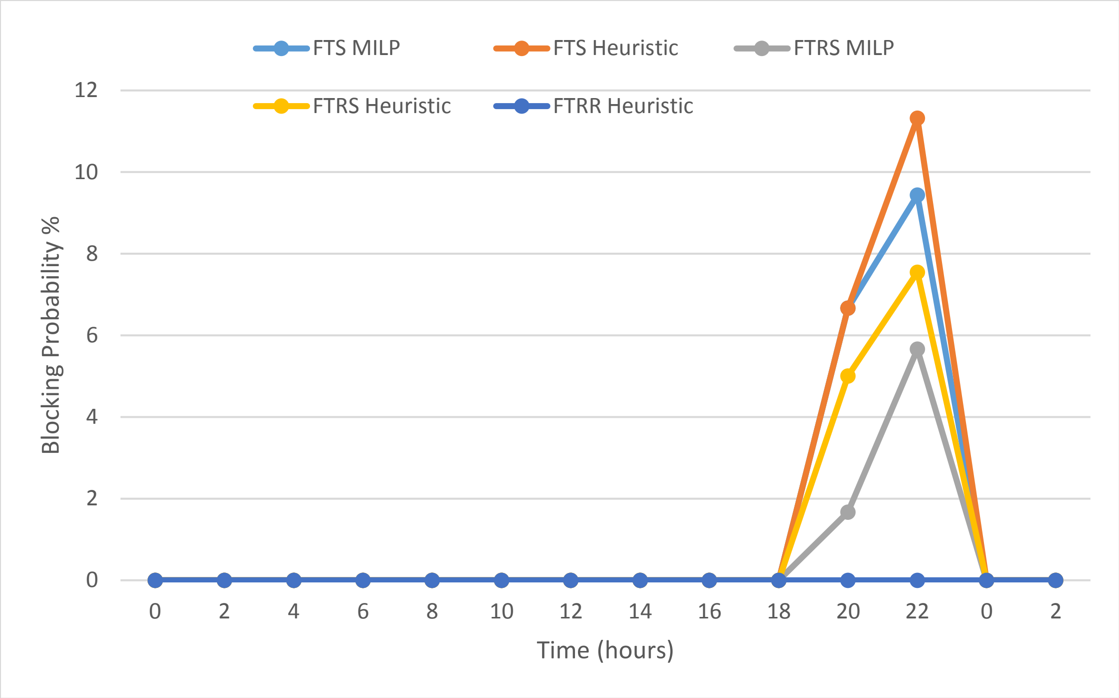


Figure 5-9 The blocking percentage for node 1

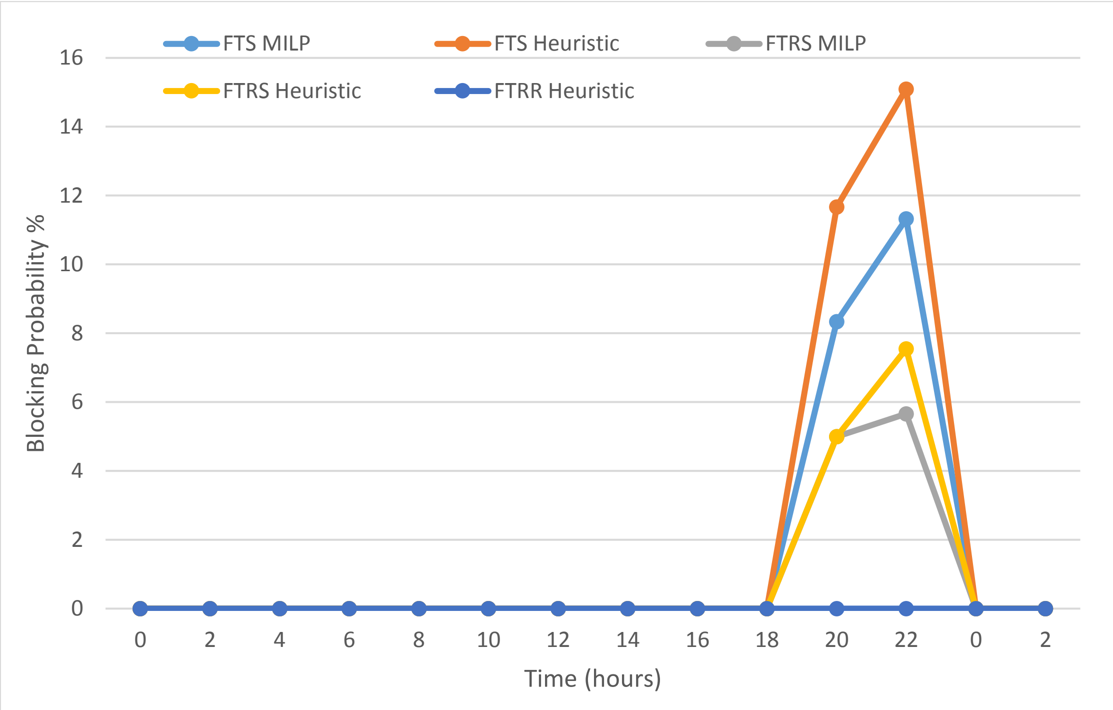


Figure 5-10 The blocking percentage for node 4

For large network topologies, the heuristic is evaluated on the NSFNET. There are five DCs located in nodes (2, 3, 7, 8 and 9). The heuristic approaches are evaluated for nodes (1, 7 and 12) considering single flooding node at a time with floods of 5x the amount of regular traffic. Two flooding scenarios are considered the first lasts for 12 hours starting from midday till midnight and the other lasts for 4 hours starting from 20:00 to 23:59.

The longer flooding scenario results are shown in Figure 5-11. The results show that the FTS approach fails to fully serve the floods within the high traffic hours while the FTRS and FTRR successfully serve all the floods as they adapt the scheduling and routing of AR requests under floods.

The location and nodal degree of the flooded node have a significant impact on the floods blocking probability. For node 1 flooding scenario, the floods blocking probability is zero, using the three approaches, because it lies next to DC nodes (2 and 3) and it is a transit node connecting the east to west of the network. This location imposes high links capacities which can be useful in flooding times. Node 7 which is a data centre located at the edge of the network with a low nodal degree has the highest blocking probability because most of its resources are already used for traffic originating/destined to the node. Due to its location at the edge of the network, transit traffic through node 12 is limited and therefore its links capacities are limited resulting in blocking the floods.

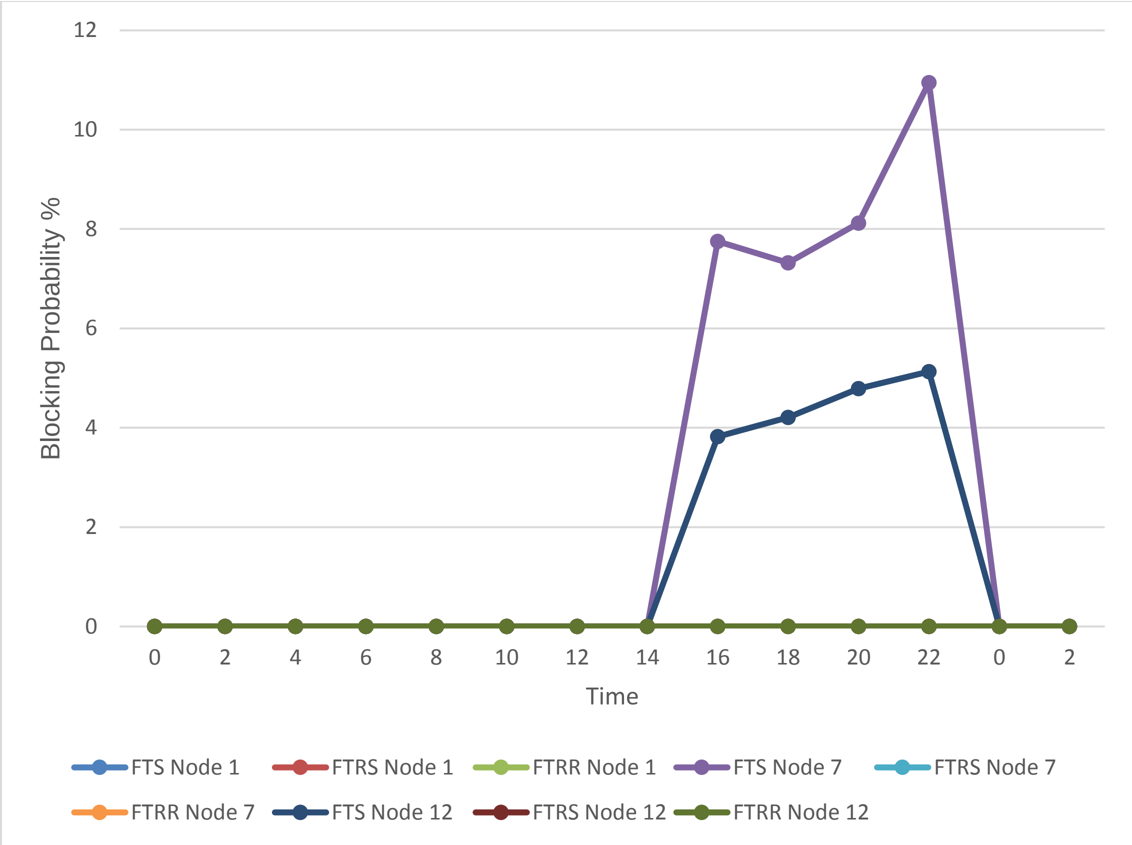


Figure 5-11 The floods blocking percentage under the 12 hours flooding scenario

In Figure 5-12 the shorter flooding scenario results are shown for the different node flooding scenarios. The FTRS fails to fully serve the floods under node 7 and node 12 scenarios at time 20:00. The FTRS attempts to reprovision the reserved ARs, however this is not enough to create capacity to accommodate the floods as the floods start within the busy hours where the active traffic is the highest. AR requests were already scheduled to start at time 20:00 and that time, 20:00, is within the busy hours. On the other hand the FTRR can fully serve the floods by rerouting the active requests (AR and IR).

