2016

Optimal Route and Spectrum Allocation in Fault Tolerant OFDM Networks

Sayeed Ahmed
University of Windsor

Optimal Route and Spectrum Allocation in Fault Tolerant OFDM Networks

by

Sayeed Ahmed

A Thesis
Submitted to the Faculty of Graduate Studies
through the School of Computer Science
in Partial Fulfillment of the Requirements for
the Degree of Master of Science at the
University of Windsor

Windsor, Ontario, Canada
2016

Optimal Route and Spectrum Allocation in Fault Tolerant OFDM Networks

by

Sayeed Ahmed

APPROVED BY:

F. Baki
Odette School of Business

X. Yuan
School of Computer Science

S. Bandyopadhyay, Advisor
School of Computer Science

Y. Aneja, Advisor
Odette School of Business

July 26, 2016

DECLARATION OF ORIGINALITY

I hereby certify that I am the sole author of this thesis and that no part of this thesis has been published or submitted for publication.

I certify that, to the best of my knowledge, my thesis does not infringe upon anyone's copyright nor violates any proprietary rights and that any ideas, techniques, quotations, or any other material from the work of other people included in my thesis, published or otherwise, are fully acknowledged in accordance with the standard referencing practices. Furthermore, to the extent that I have included copyrighted material that surpasses the bounds of fair dealing within the meaning of the Canada Copyright Act, I certify that I have obtained a written permission from the copyright owner(s) to include such material(s) in my thesis and have included copies of such copyright clearances to my appendix.

I declare that this is a true copy of my thesis, including any final revisions, as approved by my thesis committee and the Graduate Studies office, and that this thesis has not been submitted for a higher degree to any other University or Institution.

ABSTRACT

With the ever-increasing need for faster data communication, cloud services using datacenters are becoming the norm for large-scale data processing. When a disaster occurs in such a system, it is important to ensure that the users do not experience a huge data loss. Current techniques based on protection or restoration are not appropriate for such systems. Recently, the use of Orthogonal Frequency Division Multiplexing (OFDM) has been proposed for high bandwidth demands in cloud networks. Techniques for handling disasters in OFDM networks have not been investigated yet. A new scheme is developed in this research for recovering from any disaster by switching over to alternate paths that avoid the disaster. A new Integer Linear Programming (ILP) formulation has been developed, based on this scheme. The proposed formulation gives an optimal solution, based on an exhaustive search and is useful as a benchmark. A number of experiments have been conducted, which demonstrate the feasibility of the approach.

ACKNOWLEDGEMENTS

I like to take this opportunity to convey my sincere thanks to my supervisors, Dr. Subir Bandyopadhyay and Dr. Yash Aneja, for their guidance and support, throughout my graduate studies. This work could not have been achieved without their advice, suggestions and cooperation.

I would like to thank the members of my M.Sc. thesis committee, Dr. Fazle Baki, Dr. Xiaobu Yuan and Dr. Luis Rueda for their valuable time, suggestions and constructive comments.

I like to thank Dr. Quazi R. Rahman, for his cordial support and help, as well as everybody else who has offered any help, during my graduate study at the University of Windsor. I would also extend my love and gratitude to my family and friends for being so supportive and encouraging.

Finally, I would like to thank my Dad, Monsur Ali, Mom, Khaleda Begum, elder brother, Dr. Sabbir Ahmed, and younger brother, Dr. Mohammad Salim Ahmed for their endless advices, love and care.