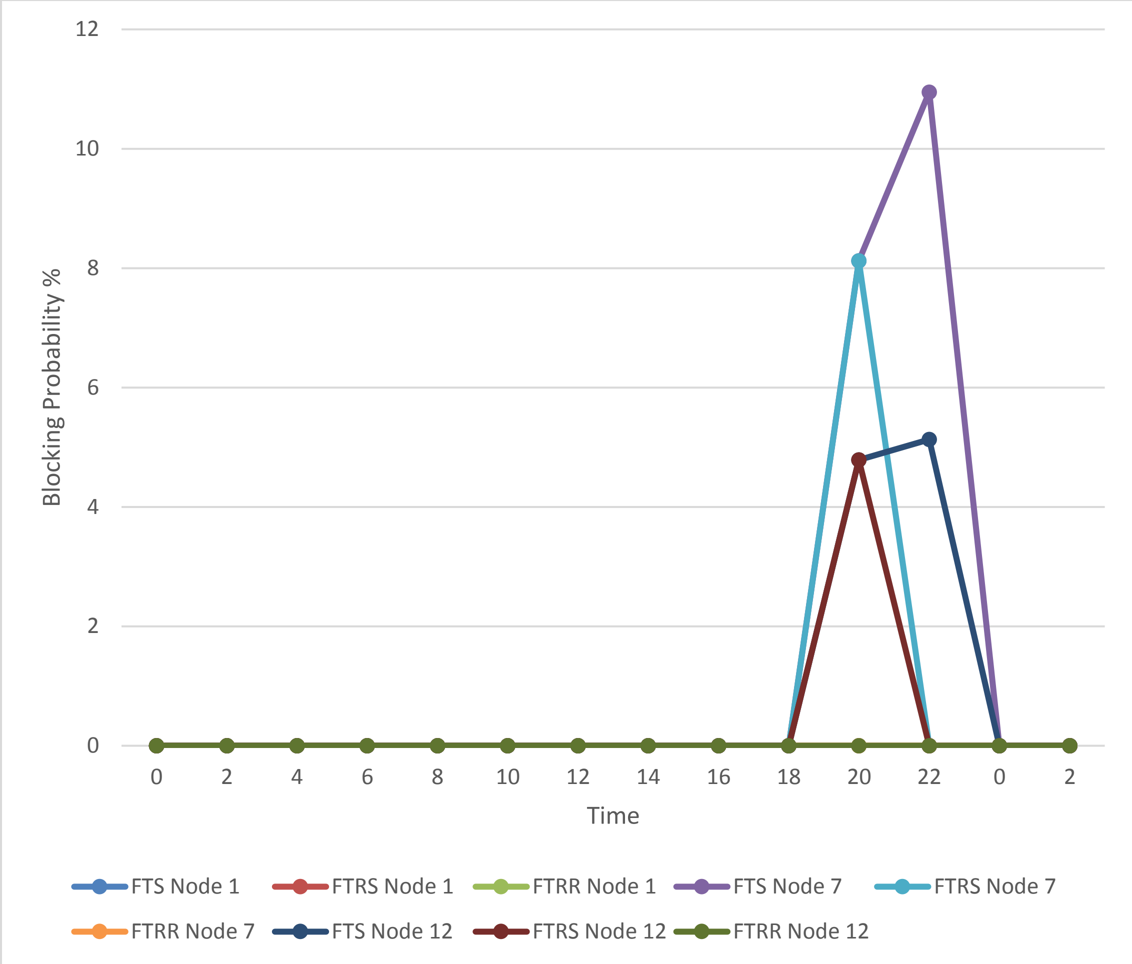


Figure 5-12 The floods blocking percentage under the 4 hours flooding scenario

5.7 Summary

In this chapter, the flexibility of advance reservation has been exploited to mitigate the short-term capacity exhaustion. To accommodate the post-disaster traffic floods, the AR requests can be delayed or rerouted to avoid flooding time and node. Three scheduling scenarios have been considered within the disaster context and their different flexibility degrees are deployed to alleviate the floods. MILP models were developed to evaluate the network performance under advance reservation and traffic floods. Also, heuristic approaches were developed independent of the MILP models for the three proposed scenarios. The heuristics verified the MILP results, and furthermore enable real time operation for larger network topologies.

A sample network topology was evaluated using the MILP models. The results show that the FTRS approach achieve a lower blocking probability compared with the FTS approach. The FTRR approach outperforms the other scenarios due to its ability to adapt to network utilisation changes but this is at the cost of a slight increase in the delay experienced by users of the interrupted requests. Furthermore, the heuristics were used to evaluate the NSFNET performance under two flooding scenarios. The first scenario where the flooding lasted for 12 hours from midday till midnight. The results showed that FTRR and FTRS approaches succeeded in eliminating blocking. While in the second scenario where the flooding lasted for 4 hours during the peak hours, the FTRS failed to react and the flooded node got blocking. On the other hand, the FTRR succeeded in both scenarios because it react to the changes online. Table 5-2 summarises the scenarios pros and cons.

Table 5-2 Reservation Scenarios Comparison

Approach	**Traffic disruption**	**Blocking**	**Cost/complexity**	**New technology/features**
FTS	No	High	Low	Scheduling
FTRS	No	Low	High	Scheduling and rescheduling
FTRR	Yes	Very low	Very high	Scheduling, rescheduling and rerouting. Dynamic routing technology.

6 Blackout Resilient Network

6.1 Introduction

A disaster may not necessarily demolish the telecom infrastructure, but instead it might affect the national grid and cause blackout and consequently disrupting the network operation unless there is an alternative power source(s). In this chapter, power outages are considered, and the network performance is evaluated during a blackout. Two approaches are presented to minimise the impact of power outage and maximise the survival time of the blackout node. A MILP model is developed to evaluate the network performance under single node blackout scenario.

6.2 Blackout Disaster

During the Japan Earthquake in 2011, the affected area was left in a blackout, where 1500 telecommunications switching offices were left without main power supply except few limited batteries. Eventually, the switching systems shut down after few hours when the batteries charge was depleted [66]. In Italy in 2003, there was a total blackout that lasted for 12 hours and impacted the whole country [1].

Most of the countries rely on a national grid network, and any disruption in the grid might bring systems in the country as a whole that relay on electricity down. The recent energy strategies that promote the use of renewable energy can help, however still the use of renewable energy is limited even in the developed countries.

Usually, the telecommunications central offices (COs) are equipped with either renewable energy supply and/or diesel generators. Obviously these are of limited availability. As stated earlier in Chapter 2, ensuring that the networks survives during disasters is essential in disaster evacuation operations. Optimising the power consumption throughout the network is essential in building disaster-resilient networks. Building energy-efficient survivable networks was investigated in a number of papers [109], [110], but the approach does not consider disaster survivability or limited power sources. Few papers in the literature have the use of renewable energy [39], [111]. The considered approaches attempted to study maximising the usage of renewable sources to replace brown energy.

In [112] the authors studied the disasters that causes power outages, and proposed a framework for disasters risk assessment. Based on the assessment, the logistic resources are planned by providing portable generators and permanent solar cells.

In this work, the survival time of blackout nodes is extended by reducing the amount of traffic that is routed through these limited power nodes. Furthermore, during renewable energy production hours, the available renewable energy is exploited first before using the battery energy.

6.3 MILP for Blackout Resilient Scenarios

A MILP model is developed to optimise the routing in core networks under a single node blackout scenario where limited alternative energy sources are available to the blackout node. The model objective is to reduce the total power consumption where the batteries power is prioritised in the minimisation.

These energy sources can be renewable sources, batteries, diesel generators added to the national power.

The model considers a bypass IP over WDM architecture. The available energy sources are assumed to be used to power on the network equipment only, i.e. the power consumption of CO cooling system, servers is not considered. In addition, as the focus in this thesis is on the core network, the access network and aggregation routers are not considered.

Before introducing the model, the parameters and variables used in the model are defined Table 6-1.

Table 6-1 Sets, parameters and variables for the blackout MILP

Notation	Description
N	Set of nodes
N_i	Set of neighbouring nodes of node i
s *and* d	Denote source and destination nodes of a traffic request
i *and* j	Denote end nodes of a virtual link in the IP layer
m *and* n	Denote end nodes of a physical link in the optical layer
TD	Time slot duration
P_r	Power Consumption of a router port
P_t	Power Consumption of a transponder
P_o	Power Consumption of an optical switch
P_e	Power Consumption of an EDFA
P_g	Power Consumption of a regenerator
B	Capacity of a wavelength
W	The number of wavelengths per fibre
A_{mn}	Number of EDFAs on physical link (m,n).

	Typically, $A_{mn} = \left(\frac{L_{mn}}{s} - 1\right) + 2$, where s the distance between two neighbouring EDFAs and L_{mn} is the distance between (m, n).
F_{mn}	Number of fibres in link (m, n)
RG_{mn}	The number of regenerators in link (m, n)
α, β, γ *and* δ	Weighing coefficients
λ^{sd}	Traffic request from node s to node d
B_i	The available battery energy at node i
R_i	The maximum output power of the renewable energy source in node i
λ_{ij}^{sd}	The traffic flow of request (s, d) that traverse the virtual link (i, j)
C_{ij}	The number of wavelength channels in the virtual link (i, j)
W_{mn}^{ij}	The number of wavelength channels in the virtual link $(i$, $j)$ that traverse link (m, n)
bl_{sd}	Binary blocking variable. If $bl_{sd} = 1$ then request from node s to node d is blocked, otherwise it is not blocked.
RE_s	The amount of renewable power consumed at node s
BT_s	The amount of power withdrawn from a battery during time slot t at node s
BR_s	The amount of grid (brown) power consumed at node s

The model is defined as follows:

Objective function: *Minimise*

$$\sum_{i \in N} (\alpha \, RE_i + \beta \, BR_i + \gamma \, BT_i) + \delta \sum_{s \in N} \sum_{d \in N : s \neq d} bl_{sd} \tag{6-1}$$

The objective function (6-1) minimises the power consumed from the different power sources at each node, while keeping the blocking to minimum. Each power source is weighted by coefficient. Tuning these coefficients adjusts the operator's energy strategy. The traffic flow conservation can be formulated as:

$$\sum_{j \in N\, i \neq j} \lambda_{ij}^{sd} - \sum_{j \in N\, i \neq j} \lambda_{ji}^{sd} = \begin{cases} \lambda^{sd}\,(1 - bl_{sd}) & m = s \\ -\lambda^{sd}(1 - bl_{sd}) & m = d \\ 0 & otherwise \end{cases} \tag{6-2}$$

$$\forall s, d, i \in N: s \neq d,$$

Constraint (6-2) is the flow conservation constraint in the IP layer. It ensures that the total outgoing traffic is equal to the total incoming traffic except for the source and destination nodes.

$$\sum_{s \in N} \sum_{d \in N\, s \neq d} \lambda_{ij}^{sd} \leq C_{ij} \tag{6-3}$$

$$\forall j, i \in N: i \neq j,$$

Constraint (6-3) is the virtual link capacity. It ensures that the summation of all traffic flows through a lightpath does not exceed the lightpath capacity.

$$\sum_{n \in N_m} W_{mn}^{ij} - \sum_{n \in N_m} W_{mn}^{ij} = \begin{cases} C_{ij} & m = i \\ -C_{ij} & m = j \\ 0 & otherwise \end{cases} \tag{6-4}$$

$$\forall i, j, m \in N: i \neq j,$$

Constraint (6-4) is the flow conservation constraint in the optical layer. It assumes that the total outgoing wavelengths in a virtual link should be equal the total incoming wavelengths except the source and the destination nodes of the virtual link.

$$\sum_{i \in N} \sum_{j \in N} W_{mn}^{ij} = W_{mn} \tag{6-5}$$

$$\forall m \in N, n \in N_m,$$

$$W_{mn} \leq W.F_{mn} \tag{6-6}$$

$$\forall m \in N, n \in N_m,$$

Constraint (6-5) finds the total wavelengths per link (m, n), while constraint (6-6) ensures that the total wavelengths per link does not exceed the fibre link capacity.

$$RE_i \leq R_i \tag{6-7}$$

$$\forall i \in N$$

$$BT_i TD \leq B_i \qquad (6\text{-}8)$$
$$\forall i \in N$$

Constraints (6-7) and (6-8) ensure that the power consumed per node does not exceed the available generated energy for renewable and battery sources. Constraints (6-7) ensures that at each time point the amount of power consumed from renewable sources does not exceed their produced power. In constraint (6-8) the formulation ensures that the power withdrawn from a battery for the duration of the time slot does not exceed the battery residual energy.

$$\sum_{s \in N} \sum_{\substack{j \in N \\ : j=i \vee s=i, \\ s \neq j}} \frac{1}{2} P_r\, C_{sj} + \sum_{m \in N} \sum_{\substack{n \in N_m \\ : m=i \vee n=i}} \frac{1}{2} P_t\, W_{mn} + \sum_{m \in N} \sum_{\substack{n \in N_m \\ : m=i \vee n=i}} \frac{1}{2} P_g\, RG_{mn} W_{mn}$$
$$+ \sum_{m \in N} \sum_{\substack{n \in N_m \\ : m=i \vee n=i}} \frac{1}{2} P_e\, F_{mn} A_{mn} + P_o = BT_i + BR_i + RE_i \qquad (6\text{-}9)$$
$$\forall i \in N$$

Constraint (6-9) makes sure that the power consumed in the node should equal the total power consumed by all energy sources.

6.4 Network Performance Evaluation

The model is evaluated using the Italian network topology shown in Figure 6-1 Italian Network which consists from 21 nodes and 35 bidirectional links and one DC located in Milan (node 19). Table 6-2 shows the simulation environment parameters in terms of number of wavelengths, wavelength capacity, distance between two neighbouring EDFAs, and energy consumption of different components in the network. The average traffic between a node pair varies throughout the day following the profile in Figure 6-2 with busy hour at 22:00. The traffic is generated using a gravity model based on the population of the city where the node is located

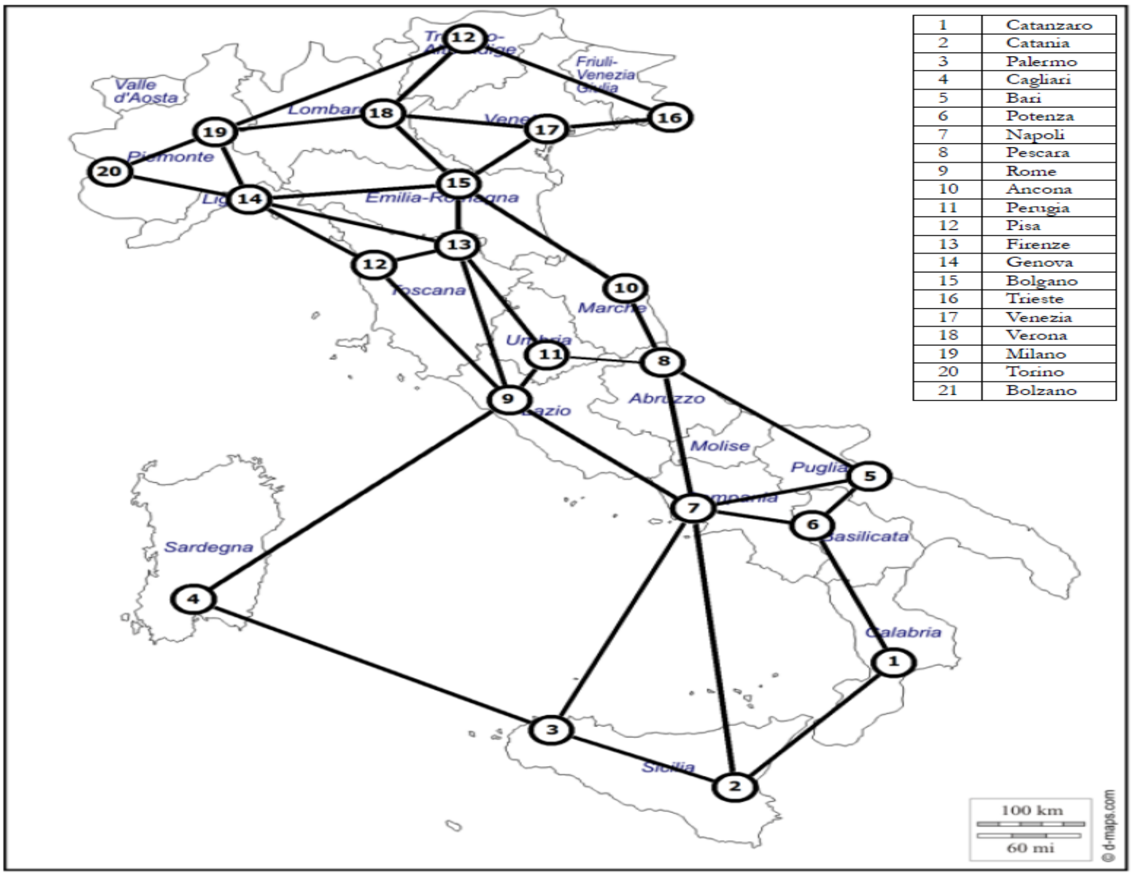


Figure 6-1 Italian Network

Solar energy is used as the renewable energy source. Each CO is equipped with 100 m^2 of solar panels, so the peak solar energy produced in a day equals is approximately 70 kW as shown in Figure 6-3 [113]. The sunrise and sunset and the perceived irradiance of April are considered where the sun light available for 12 hours [114].

Table 6-2 Input Data for the dimensioning MILP Model

Distance between two neighbouring EDFAs (*S*)	80 (km)
Number of wavelengths in a fibre (*W*)	32
Capacity of a wavelength (B)	40 (Gb/s)
Power consumption of a router port (P_r)	825 (W)
Power consumption of a transponder (P_t)	167 (W)
Power consumption of a regenerator (P_g)	334 (W)
Power consumption of an EDFA (P_e)	55 (W)
Power consumption of an optical switch (P_o)	85 (W)

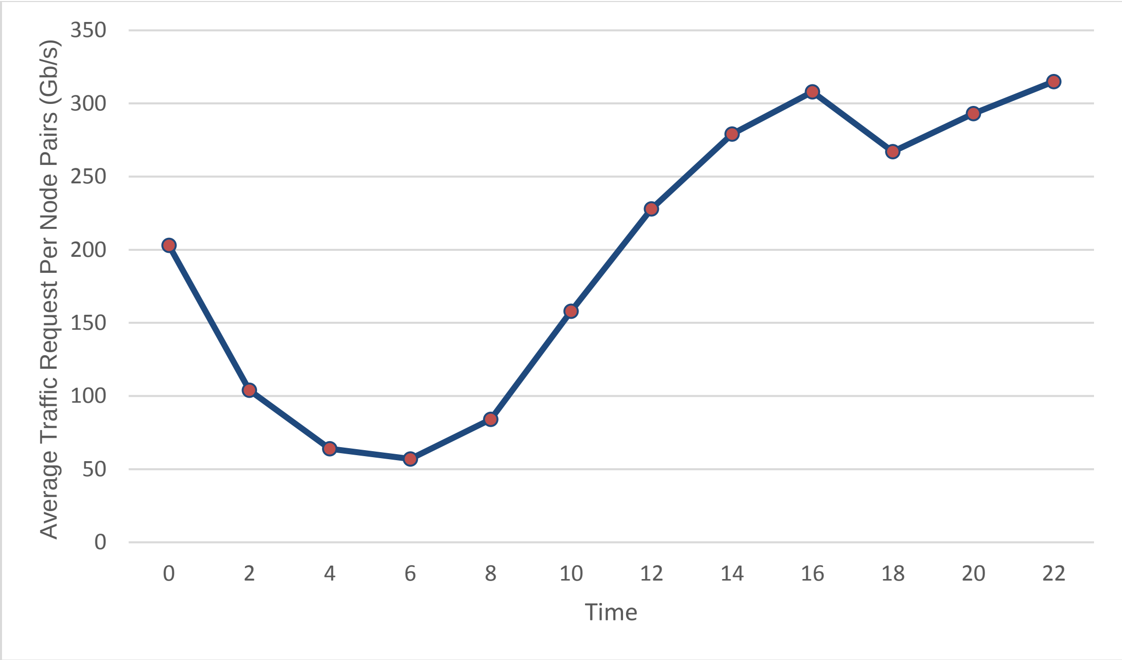


Figure 6-2 Average traffic request

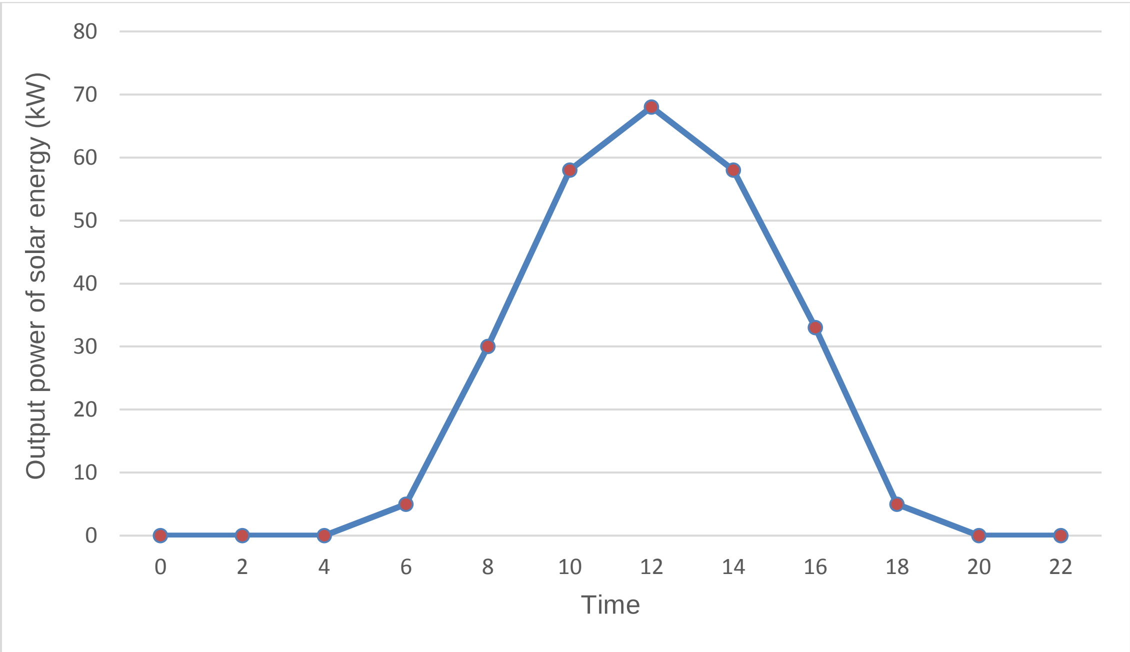


Figure 6-3 Solar cells output power at each node

Two optimisation approaches were considered using the developed MILP model with varying objective function coefficients to study the trade-off between blocking and energy preservation.

1- Blocking minimisation scenario: the power consumption coefficients $\alpha, \beta \; and \; \gamma$ were set to 1 while δ was given a very high number (1,000,000 here), as the main objective is to minimise the total network blocking while minimising the consumed power in total.

2- Weighted Energy Sources Optimisation (WESO) scenario: In this scenario the weights are set in a way that ensures that the use of grid power is prioritised over the battery and renewable power to preserve the battery energy and the renewable energy of the blackout node. Therefore, this objectives attempts to ensure that during a blackout the transit traffic should be routed away from the blackout node to other nodes where grid power is available. Also the use of renewable energy in the blackout node is given priority over the power drawn from the battery as long as renewable energy is available to preserve the battery energy to the times when there is no sunlight. Table 6-3 shows the three different combinations of weighing coefficients.

Table 6-3 Weighing Coefficients

	$\boldsymbol{\alpha}$	$\boldsymbol{\beta}$	$\boldsymbol{\gamma}$
WESO 1	10	1	100
WESO 2	8	6	20
WESO 3	15	5	25

The blackout is considered to happen at the beginning of the day (00:00) and last 24 hours. The model was run for a whole day in a two hour basis in a sequential manner. By assuming that the network receives the requests each two hours and route them, at the end of the two hours the residual battery energy is passed over to the next time point and so on till the end of the day.

The four proposed scenarios (blocking minimisation and three weighted energy optimisation) are evaluated for a day long blackout at node 14. The node is assumed to have 360 kWh batteries, (a small saloon, 12 V, car battery is typically rated at 40 ampere hours, which translates to 0.48 kWh. The Tesla electric vehicle battery is 60 kWh to 85 kWh according to model [115]). Figure 6-4 Figure 6-7 show the power consumed for each power source throughout the day and the battery residual energy for node 14.

In Figure 6-4, the blocking minimisation approach results are shown. In this scenario, the node used the battery energy during the midnight hours till 4:00 am, because the traffic is relatively high. Then from 04:00 to 06:00, the node turned off as no energy source is available yet. At 06:00 the sun rises and the node operation is resumed until the sunset at 18:00 where the node shut down again until the end of the day. During the renewable power availability, the node fully utilised the renewable energy generated to serve the node traffic and the transit traffic.