Sayeed Ahmed

CONTENTS

DECLARATION OF ORIGINALITY iii

ABSTRACT iv

ACKNOWLEDGEMENTS v

TABLES viii

FIGURES ix

LIST OF ACRONYMS xi

1 Introduction **1**

1.1 Optical Networks 1

1.2 Overview of OFDM Networks and Datacenters 2

1.3 Work done and its importance 4

1.4 Structure of thesis 5

2 Review of Related Topics **6**

2.1 Fundamentals of Fiber-optics 6

2.2 Optical Network Components 8

2.2.1 Transmitter and Receiver 9

2.2.2 Optical Amplifier 10

2.2.3 Multiplexers and Demultiplexers 10

2.2.4 Optical Cross-Connects 10

2.3 Optical OFDM 11

2.4 Route and Spectrum Allocation (RSA) for OFDM networks 12

2.5 Fault tolerance in OFDM network 16

2.5.1 Related works in fault tolerance for OFDM network 17

2.6 Disaster-resilient techniques in optical networks 19

2.6.1 Related works in disaster resilient techniques 21

3 Approaches for designing robust OFDM networks for datacenters 24

3.1 Introduction to the problem 24

3.2 Assumptions made 26

3.3 Problem statement 27

3.4 Research objective 28

3.4.1 Notations used in the proposed ILP 32

3.5 An approach for designing OFDM networks 34

3.5.1 Formulation of ILP 34

3.5.2 Justification of the ILP 37

3.6 Analysis of the ILP formulation 40

4 Experimental Results 42

4.1 Experimental setups 43

4.2 Performance study 45

5 Conclusions and Future Works 52

5.1 Conclusions 52

5.2 Future Works 53

Bibliography 54

VITA AUCTORIS 58

TABLES

3.1 Table for constraints (3.16), (3.17), (3.18) and (3.19) 39

3.2 Table for constraints (3.20), (3.21) and (3.22) 40

4.1 A list of 4 requests 43

4.2 Summary of the input values for variables 45

4.3 Relation between number of disaster and average time 46

4.4 Average time and number of subcarriers for number of file 3 48

4.5 Average times by considering number of files 3, 5 and 7 49

4.6 Number of subcarriers vs Max number of requests 50

4.7 Blocking probability 51

FIGURES

2.1 Optical fiber 7

2.2 Optical fiber components 7

2.3 Internal Reflection 8

2.4 Single and multimode optical fiber 8

2.5 Optical fiber with different devices 9

2.6 An optical cross-connect switch (static) [1] 11

2.7 Signal bandwidth and guard band in *OFDM* network 12

2.8 Spectrum of *WDM* and *OFDM* signal [10] 13

2.9 A network with two lightpaths: Lightpath 1 and Lightpath 2 14

2.10 Examples (a) Available spectrums for Lighpath 1 (b) Available spectrum after establishing Lightpath 1 15

2.11 Spectrum available for Lightpath 2 15

2.12 Fault management schemes [1] 17

2.13 Resilient strategy for Optical Network [20] 20

3.1 Dominant disaster 25

3.2 Unused spectrum (Gaps) and used spectrum (Slots) 28

3.3 Virtual node and virtual edges 30

3.4 Examples (a) Path for disaster free situation (b) Path when disaster happens 31

4.1 Flow diagram for experimental setup 44

4.2 Number of disaster vs average time 46

4.3 Number of requests vs average time for (a) 50 subcarriers (b) 100 subcarriers 47

4.4 Number of requests vs average time for (a)150 subcarriers (b) 200 subcarriers 47

4.5 Number of requests vs average time for (a)250 subcarriers (b) 300 subcarriers 47

4.6 Average time vs no of subcarriers for number of files, 3 48

4.7 Average time vs number of subcarriers 49

4.8 Number of subcarriers vs Max number of requests 50

4.9 Blocking probability 51

LIST OF ACRONYMS

DZF - Disaster-zone failure

ESPAC - Elastic Separate Protection at the Connection

ILP - Integer Linear Programming

MCM - Multi-Carrier Modulation

MILP - Mixed Integer Linear Program

MIP - Mixed Integer Programming

OFDM - Orthogonal Frequency-Division Multiplexing

QCP - Quadratically Constrained Programming

QP - Quadratic Programming

RSA - Route and Spectrum Allocation

RWA - Routing and Wavelength Assignment

SLICE - Spectrum-sliced Elastic Optical Path Network

SSR - Successful Service Ratio

WDM - Wavelength Division Multiplexing

WMD - Weapons of Mass Destruction

Chapter 1

Introduction

1.1 Optical Networks

The continuous growth in the telecommunication industry, driven by endless demands for additional capacity in network throughput has been remarkable. This constant demand is fuelled by tremendous growth of Internet users with constant need for enhanced services and applications. These applications include video on demand, cloud computing, high definition TV with online gaming options. At the same time, businesses today increasingly rely on high-speed networks for their day-to-day businesses. This high demand is not only due to services to end-users, but also the increasing integration of mainstream businesses with computerized marketing and controlling of inventory, management and daily transactions. All these demands put an incredible pressure on the requirements of new technologies and at the same time, optimally utilize current available communication resources.