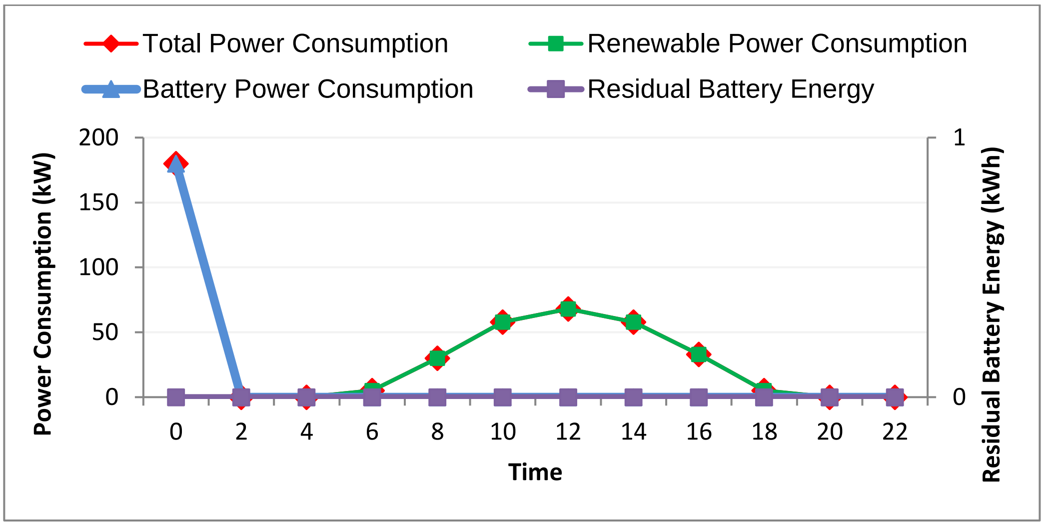


Figure 6-4 Node 14 power consumption and battery residual energy under blocking minimisation scenario

The WESO 1 scenario results are shown in Figure 6-5. The node used minimal energy from the battery energy, because the node handled its own traffic only (originating and destined traffic) while the transit traffic is rerouted. This can be seen as the maximum consumed power in the node is 14 kW. During the sunlight hours, the node used renewable energy, while after the sunset, the batteries were used.

The WESO 2 scenario results are shown in Figure 6-6. The results show that the switching between the batteries and renewable energy is the same as the WESO 1 scenario. During the sunlight hours, however, the node fully used the available renewable energy to route both the destined/originating traffic and transit traffic as the weight given to renewable energy did not stop routing the transit traffic.

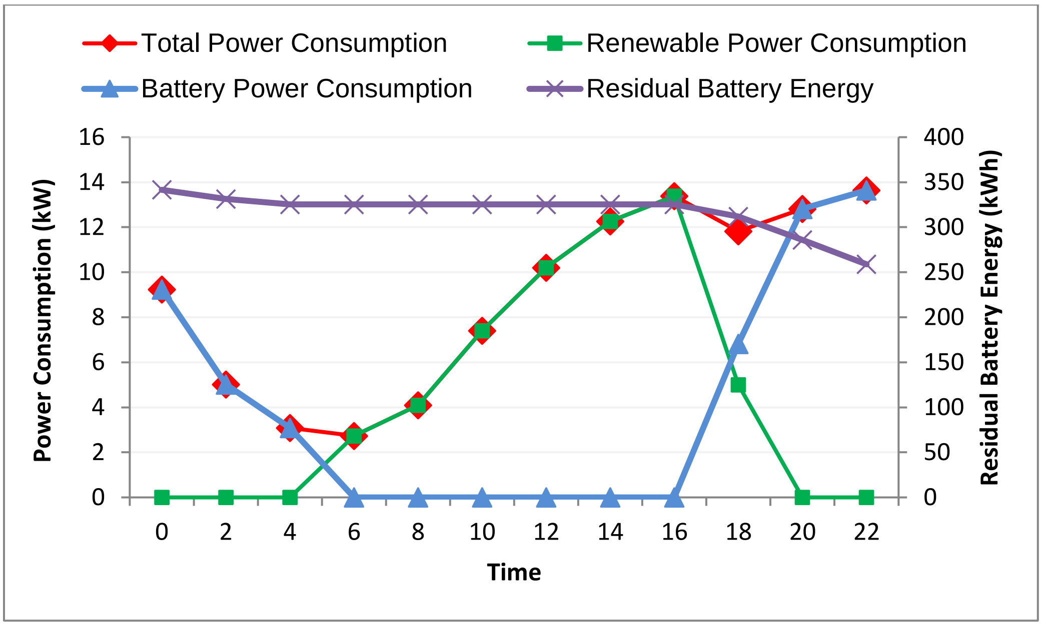


Figure 6-5 Node 14 power consumption and battery residual energy under WESO 1

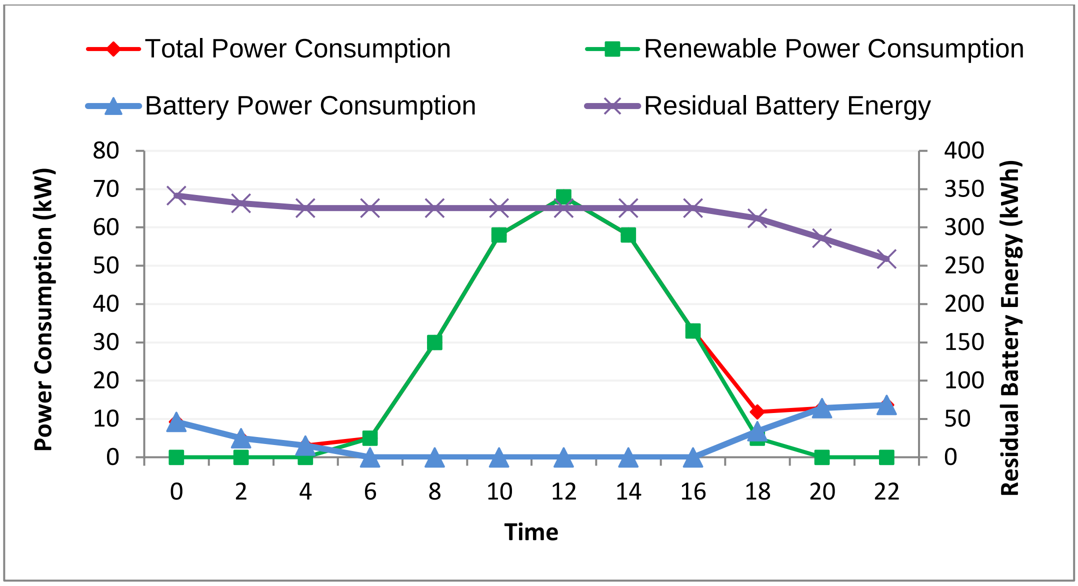


Figure 6-6 Node 14 power consumption and battery residual energy under WESO 2

The WESO 3 scenario results are shown in Figure 6-7. This scenario behaves similar to WESO 1 and 2 in switching between the batteries and renewable. The only difference is that in WESO 3, the difference in weights between renewable and battery is larger. Therefore less transit traffic is routed through the blackout node resulting in lower blackout node power consumption. This can be verified by checking the total consumed power in the node. In WESO 1, the node consumed 14 kW maximum, while in WESO 2 it consumed 70 kW and in WESO 3 it consumed 28 kW. In conclusion, the three scenarios avoided using the battery energy in two cases. The first when the renewable is sufficient for routing the node traffic and the other situation where the battery power was not used is the situation where the node would have had to route transit traffic under normal conditions when the renewable energy is unavailable. The differences are during the availability of the renewable energy.

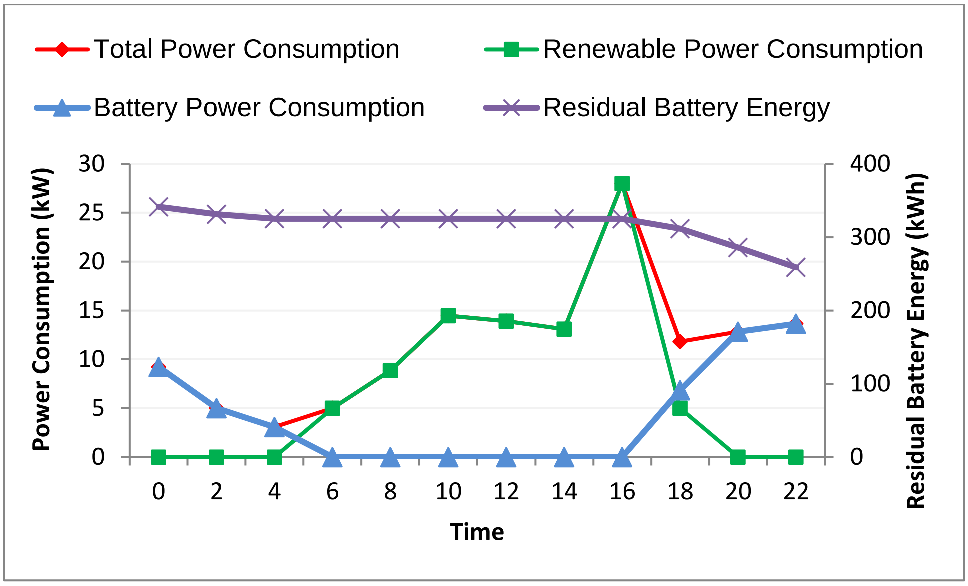


Figure 6-7 Node 14 power consumption and battery residual energy under WESO 3

The WESO 1 scenario is studied throughout this section, because it avoided the blackout node during the 24 hour blackout.

To maximise the impact of the blackout, the nodes with the most transit traffic are considered to suffer a blackout. To evaluate the most critical nodes, the MILP model is used assuming that there is no blackout in any node. Figure 6-8 shows the amount of traffic (transit, originating and destined) carried by each node throughout the day. The figure shows that nodes 7, 9, 12, 13, 14 and 19 are carrying very high traffic as compared with the other nodes. So, these nodes are assumed to have a blackout and would be evaluated.

The two scenarios are evaluated for each node to identify the blocking incurred and how much battery power is required. To compare the blocking, the same battery is considered for the two scenarios. A high power battery is assumed which is enough to run the node till the end of the day.

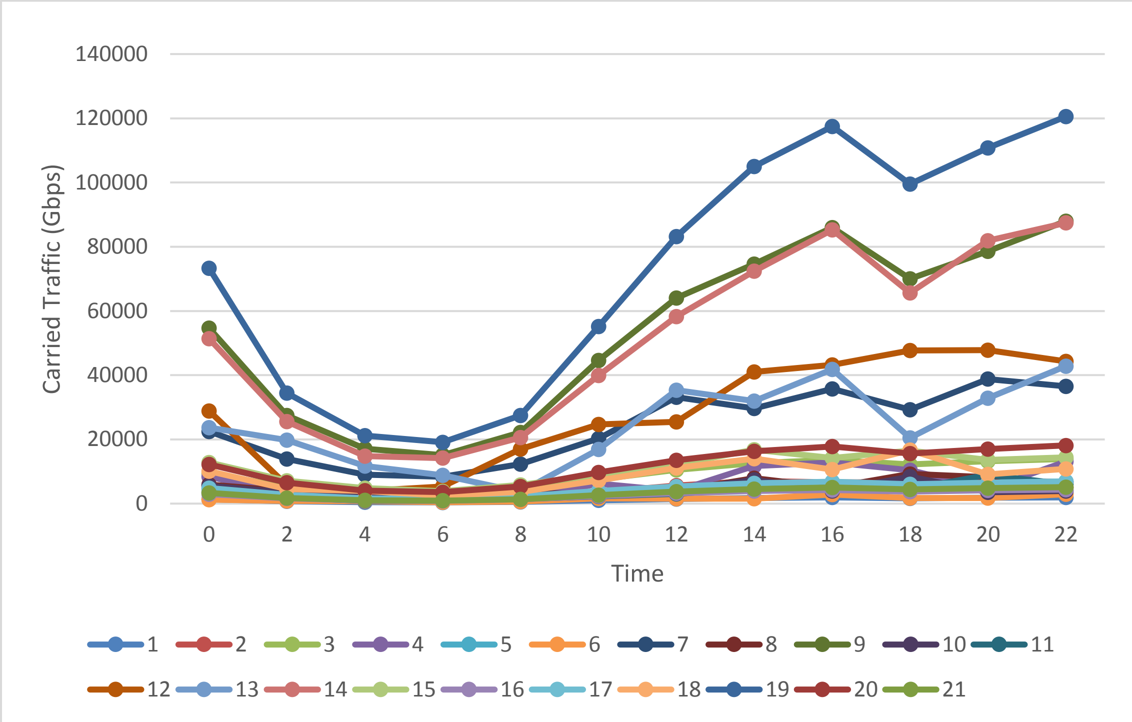
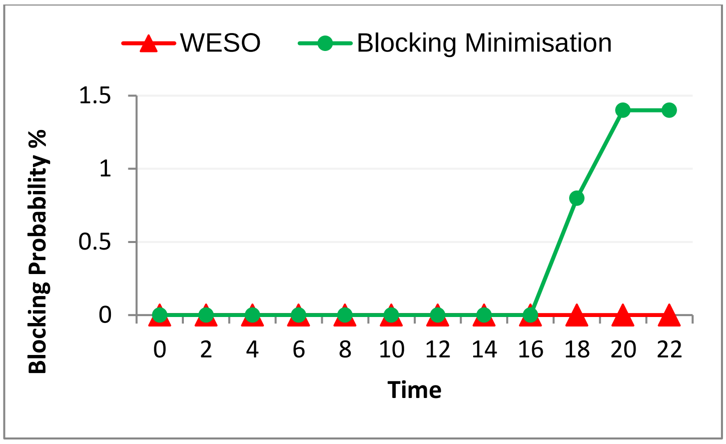