The use of more conventional media, for example, copper wire cables, has many shortcomings such as, sensitivity to environmental noise, lack of bandwidth capacity, high latency and ability to cover low distance propagation. Optical networks have the capacity to solve all the above shortcomings. As a result, optical communication have become the key technology for data communication through the past decade.

Optical networking is a communication technology, in which the data to be communicated encodes optical signals. Optical networks can be used in local area networks as well as in wide area networks. This kind of optical communication relies on optical amplifiers for long distance data transmission through fiber optic cables. Because of its capability of achieving extremely high bandwidth, today's internet and the other communication network infrastructures mainly rely on optical networks for the vast majority of human to human and machine to machine communication.

Optical fibers are able to provide a higher rate of data communication bandwidth, compared to copper cables. It also has many advantages: less costly, more resilience towards electromagnetic interference and is capable of covering increased distances without the requirement of amplifiers or repeaters. Optical fibers can provide higher bandwidth capacity of the order of *Gigabits per second (Gbps)*. In *Wavelength Division Multiplexing (WDM)* optical networks, up to 40 Gbps capacity per channel is available in backbone networks and 100 Gbps capacity of interfaces are now commercially available [19]. As a result, an optical network can span through cities and countries and act as a backbone for both data networks and telecommunication infrastructure.

Recently, *Orthogonal Frequency-Division Multiplexing (OFDM)* has been proposed as a promising technology for future high-speed optical transmission. In *WDM*, the inflexible nature of wavelength-routed optical networks creates limitations on network utilization. One limitation is that wavelength-routed networks require the allocation of a fixed bandwidth to a request for a connection, even when the data rate requested for the communication is not sufficient to fill the entire data carrying capacity of that bandwidth. As *OFDM* has a special modulation technique for achieving better spectral efficiency and impairment tolerance [18], it elastically delivers the requisite capacity of bandwidth depending on the demand size. As a result, by using *OFDM*, higher bandwidth capacity with an order of *Terabits per second (Tbps)* can be achieved.

1.2 Overview of OFDM Networks and Datacenters

Currently, *Orthogonal Frequency Division Multiplexing (OFDM)* is gaining interest for an effective modulation technique for optical fiber networks. Elastic allocation of bandwidth depends on the connection demand, making *OFDM* the most suitable technology compared to *Wavelength Division Multiplexing (WDM)* for optical networks. Fixed bandwidth of channels are allocated for *WDM* network whereas, flexible and overlapping channel allocation provide an efficient and higher amount of data transfer much more easily for *OFDM* optical networks. *OFDM* is a special class of the *Multi-Carrier Modulation (MCM)* scheme, which communicates a data scheme by dividing it into a number of channels, commonly referred to as subcarriers, each carrying a relatively low data rate signal [10]. This proposed *Spectrum-sliced Elastic Optical Path Network (SLICE)* is expected to increase the network utilization efficiency, compared to *WDM* networks by allocating a portion of the available spectrum according to the traffic demands. However, this new concept provides new challenges at the networking level, as the *Routing and Wavelength Assignment (RWA)* algorithms of traditional *WDM* networks are no longer applicable. At the same time, to establish a connection in *OFDM* for capacity greater than that of one subcarrier, a number of contiguous subcarriers are required to be established for achieving improved spectral efficiency [18]. As a result, spectrum continuity constraint is required in *OFDM* networks instead of wavelength continuity constraint that has to be satisfied in traditional *WDM* networks.