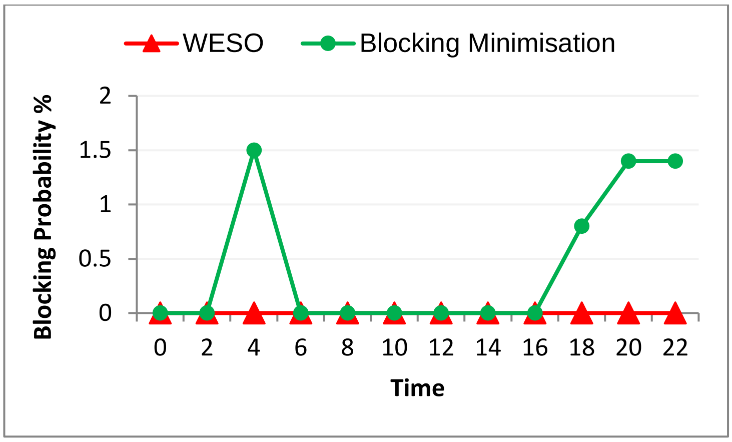
Figure 6-8 Node carried traffic through the day

Generally, the nodes can be classified into high traffic nodes and low traffic nodes. The high traffic comes from either a high population in the city, from a DC or from transit traffic passing by the node. According to this classification, nodes 7 and 9 which are in Rome and Napoli have large population, while node 19 is in Milan has a large population and there is a DC collocated as well. Nodes 12, 13 and 14 lie in the path leading to the DC. The suggested approaches mainly deal with traffic distribution in the network.

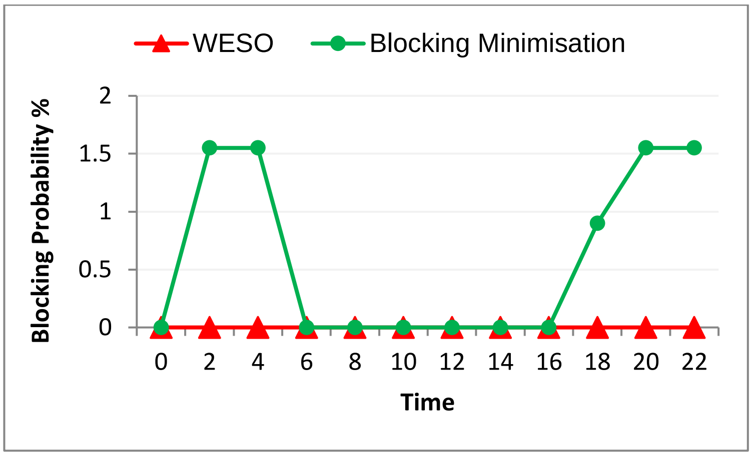
First nodes 12, 13 and 14 are evaluated for both scenarios considering each node to be equipped with a battery of 360 kWh. This is the battery capacity needed to reduce the blocking probability to be zero (i.e. a battery is enough to last the node for 24 hours for the traffic it generates and sinks). Figure 6-9 shows the blocking probability of these nodes. Clearly, the WESO scenario outperforms the blocking minimisation approach as it managed to run the node for a whole day while under the blocking minimisation scenario blocking occurred due to the blackout nodes not being able to send/forward traffic after running out of battery when sunlight is unavailable. The blocking minimisation scenario used the battery to run the node for the first hours of the day after which the available renewable energy was enough to serve all the demands, then blocking starts when no renewable energy is available. Nodes 13 and 14 start blocking from early hours because all the battery energy is used for carrying the transit traffic in the four early hours of the day. The nodes' total blocking probability throughout the day as seen in the figure show that node 14 is the worst, then node 13 follows and the least blocking is in node 12. This variation is due to the node running out of battery energy before sunrise. In this sense, node 14 drained the battery energy by 02:00 hour, while node 13 exploited the battery energy from 00:00 to 04:00, node 12 used the battery energy until sunrise. The amount of energy used depends to a large extent, in many cases on the node transit traffic.



(a) Node 12



(b) Node 13



(c) Node 14

Figure 6-9 The blocking probability for nodes a) 12 b) 13 c) 14

Figure 6-10 shows the total number of hops in three scenarios: WESO scenario, blocking minimisation and WESO with no blackout. The no blackout scenario has the lowest number of hops to keep the energy minimised. The WESO scenario rerouted the traffic paths away from the blackout node and this can be seen in the figure as the number of hops stays constant above that of the no blackout scenario. The blocking minimisation approach routed based on the minimum-hop paths (because the objective includes minimise total power consumption, and minimum hop (not shortest path) minimises power consumption) during the first two hours of the day till the battery power was exhausted. When the node shut down (02:00 and 04:00), the number of hops decreased due to blocked requests. To minimise the blocking at 06:00, the blackout node was avoided, so the number of hops increased till 20:00 where the renewable power became insufficient to serve the traffic. After sunset, the node has no power to keep it working, so it shut down, and the number of hops decreased.

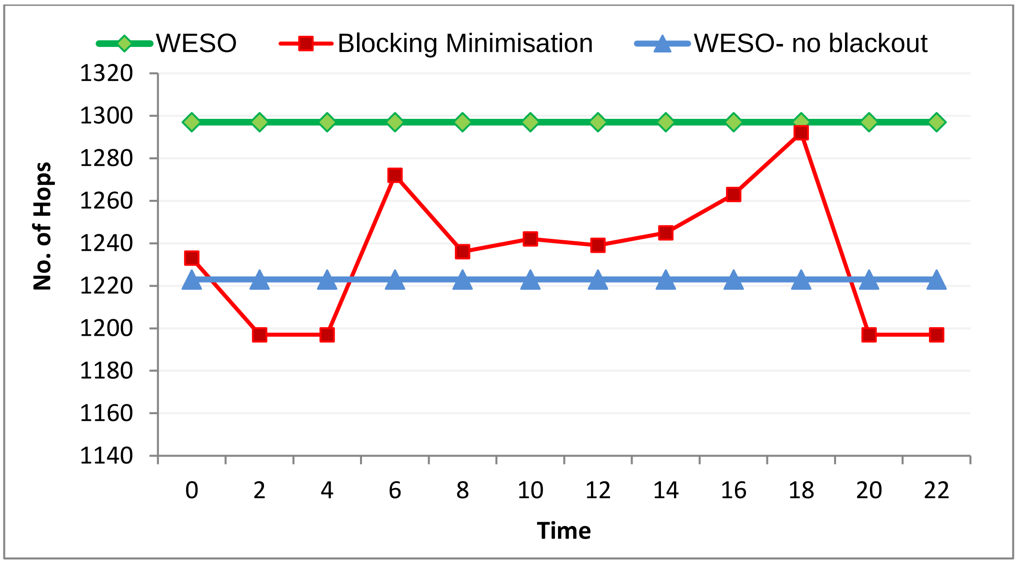
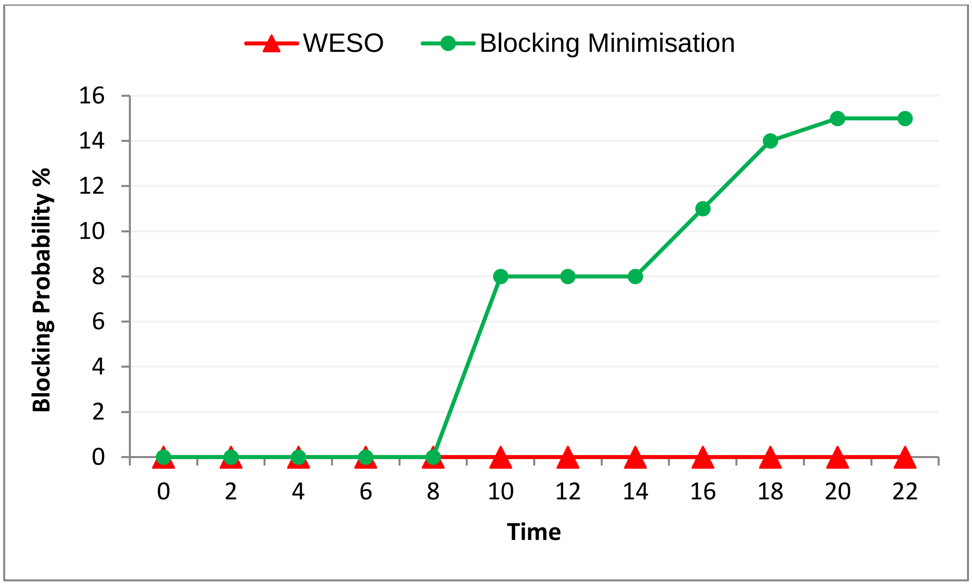
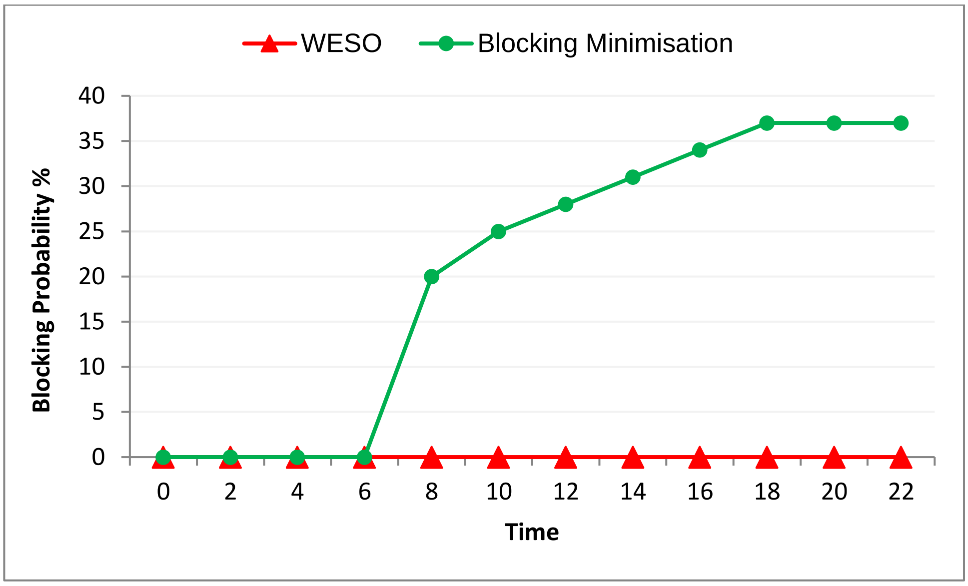


Figure 6-10 Number of hops

Due to their high originating and destined traffic nodes 7 and 9 are considered to be equipped with batteries of 720 kWh and 1500 kWh, respectively. Figure 6-11 shows the blocking probability for nodes 7 and 9 when a blackout takes place for 24 hours. The WESO scenario has succeeded in keeping the node running for the 24 hours, while the node goes completely out of service during the last four hours of the day in the blocking minimisation approach. Under 24 hours blackout at nodes 7 and 9 the blocking minimisation approach started blocking earlier than the scenarios with blackouts at nodes 12,13 and 14 because the available renewable energy during the sunlight hours is not enough to serve all the traffic.



(a) Node 7



(b) Node 9

Figure 6-11 The blocking probability for nodes a) 7 b) 9

Nodes 7 and 9 have high amount traffic requests but also they carry the transit traffic between the datacenter (in the north) and the south edge nodes. So the WESO scenario can perform better by rerouting the transit traffic away from them. For datacenter node 19 which lies in the far edge of the network and has originating and destined traffic, the WESO scenario cannot solve the problem.

6.5 Summary

Blackouts are another source of disruption in the network operations during disasters unless there is a backup power source. In this chapter, building a blackout resilient network has been investigated in the optical core network. The problem is an issue that can be tackled on different levels. Two scenarios have been considered one with the objective of minimising blocking and the other has the aim of optimising power sources usage where the blackout nodes is considered to have access to solar energy and batteries. A weighted energy optimisation scenario was introduced. This attempts to maximise the blackout survival time while minimising the blocking. A MILP model was developed for optimising the IP over WDM network under the two scenarios. An example network was used to evaluate the model with realistic traffic demands. The results show that the WESO scenario succeeded in extending the network life time with the smallest battery resource compared with the blocking minimisation approach.

7 Conclusions and future directions

This chapter summarises the main contributions for the work described in this thesis. Furthermore, it states the main conclusions and highlights directions for future research.

7.1 Conclusions

The thesis discusses the design of disaster resilient optical network. It considers two issues which are the short-term capacity exhaustion due to post-disaster traffic floods and power outage.

Starting with post-disaster traffic floods, the first contribution in the thesis was to propose five mitigation approaches to maximally serve these floods using the operators' existing technologies. The mitigation approaches explored different strategies, starting from exploiting links capacities, to traffic filtration, and protection paths rerouting or rerouting working and protection paths and finally differentiated services. Excluding the exploitation of excess overprovisioned capacity (which is straightforward), the approaches introduced have advantages and limitations but have achieved a reduction in traffic blocking probability when disasters occur. The results showed that the rerouting with differentiated services approach succeeded in reducing the blocking for DC nodes by 50% compared with the "exploiting excess capacity" approach. For non-DC nodes the blocking was reduced to zero and this achievement came at the expense of disrupting the active traffic until all flows are rerouted. This also left less critical traffic without protection.

The second contribution in this thesis is the development of a framework to provision advance reservation requests in an energy-efficient manner in optical networks. The problem of scheduling and routing advance reservation requests was investigated in different scenarios to exploit the flexibility provided by the sliding-window demands. Three scenarios were proposed for scheduling and rescheduling. Different evaluation schemes were presented for different traffic volumes and sliding-window sizes. The results showed that scheduling advance reservation requests at their arrival time reduces the power consumption by 3% compared to no scheduling, while adding the flexibility of rescheduling and rerouting of the reserved traffic requests yet to start saves up to 5% of the network power consumption. In addition, the results showed that disrupting the active traffic requests and rerouting them increased the power savings to 10%. This improvement because of its dynamic nature to adapt to network utilisation changes, however it came at the cost of a slight increase in the delay experienced by users of the interrupted requests till reprovisioing the paths for the interrupted requests. Furthermore, larger sliding-window sizes were considered with 12-hours and 24-hour holding-time, and, therefore, power savings of 7% and 8.5% can be achieved respectively.

The third contribution is the use of the developed scheduling scenarios to mitigate post-disaster traffic floods and minimise network blocking. The results show that rescheduling and rerouting AR requests that have not started yet can reduce the blocking by 4%, while disrupting the network traffic and rerouting the active requests and rescheduling the AR requests can eliminate the blocking. Although rescheduling the reserved AR requests can reduce the blocking for larger networks, it fails to cope with a flooding scenario that starts in a highly utilised network. On the other hand, rerouting and rescheduling all the requests can successfully absorb the floods, but at the expense of disrupting the network active traffic till rerouting them.

Finally, the last contribution in the thesis was the investigation of the blackout issue and its impact on the network performance. Two scenarios were considered, one with the objective of minimising blocking and the other with the objective of optimising the energy source usage. The weighted energy source optimisation approach attempted to extend the node lifetime during blackouts by rerouting the traffic and avoiding traffic routing through blackout nodes. This objective succeeded in reducing the energy required to power the blackout node. The Italian network was evaluated with a blackout that lasted for 24 hours at a single node. Three energy sources were assumed to be available in each node which are grid power, renewable energy and batteries, while the blackout node has access only to the last two. The weighted energy source optimisation scenario succeeded in keeping the node working for 24 hour with minimal battery energy, while the blocking minimisation scenario failed to keep the node working; and to keep it working it requires a large amount of backup energy sources that cannot be practically stored in a core node.

In a final conclusion, the suggested approaches have a variant results from worst to best. Although, the best approaches satisfied the objective but this always comes at a cost or a sacrifice. For example, to reduce blocking or power consumption, always online routing (or optical rerouting) achieved the best results. While, the fixed routing always fails to adapt the network changes and got higher blocking and power consumption. The cost of rerouting is to disrupt the network traffic till reroute the paths and reconfigure the lightpaths. That means using an online routing technology (or programmable networks) is always a solution such as the SDN.

7.2 Future work

The thesis has tackled two disaster related consequences which are the post-disaster traffic floods and the blackout. More challenges exist and need to be addressed, and below is a list of potential future directions.

7.2.1 Blackout Resilient Network

The work in chapter 6 have considered mathematical modelling for designing a blackout resilient network, and considered a single node blackout with an objective of optimising the power usage optimisation. The work can be extended by building a real time heuristic to overcome MILP limitations. Also, other objectives can be considered such as promoting the use of renewable energy and minimise delay. Considering a blackout for a region that has more than one node lies within.

In addition to network engineering approach, the traffic engineering approach can be explored by optimise the traffic routing within a capacitated network using programmable networks in collaboration with disaster warning system. That means whenever a warning issued for a blackout, the network should reroute and reprovision the lightpaths by avoiding the limited power nodes. In this approach, a spare capacity should exist on alternative paths that is similar to protection paths to avoid blocking due to capacity exhaustion.

7.2.2 Blackout-Floods Resilient Network

An early warning system is widely deployed for issuing disaster warning at the early stages. This warning system can be adapted and used within the core network to predict the disaster influences on network using a signalling system that stimulate changing the routing decisions based on the network topological and behavioural changes. These changes can include network topology modifications due to losing links or nodes, traffic increase and power outages. An online integrated approach could be used to improve the network resilience during disasters. By making use of the proposed scenarios such as the FRDS, FTRR and energy optimisation approaches. For each possible scenario there should be an appropriate routing strategy that mitigate the disaster impact and maximise the network QoS.

For example, when there is links cut and power outage due to an earthquake in a city, the warning system should send a blackout warning. Based on this warning, the routing algorithm should change the paths for the transit traffic that pass through the blackout node and reroute the traffic that use the failed link on the protection path. These different topological and behavioural changes require a seamless and fast action that can react to these changes.

7.2.3 Multi-Vendor and Multi-Domain Interoperability

Different ISPs own the backbone optical networks which span large areas, and each ISP may use different vendors/technologies. For fast recovery, collaboration between the ISPs by interconnecting their networks through backup links could be a mitigation strategy. This interconnection requires two aspects to be considered which are the multi-vendor interoperability and multi-domain interoperability.

Usually more than one core node is collocated at the same city but owned by different ISPs. In a disaster situation, one of the ISP's nodes may fail while the other's node is not affected, in such a case the interconnection between the two ISPs will survive the disconnected part of one of ISPs networks.

The other problem is the integration between multi-vendor networks to connect the survived parts of the networks in metropolitan areas. The standards bodies dealing with optical networks (ITU-T, OIF and IETF) already have frameworks for connecting the data and control planes of different vendors. However, building an integrated optical network using optical-electrical and all-optical technologies is essential in recovering the service. The integration should address the concept of bypassing the lightpath through different networks. The other aspect is building a network management system (NMS) system to manage the operation during disasters.

7.2.4 Recovery Process

After a disaster, the traffic requests are expected to rise and become difficult to satisfy, as there is a partial damage in the network. Therefore, the recovery plan should take in consideration how to gradually and optimally add repaired resources (or limited recovery resources) to the network to accommodate maximum traffic requests and reduce the congestion.

In large size disasters that destruct the infrastructure in a big area, and the online routing approaches fail to react to topological modifications. Then a repair plan should be set up in a way that maximise network availability. For example, when a large earthquake hits a region and leave the two ends of the network disconnected. The recovery plan should restore the connectivity by repairing the highest traffic path first and the lowest at the end.

7.2.5 Wireless Backup Links

Optical networks are considered more resilient to disasters compared to wireless networks, as long as the disaster impact is overground and the central office is not affected by the disaster. But if the disaster is an earthquake which is underground and it affected the fibre infrastructure it would be very difficult to rapidly recover. So the recovery time for the wireless networks can be faster than optical networks in earthquake disasters. However, the outage of the optical backbone is considered a disaster by itself due to the high bandwidth it provides.

For fast connectivity restoration of the optical backbone, wireless technologies can be used. Deploying wireless system is fast enough to tackle the disaster consequences. There are two wireless techniques that can be used point-to-point (PTP) wireless links or satellite systems (Via-SAT). Satellite systems have less bandwidth, fast installation, and are distance independent, while the PTP has a higher bandwidth, slow installation and depends on the distance between nodes. Multiple satellite systems can be deployed to support core network traffic although it has high latency as compared with PTP but still the fast deployment makes it a valid short term solution. Also, Via-SAT system can be used to migrate an isolated datacentre content into another one. The PTP links require line of sight, therefore in long links more than one PTP link could be needed to restore a failed link.

References

[1] J. Rak, D. Hutchison, E. Calle, T. Gomes, M. Gunkel, P. Smith, J. Tapolcai, S. Verbrugge, and L. Wosinska, "RECODIS: Resilient Communication Services Protecting End-user Applications from Disaster-based Failures," in 2016 18th International Conference on Transparent Optical Networks (ICTON), 2016, pp. 1–4.

[2] J. P. G. Sterbenz, D. Hutchison, E. K. Çetinkaya, A. Jabbar, J. P. Rohrer, M. Schöller, and P. Smith, "Resilience and survivability in communication networks : Strategies , principles , and survey of disciplines," Computer Networks, vol. 54, no. 8, pp. 1245–1265, 2010.

[3] M. F. Habib, M. Tornatore, F. Dikbiyik, and B. Mukherjee, "Disaster survivability in optical communication networks," Computer Communications, vol. 36, no. 6, pp. 630–644, Mar. 2013.

[4] N. Ghani, S. Dixit, and T.-S. Wang, "On IP-WDM integration: a retrospective," IEEE Communications Magazine, vol. 41, no. 9, pp. 42–45, 2003.

[5] K. Rajagopalan, Bala and Pendarakis, Dimitrios and Saha, Debanjan and Ramamoorthy, Ramu S and Bala, "IP over optical networks: Architectural aspects," IEEE Communications Magazine, pp. 94–102, 2000.

[6] J. Zheng and H. T. Mouftah, Optical WDM networks: concepts and design principles. John Wiley & Sons, 2004.

[7] B. Mukherjee, Optical WDM networks. Springer Science & Business Media, 2006.

[8] I. Chlamtac, A. Ganz, and G. Karmi, "Lightpath communications: An approach to high bandwidth optical WAN's," IEEE transactions on communications, vol. 40, no. 7, pp. 1171–1182, 1992.

[9] D. Banerjee and B. Mukherjee, "A practical approach for routing and wavelength assignment in large wavelength-routed optical networks," IEEE Journal on selected areas in communications, vol. 14, no. 5, pp. 903–908, 1996.

[10] H. U. I. Zang, "A Review of Routing and Wavelength Assignment Approaches for Wavelength- Routed Optical WDM Networks," Optical Networks Magazine, vol. 1, no. January, pp. 47–60, 2000.

[11] A. Mokhtar and M. Azizo\uglu, "Adaptive wavelength routing in all-optical networks," IEEE/ACM Transactions on Networking (TON), vol. 6, no. 2, pp. 197–206, 1998.

[12] A. Wason and R. S. Kaler, "Optical Fiber Technology Rerouting technique with dynamic traffic in WDM optical networks," Optical Fiber Technology, vol. 16, no. 1, pp. 50–54, 2010.