In recent years, it is evident that the computing concept is shifting from personal computing towards cloud computing. In a cloud computing environment, datacenters provide a key role to provide computing facilities as services and store a very large amount of data. A datacenter can be defined as a facility used to house computer systems and associated services such as telecommunication and storage systems [4]. Various other facilities like backup power supply, redundant data communication connections, environmental controls and numerous security devices also needed in datacenters. To provide a robust communication system that may withstand faults, file replication is an important technique for backup file storage. In the case of disasters like earthquakes, hurricanes or terrorist activities, datacenters must be able to provide data files requested by clients or users.

In the last few years, disasters such as *Hurricane Sandy* in the USA and *Sichuan Earthquake* in China show that backbone networks are highly vulnerable to disasters. In *Sichuan* province alone, telecommunication provider *China Unicom's* services to nearby counties were cut off with more than 700 towers affected [5]. Today's network protections do not take such cascading disaster management into account. It needs to be noted that telecom backbone networks mainly consist of optical fibers that create the optical mesh structures to provide high-volume connectivity across large distances covering several datacenters and are ultimately responsible for national security, cloud computing and battlefield surveillance. Thus, survivability against disasters is critical and undoubtedly needs urgent attention. In traditional WDM networks, the probability of node failure is taken to be negligibly small. Techniques have been proposed to handle the failure affecting any fiber in the networks. These failures have been extended to handle limited cases of nodes/multiple-fiber failures. In datacenter networks, data is replicated so that, each file is stored at multiple locations. A disaster can affect any number of nodes and/or edges. Some copies of a file stored in datacenter networks may be destroyed when a disaster happens. Disaster management in such networks includes selecting an appropriate surviving node that has a copy of the request file and a fault-free path from that node to the node that requests the file. This is a problem different from that studied in WDM networks and needs special attention.

1.3 Work done and its importance

Our research environment consists of optical networks with nodes representing both the datacenters and users. The main objective of this research is to propose a solution for handling requests for transmitting files from datacenters using *OFDM* and a specified communication rate requiring a specified number of contiguous subcarriers in both disaster-prone and disaster-free environments. Our purpose for this work is to study and propose a scheme to minimize the resources needed to handle the requests for communication in both such situations. We measure the resources used to handle these new requests by the total number of new sub-carriers on each fiber, which were not needed by any of the existing communication. We address this problem by using *Integer Linear Programming (ILP)* formulations and an optimal problem-solving approach. This *ILP* formulation approach performs an exhaustive search to find an optimal path and an optimal bandwidth for the primary path for the disaster-free situation and backup paths for each disaster scenario. To the best of our knowledge, no other researcher has developed such an *ILP* formulation, to determine an optimal scheme for disaster management, particularly in creating primary and backup paths for datacenters using *OFDM* technology. The inputs to our *ILP* formulation include the physical topology of the network, disaster scenarios, file replication strategy used and a request for communication. Finally, we have studied, using simulation, the reliability of our approach in terms of the running time of our proposed solution.

1.4 Structure of thesis

The rest of this thesis is organized as follows. In Chapter 2, we have reviewed basic concepts of optical networks based on *OFDM*, the notion of disaster resilient techniques and datacenter networks. We have presented our proposed approach in Chapter 3. A detailed analysis of the ILP formulation, along with the number of integer variables generated by our formulations is also given in Chapter 3. Chapter 4 describes the implementation details of this approach, the simulation results, with critical comments. Finally, the conclusions and possible future work are presented in Chapter 5.

Chapter 2

Review of Related Topics

This chapter reviews the topics related to the research reported in this thesis including the following topics:

1. Fundamentals of fiber-optics.
2. Fault tolerance in *OFDM* network.
3. Disaster resilient techniques in optical networks.

2.1 Fundamentals of Fiber-optics

Optical-fiber communication is a system of data transmission from one place to another by the use of light pulses. This optical signal forms an electromagnetic carrier wave, which is modulated for carrying information over long distances [21]. A special kind of optical cables is used for sending these modulated optical signals. An optical fiber is made of very thin and long strands of pure glass or high quality plastic with the diameter of a human hair. These fibers are bundled together to form an optical cable. When an optical signal enters one end of the fiber, it travels through it until it reaches the other end of the fiber. Because of this special characteristic, a very minimal loss of signal happens during this journey along the fiber.

A single optical fiber can be divided into following three parts:

- *Core*: Thin cylinder of glass or plastic, through which the light travels.

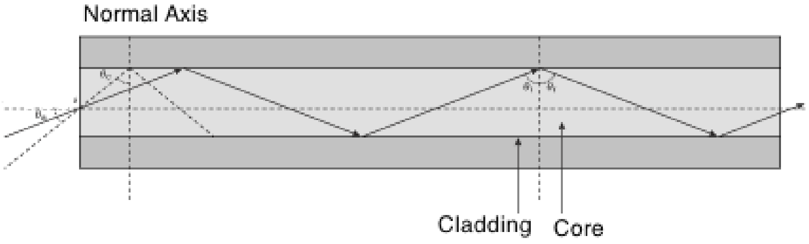

Fig. 2.1: Optical fiber

- *Cladding*: The core is surrounded by outer optical material with a lower index of reflection, where light is reflected and makes its way back to the core.

- *Buffer*: In a fiber optic cable, a buffer is a kind of component used to encapsulate a fiber to protect it from physical damage and is moisture and also used for fiber identification. Sometimes there are two layers of buffer, primary and secondary buffer.

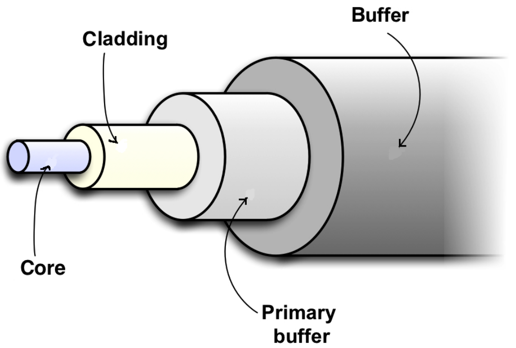

Fig. 2.2: Optical fiber components

Optical signals propagate through the optical fiber based on the laws of refraction and reflection. When light experiences a change in speed while passing through two mediums of different densities, refraction happens. A ray of light entering a fiber guides through the fiber by repetitively reflecting back and forth between the higher refractive index core and the lower refractive index cladding. When light moving through a medium with refracting index of n_1 to a second medium, having a refractive index of n_2, with $n_1>n_2$ and incident angle greater than the critical angle $\sin^{-1}\left(\frac{n_2}{n_1}\right)$, the light will reflected back and will propagate without loss. This is called internal reflection.

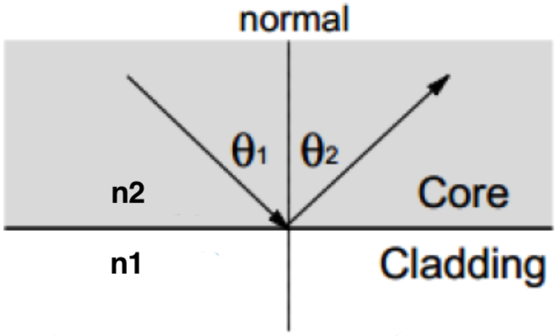

Fig. 2.3: Internal Reflection

By this way, an optical signal travels from one end of the optical medium towards the other end with internal reflection. This internal reflection is determined by critical angle, which is estimated by the reflecting index of both core and cladding based on Snell's Law.

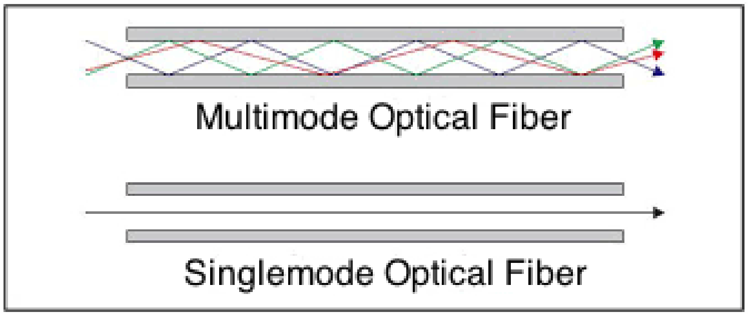

Fig. 2.4: Single and multimode optical fiber

A single mode optical fiber has a core diameter of 8 μm, the cladding has a diameter of 125 μm and the buffer has a diameter of 250 μm.