[13] T. Stidsen and P. Kjærulff, "Complete rerouting protection," Journal of Optical Networking, vol. 5, no. 6, pp. 481–492, 2006.

[14] K.-C. Lee and V. O. K. Li, “A wavelength rerouting algorithm in wide-area all-optical networks,” Journal of lightwave technology, vol. 14, no. 6, pp. 1218–1229, 1996.

[15] P. Saengudomlert, E. Modiano, and R. G. Gallager, “On-line routing and wavelength assignment for dynamic traffic in WDM ring and torus networks,” IEEE/ACM Transactions on Networking (TON), vol. 14, no. 2, pp. 330–340, 2006.

[16] A. Narula-Tam, P. J. Lin, and E. Modiano, “Efficient routing and wavelength assignment for reconfigurable WDM networks,” IEEE Journal on Selected Areas in Communications, vol. 20, no. 1, pp. 75–88, 2002.

[17] L.-W. Chen and E. Modiano, “Efficient routing and wavelength assignment for reconfigurable WDM ring networks with wavelength converters,” IEEE/ACM Transactions on Networking (TON), vol. 13, no. 1, pp. 173–186, 2005.

[18] P. Saengudomlert, E. H. Modiano, and R. G. Gallager, “Dynamic wavelength assignment for WDM all-optical tree networks,” IEEE/ACM Transactions on Networking, vol. 13, no. 4, pp. 895–905, 2005.

[19] G. Mohan and C. S. R. Murthy, “A time optimal wavelength rerouting algorithm for dynamic traffic in WDM networks,” Journal of lightwave technology, vol. 17, no. 3, p. 406, 1999.

[20] A. Caprara, G. F. Italiano, G. Mohan, A. Panconesi, and A. Srinivasan, “Wavelength rerouting in optical networks, or the Venetian routing problem,” Journal of Algorithms, vol. 45, no. 2, pp. 93–125, 2002.

[21] K.-C. Lee and V. O. K. Li, “A circuit rerouting algorithm for all-optical wide-area networks,” in INFOCOM’94. Networking for Global Communications., 13th Proceedings IEEE, 1994, pp. 954–961.

[22] M. Koubàa and M. Gagnaire, “Lightpath rerouting strategies in WDM all-optical networks under scheduled and random traffic,” Journal of Optical Communications and Networking, vol. 2, no. 10, pp. 859–871, 2010.

[23] N. Amdouni, M. Koubàa, and T. Aguili, “Lightpath rerouting scheme for dynamic traffic in WDM all-optical networks,” in 2012 International Conference on Computer Systems and Industrial Informatics, 2012, pp. 1–6.

[24] X. Chu and J. Liu, “DLCR: A new adaptive routing scheme in WDM mesh networks,” in Communications, 2005. ICC 2005. 2005 IEEE International Conference on, 2005, vol. 3, pp. 1797–1801.

[25] N. Amdouni, M. Koubaa, and T. Aguili, “A new intentional lightpath rerouting scheme for dynamic traffic in WDM all-optical networks,” in Telecommunications (ICT), 2013 20th International Conference on, 2013, pp. 1–5.

[26] N. Amdouni, M. Koubàa, and T. Aguili, “A new hybrid rerouting scheme in WDM all-optical networks under dynamic traffic,” in Computer & Information Technology (GSCIT), 2014 Global Summit on, 2014, pp. 1–7.

[27] P. Chołda, E. L. Følstad, B. E. Helvik, P. Kuusela, M. Naldi, and I. Norros, “Towards risk-aware communications networking,” Reliability Engineering & System Safety, vol. 109, pp. 160–174, Jan. 2013.

[28] F. Dikbiyik, M. Tornatore, and B. Mukherjee, “Minimizing the Risk From Disaster Failures in Optical Backbone Networks,” vol. 32, no. 18, pp. 3175–3183, 2014.

[29] S. Kaplanl, “The Words of Risk Analysis,” Risk Analysis, vol. 17, no. 4, p. 407, 1997.

[30] D. Duffie and S. Schaefer, Quantitative Risk Management. .

[31] N. Sahebjamnia, S. A. Torabi, and S. A. Mansouri, “Integrated business continuity and disaster recovery planning : Towards organizational resilience,” European Journal of Operational Research, vol. 242, no. 1, pp. 261–273, 2015.

[32] J. C. Oberg, V. Wireless, A. G. Whitt, R. M. Mills, and V. Vso, “Disasters Will Happen — Are You Ready ?,” IEEE Communications Magazine, vol. 49, no. 1, pp. 36–42, 2011.

[33] P. Cholda, T. Cinkler, K. Wajda, and A. Jajszczyk, “Quality of Resilience as a Network Reliability Characterization Tool,” IEEE Network, no. April, pp. 11–19, 2009.

[34] O. Diaz, F. Xu, N. Min-Allah, M. Khodeir, M. Peng, S. Khan, and N. Ghani, “Network Survivability for Multiple Probabilistic Failures,” IEEE Communications Letters, vol. 16, no. 8, pp. 1320–1323, Aug. 2012.

[35] J. Cao, L. Guo, H. Yu, and L. Li, “Partial SRLG-disjoint shared path protection with differentiated reliability in survivable WDM network,” AEU-International Journal of Electronics and Communications, vol. 61, no. 6, pp. 353–362, 2007.

[36] J. Cao, L. Guo, H. Yu, and L. Li, “Partial SRLG-disjoint shared path protection with differentiated reliability in survivable WDM network,” AEU - International Journal of Electronics and Communications, vol. 61, no. 6, pp. 353–362, Jun. 2007.

[37] H. Lee, E. Modiano, and K. Lee, “Diverse Routing in Networks With Probabilistic Failures,” IEEE/ACM TRANSACTIONS ON NETWORKING, vol. 18, no. 6, pp. 1895–1907, 2010.

[38] P. N. Tran and H. Saito, “Geographical route design of physical networks using earthquake risk information,” IEEE Communications Magazine, vol. 54, no. 7, pp. 131–137, 2016.

[39] X. Dong, T. El-Gorashi, and J. M. H. Elmirghani, “Green IP Over WDM Networks With Data Centers,” Journal of Lightwave Technology, vol. 29, no. 12, pp. 1861–1880, Jun. 2011.

[40] M. F. Habib, M. Tornatore, M. De Leenheer, F. Dikbiyik, and B. Mukherjee, “Design of Disaster-Resilient Optical Datacenter Networks,” Journal of Lightwave Technology, vol. 30, no. 16, pp. 2563–2573, Aug. 2012.

[41] Y. Wu, M. Tornatore, C. U. Martel, and B. Mukherjee, “Green and Low-Risk Content Placement in optical content delivery networks,” in 2016 IEEE International Conference on Communications (ICC), 2016, pp. 1–6.

[42] S. Ferdousi, F. Dikbiyik, M. F. Habib, and B. Mukherjee, “Disaster-Aware Data-Center and Content Placement in Cloud Networks,” pp. 3–5.

[43] A. Bianco, J. Finochietto, L. Giraudo, M. Modesti, and F. Neri, "Network planning for disaster recovery," 2008 16th IEEE Workshop on Local and Metropolitan Area Networks, pp. 43–48, Sep. 2008.

[44] U. Mandal, M. Habib, S. Zhang, B. Mukherjee, and M. Tornatore, "Greening the cloud using renewable-energy-aware service migration," IEEE network, vol. 27, no. 6, pp. 36–43, 2013.

[45] U. Mandal, M. F. Habib, S. Zhang, M. Tornatore, and B. Mukherjee, "Bandwidth and routing assignment for virtual machine migration in photonic cloud networks," in Optical Communication (ECOC 2013), 39th European Conference and Exhibition on, 2013, pp. 1–3.

[46] C. C. Meixner, F. Dikbiyik, M. Tornatore, C. Chuah, and B. Mukherjee, "Disaster-Resilient Virtual-Network Mapping and Adaptation in Optical Networks," pp. 107–112, 2013.

[47] H. Yu, C. Qiao, V. Anand, X. Liu, H. Di, and G. Sun, "Survivable Virtual Infrastructure Mapping in a Federated Computing and Networking System under Single Regional Failures," 2010 IEEE Global Telecommunications Conference GLOBECOM 2010, pp. 1–6, Dec. 2010.

[48] A. Fumagalli and L. Valcarenghi, "IP restoration vs. WDM protection: Is there an optimal choice?," IEEE network, vol. 14, no. 6, pp. 34–41, 2000.

[49] J. Zhang, K. Zhu, and B. Mukherjee, "Backup reprovisioning to remedy the effect of multiple link failures in WDM mesh networks," IEEE Journal on Selected Areas in Communications, vol. 24, no. 8, pp. 57–67, 2006.

[50] C. Assi and W. Huo, "On the benefits of lightpath re-provisioning in optical mesh networks," in Communications, 2005. ICC 2005. 2005 IEEE International Conference on, 2005, vol. 3, pp. 1746–1750.

[51] B. A. A. Nunes, M. Mendonca, X.-N. Nguyen, K. Obraczka, and T. Turletti, "A survey of software-defined networking: Past, present, and future of programmable networks," IEEE Communications Surveys & Tutorials, vol. 16, no. 3, pp. 1617–1634, 2014.

[52] N. Feamster, J. Rexford, and E. Zegura, "The road to SDN: an intellectual history of programmable networks," ACM SIGCOMM Computer Communication Review, vol. 44, no. 2, pp. 87–98, 2014.

[53] S. S. Savas, M. Tornatore, M. F. Habib, P. Chowdhury, and B. Mukherjee, "Disaster-resilient control plane design and mapping in software-defined networks," in 2015 IEEE 16th International Conference on High Performance Switching and Routing (HPSR), 2015, pp. 1–6.

[54] Nguyen, Kien, Quang Tran Minh, and Shigeki Yamada. "A software-defined networking approach for disaster-resilient WANs." In Computer Communications and Networks (ICCCN), 2013 22nd International Conference on, 2013, pp. 1-5.

[55] E. Oki, Linear Programming and Algorithms for Communication Networks. .

[56] Eiselt, Horst A., and Carl-Louis Sandblom. Integer programming and network models. Springer Science & Business Media, 2013.

[57] G. D. Corne, David and Oates, Martin J and Smith, Telecommunications Optimization: Heuristic and Adaptive Techniques, vol. 3. Wiley Online Library, 2000.

[58] Yamada, Hirohito, Toru Miura, and Shinya Chikui. "Controlling networks with an intelligent power system—Toward disaster-resilient networks." In Wireless Personal Multimedia Communications (WPMC), 2012 15th International Symposium on, pp. 29-29.

[59] S. E. Middleton, L. Middleton, and S. Modafferi, “Real-time crisis mapping of natural disasters using social media,” IEEE Intelligent Systems, vol. 29, no. 2, pp. 9–17, 2014.

[60] M. Kaigo, “Social media usage during disasters and social capital: Twitter and the Great East Japan earthquake,” Keio Communication Review, vol. 34, no. 1, pp. 19–35, 2012.

[61] D. E. Alexander, “Social media in disaster risk reduction and crisis management,” Science and engineering ethics, vol. 20, no. 3, p. 717, 2014.

[62] J. B. Houston, J. Hawthorne, M. F. Perreault, E. H. Park, M. Goldstein Hode, M. R. Halliwell, S. E. Turner McGowen, R. Davis, S. Vaid, J. A. McElderry, and others, “Social media and disasters: a functional framework for social media use in disaster planning, response, and research,” Disasters, vol. 39, no. 1, pp. 1–22, 2015.

[63] Fraustino, Julia Daisy, Brooke Liu, and Yan Jin. "Social media use during disasters: a review of the knowledge base and gaps." (2012).

[64] T. Gomes, J. Tapolcai, C. Esposito, D. Hutchison, F. Kuipers, J. Rak, A. de Sousa, A. Iossifides, R. Travanca, J. André, L. Jorge, L. Martins, P. O. Ugalde, A. Pašić, D. Pezaros, S. Jouet, S. Secci, and M. Tornatore, “A survey of strategies for communication networks to protect against large-scale natural disasters,” in 2016 8th International Workshop on Resilient Networks Design and Modeling (RNDM), 2016, pp. 11–22.