2.2 Optical Network Components

An optical network consists of several components. Full coordination is required among all these components for successful communication between a source and destination. The primary components are as follows:

- Transmitter and Receiver

- Amplifiers
- Regenerators
- Switches

These components are shown in Figure 2.5.

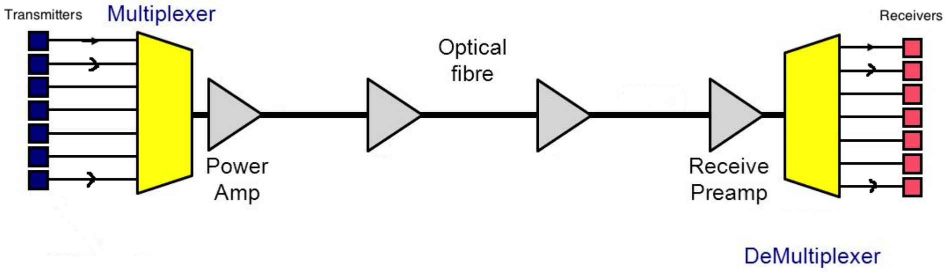

Fig. 2.5: Optical fiber with different devices

2.2.1 Transmitter and Receiver

The transmitter is an electronic device, used to generate optical signals of a specific carrier wavelength. Thus, multiple transmitters with different signals with separate data transmissions can be transmitted by means of one single optical fiber by use of different separate carrier wavelengths. Different modulation techniques are used to encode the optical signals.

The receiver receives and extracts the information from the encoded optical signals at the destination node.

2.2.2 Optical Amplifier

During the transmission through a medium, a particular amount of reduction in the intensity of the optical signal occurs depending on the distance traveled. This phenomenon is called *Attenuation*. This kind of attenuation can cause severe errors during the interpretation of the signal at a destination. As a result, an enhancement of the strength of an optical signal is required. For this reason, an optical amplifier is placed at periodic intervals along the optical fiber. These amplifiers enhance the signal strength and prevent any transmission error.

2.2.3 Multiplexers and Demultiplexers

Multiplexers are used to create different channels by combining optical signals and help transmit the signal through a single optical fiber.

On the other hand, a *demultiplexer* receives a single input signal and transmits it through a single line selected from several other data-output-lines. Usually, multiplexers and demultiplexers work together at both ends of the transmission line.

2.2.4 Optical Cross-Connects

Optical cross-connects are used to switch high-speed optical signals through optical fiber networks. An *optical cross-connect* is capable of operating in an optical level without converting optical signals to electrical signals. As a result, much faster speed can be achieved by using *optical cross-connects*. Usually, *optical cross-connects* work together with *multiplexers* and *demultiplexers*. Incoming signals in an optical network are demultiplexed before being connected to optical switching modules. Then, an *optical multiplexer* is used to multiplex the signals into an optical fiber.

Optical cross-connects can be static or dynamic. In Figure 2.6, the optical cross-connect is static.