[65] Baklan, Poyraz, Kyoko Yamori, and Yoshiaki Tanaka. "Measure of user behaviour before and during disaster congestion." In Advanced Communication Technology (ICACT), 2014 16th International Conference on, 2014, pp. 135-140.

[66] K. Fukuda, M. Aoki, S. Abe, Y. Ji, M. Koibuchi, M. Nakamura, S. Yamada, and S. Urushidani, “Impact of Tohoku earthquake on R&E network in Japan,” Proceedings of the Special Workshop on Internet and Disasters - SWID ’11, vol. i, pp. 1–6, 2011.

[67] J. M. Simmons, Optical network design and planning. Springer, 2014.

[68] R. W. Tkach, “Scaling Optical Communications for the Next Decade and Beyond,” Bell Labs Technical Journal, vol. 14, no. 4, pp. 3–9, 2010.

[69] R. Stankiewicz and A. Jajszczyk, “A survey of QoE assurance in converged networks,” Computer Networks, vol. 55, no. 7, pp. 1459–1473, 2011.

[70] A. P. Vela, M. Ruiz, and L. Velasco, “Distributing data analytics for efficient multiple traffic anomalies detection,” Computer Communications, vol. 107, pp. 1–12, 2017.

[71] A. P. Vela, M. Ruiz, and L. Velasco, “Reducing Virtual Network Reconfiguration and Traffic Losses under Multiple Traffic Anomalies,” in Asia Communications and Photonics Conference, 2016, p. AF3E–5.

[72] F. Dikbiyik, S. Member, and L. Sahasrabuddhe, “Exploiting Excess Capacity to Improve Robustness of WDM Mesh Networks,” IEEE/ACM Transactions on Networking (TON) vol. 20, no. 1, pp. 114–124, 2012.

[73] Dikbiyik, Ferhat, Laxman Sahasrabuddhe, Massimo Tornatore, and Biswanath Mukherjee. "Exploiting excess capacity for improved robustness in optical WDM backbone mesh networks." In Optical Fiber Communication Conference (OFC), 2010, p. JThA22.

[74] F. Dikbiyik, M. Tornatore, and B. Mukherjee, “Exploiting Excess Capacity for Survivable Traffic Grooming in Optical Backbone Networks,” vol. 6, no. 2, pp. 127–137, 2014.

[75] F. Dikbiyik, M. Tornatore, and B. Mukherjee, “Exploiting Excess Capacity , Part II : Differentiated Services Under Traffic Growth,” IEEE*/ACM Transactions on Networking (TON),* vol. 23, no. 5, pp. 1599–1609, 2015.

[76] H. Le Vu and M. Zukerman, “Blocking probability for priority classes in optical burst switching networks,” *IEEE Communications Letters*, vol. 6, no. 5, pp. 214–216, 2002.

[77] S. Dharmapurikar, P. Krishnamurthy, T. Sproull, and J. Lockwood, “Deep packet inspection using parallel bloom filters,” in *High performance interconnects, 2003. proceedings. 11th symposium on*, 2003, pp. 44–51.

[78] S. Krile and M. Kos, “A heuristic approach for path provisioning in Diff-Serv networks,” in *IEEE Seventh International Symposium on Spread Spectrum Techniques and Applications,*, 2002, vol. 3, pp. 692–696 vol.3.

[79] Y. Ye, S. Dixit, and M. Ali, “On joint protection/restoration in IP-centric DWDM based optical transport networks,” *IEEE Communications Magazine*, vol. 38, no. 6, pp. 174–183, 2000.

[80] R. Bhandari, “Optimal diverse routing in telecommunication fiber networks,” in *INFOCOM ’94. Networking for Global Communications., 13th Proceedings IEEE*, 1994, pp. 1498–1508 vol.3.

[81] K. Hinton, “Traffic modelling for the core network,” in *GreenTouch Confidential,* 2013.

[82] V. N. I. Cisco, “Forecast and methodology, 2012--2017,” *White Paper*, 2013.

[83] GreenTouch, “Reducing the Net Energy Consumption in Communications Networks by up to 90% by 2020,” *White Paper*, 2013.

[84] K. C. Claffy, G. C. Polyzos, and H.-W. Braun, “Traffic characteristics of the T1 NSFNET backbone,” in *INFOCOM’93. Proceedings. Twelfth Annual Joint Conference of the IEEE Computer and Communications Societies. Networking: Foundation for the Future, IEEE*, 1993, pp. 885–892.

[85] P. Batchelor, B. Daino, P. Heinzmann, C. Weinert, J. Späth, B. Van Caenegem, D. R. Hjelme, R. Inkret, H. A. Jäger, M. Joindot, and others, “Ultra high capacity optical transmission networks: Final report of action COST 239,” *Faculty of Electrical Engineering and Computing, University of Zagreb, Tech. Rep*, 1999.

[86] C. V. N. I. Forecast, “Cisco visual networking index: Global mobile data traffic forecast update 2009-2014,” *Cisco Public Information, February*, vol. 9, 2010.

[87] A. Zhou, S. Wang, Z. Zheng, C. H. Hsu, M. R. Lyu, and F. Yang, “On Cloud Service Reliability Enhancement with Optimal Resource Usage,” *IEEE Transactions on Cloud Computing*, vol. 4, no. 4, pp. 452–466, Oct. 2016.

[88] D. Simeonidou, R. Nejabati, G. Zervas, D. Klonidis, A. Tzanakaki, and M. J. O’Mahony, “Dynamic optical-network architectures and technologies for existing and emerging grid services,” *Journal of Lightwave Technology*, vol. 23, no. 10, pp. 3347–3357, Oct. 2005.

[89] N. I. Osman, T. El-Gorashi, L. Krug, and J. M. H. Elmirghani, “Energy-Efficient Future High-Definition TV,” *Journal of Lightwave Technology*, vol. 32, no. 13, pp. 2364–2381, Jul. 2014.

[90] N. Charbonneau, V. M. Vokkarane, and S. Member, “A Survey of Advance Reservation Routing and Wavelength Assignment in Wavelength-Routed WDM Networks,” IEEE *Communications Surveys & Tutorials,* vol. 14, no. 4, pp. 1037–1064, 2012.

[91] E. M. Varvarigos, V. Sourlas, and K. Christodoulopoulos, “Routing and scheduling connections in networks that support advance reservations,” *Computer Networks*, vol. 52, no. 15, pp. 2988–3006, 2008.

[92] S. Tanwir, L. Battestilli, H. Perros, and G. Karmous-Edwards, “Dynamic scheduling of network resources with advance reservations in optical grids,” *International Journal of Network Management*, vol. 18, no. 2, pp. 79–105, 2008.

[93] W. Lu and Z. Zhu, “Dynamic service provisioning of advance reservation requests in elastic optical networks,” *Journal of Lightwave Technology*, vol. 31, no. 10, pp. 1621–1627, 2013.

[94] E. He, X. Wang, and J. Leigh, “A flexible advance reservation model for multi-domain WDM optical networks,” in *Broadband Communications, Networks and Systems, 2006. BROADNETS 2006. 3rd International Conference on*, 2006, pp. 1–10.

[95] N. Charbonneau and V. M. Vokkarane, “Static routing and wavelength assignment for multicast advance reservation in all-optical wavelength-routed WDM networks,” *IEEE/ACM Transactions on Networking (TON)*, vol. 20, no. 1, pp. 1–14, 2012.

[96] Y. Chen and A. Jaekel, “Energy-Aware Scheduling and Resource Allocation for Periodic Traffic Demands,” *Journal of Optical Communications and Networking,* vol. 5, no. 4, pp. 261–270, 2013.

[97] Z. Xiaoning and X. U. Lingfei, “Energy-efficient Traffic Grooming Under Sliding Scheduled Traffic Model for IP over WDM Optical Networks,” *China Communications,* vol. 11, no. 7, 2014, pp. 74–83.

[98] S. Zhang, S. Member, D. Shen, S. Member, C. Chan, and S. Member, “Energy-Efficient Traffic Grooming in WDM Networks With Scheduled Time Traffic,” *Journal of Lightwave Technology,* vol. 29, no. 17, pp. 2577–2584, 2011.

[99] C. Xie, H. Alazemi, and N. Ghani, “Rerouting in advance reservation networks,” *Computer Communications*, vol. 35, no. 12, pp. 1411–1421, 2012.

[100] J. Zheng and H. T. Mouftah, “Routing and wavelength assignment for advance reservation in wavelength-routed WDM optical networks,” in *Communications, 2002. ICC 2002. IEEE International Conference on*, 2002, vol. 5, pp. 2722–2726.

[101] K. Zhu, S. Member, and B. Mukherjee, “Traffic Grooming in an Optical WDM Mesh Network,” *IEEE Journal on selected areas in communications,* vol. 20, no. 1, pp. 122–133, 2002.

[102] T. K. C. Chan, E. W. M. Wong, and Y.-W. Leung, “High-capacity time-domain wavelength interleaved networks,” *Journal of Lightwave Technology*, vol. 27, no. 17, pp. 3948–3958, 2009.

[103] J. M. H. Elmirghani, T. Klein, K. Hinton, T. e. h. El-Gorashi, A. Q. Lawey, and X. Dong, “GreenTouch GreenMeter core network power consumption models and results,” in *2014 IEEE Online Conference on Green Communications (OnlineGreenComm)*, 2014, pp. 1–8.

[104] S. Naiksatam, S. Figueira, S. Chiappari, and N. Bhatnagar, “Modeling Advanced Reservation Requests in Optical Network Grids,” *COEN/SCU Technical Report*, 2004.

[105] M. Shalom, W. Unger, and S. Zaks, “On the complexity of the traffic grooming problem in optical networks,” in *Fun with Algorithms*, 2007, pp. 262–271.

[106] A. Greenberg, R. Srikant, and W. Whitt, “Resource sharing for book-ahead and instantaneous-request calls,” *Teletraffic Science and Engineering*, vol. 2, pp. 539–548, 1997.

[107] X. Zhu, S. Member, M. Veeraraghavan, and S. Member, “Analysis and design of book-ahead bandwidth-sharing mechanisms,” *IEEE Transactions on Communications,* vol. 56, no. 12, pp. 2156–2165, 2008.

[108] J. Triay, C. Cervelló-pastor, V. M. Vokkarane, and S. Member, “Analytical Blocking Probability Model for Hybrid Immediate and Advance Reservations in Optical WDM Networks,” *IEEE/ACM Transactions on Networking (TON)*, vol. 21, no. 6, pp. 1890–1903, 2013.

[109] Aldraho, Abdelnour, and Alexander A. Kist. "Enabling energy efficient and resilient networks using dynamic topologies." In Sustainable Internet and ICT for Sustainability (SustainIT), 2012, pp. 1-8.

[110] S. Tan, X. Zhang, L. Li, and S. Wang, “Green optical networks with availability guarantee,” *2011 11th International Symposium on Communications & Information Technologies (ISCIT)*, no. Iscit, pp. 97–102, Oct. 2011.

[111] X. Dong, T. El-Gorashi, and J. M. H. Elmirghani, “IP over WDM networks employing renewable energy sources,” *Journal of Lightwave Technology*, vol. 29, no. 1, pp. 3–14, 2011.

[112] A. Kwasinski and P. T. Krein, “Telecom power planning for natural and man-made disasters,” in *INTELEC 07 - 29th International Telecommunications Energy Conference*, 2007, pp. 216–222.

[113] European Commission-Joint Research Centre, “No Title,” *2012*. [Online]. Available: http://re.jrc.ec.europa.eu/pvgis/.

[114] T. A. Huld, M. Suri, R. P. Kenny, and E. D. Dunlop, “Estimating PV performance over large geographical regions,” in *Photovoltaic Specialists*

Conference, 2005. Conference Record of the Thirty-first IEEE, 2005, pp. 1679–1682.

[115] Tesla, “Tesla Power Wall.” [Online]. Available: https://www.renewableenergyhub.co.uk/uploads/products/17672/product_brochures/Tesla_Powerwall_Datasheet_v3-2_English.pdf.