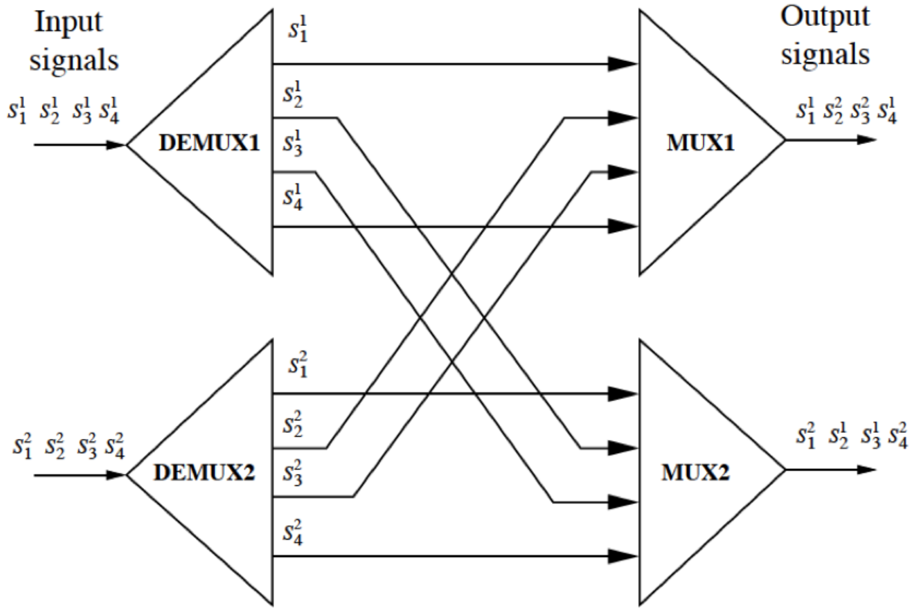
Input signals
s_1^1 s_2^1 s_3^1 s_4^1
DEMUX1
s_1^1
s_2^1
s_3^1
s_4^1
s_1^2 s_2^2 s_3^2 s_4^2
DEMUX2
s_1^2
s_2^2
s_3^2
s_4^2
Output signals
MUX1
s_1^1 s_2^2 s_3^2 s_4^1
MUX2
s_1^2 s_2^1 s_3^1 s_4^2

Fig. 2.6: An optical cross-connect switch (static) [1]

2.3 Optical OFDM

The constant growth in data traffic demands more efficient and powerful transmission platform for data speed of more than 100 Gbps. As a result, it becomes vital to reduce the requirement of total bandwidth for data transmission. So we need some technology other than *WDM*. *Orthogonal Frequency-Division Multiplexing (OFDM)* has emerged as a promising alternative to *WDM*. The main reason behind this is the elastic nature of bandwidth with *OFDM*. *OFDM* based spectrum-sliced elastic optical path network (SLICE) has higher spectrum efficiency compared to *WDM* because of its fine granularity of sub-carrier frequencies. For achieving better spectral efficiency, a number of contiguous subcarriers need to be allocated when connection needs a capacity larger than single *OFDM* subcarrier. In this way, *OFDM* technology is able to accommodate an hourappropriate number of sub-carriers according to the demand requirements.

In Figure 2.7 , each optical signal is assigned a distinct channel with required flexible bandwidth. Moreover, to avoid the interference between different optical signals, each channel is separated by a certain bandwidth known as channel spacing or guard band. In this particular figure, the value of channel spacing or guard band is 100 GHz. In *WDM*,

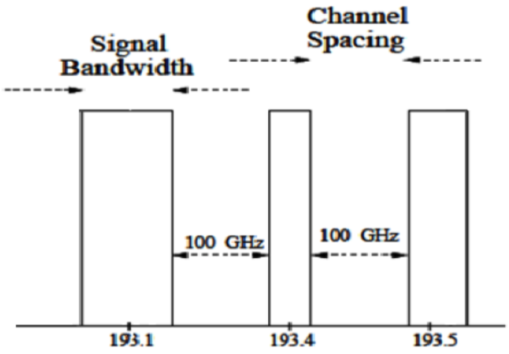

Fig. 2.7: Signal bandwidth and guard band in *OFDM* network

fixed channel spacing between the wavelengths is required to eliminate crosstalk. On the other hand, *OFDM* permits the spectrum of individual subcarriers to overlap because of the property of orthogonality, as indicated in Figure 2.8. As a result, when a subcarrier is sampled at its peak, other subcarriers have zero crossing at that particular point. As a result, the subcarriers are free from any kind of interference. This leads to much greater efficiency with regard to the usage of spectral resources.

2.4 Route and Spectrum Allocation (RSA) for OFDM networks

Routing and Spectrum Allocation (RSA) is a problem for allocating a path depending on the available bandwidths in each link for requests, where the network topology and a predefined set of demand-set requests are given. Again, the main objective of *RSA* is to establish connections from sources to destinations to achieve the required spectrum allocations. For this purpose, the system must not allow overlapping spectrum for requests where one or more edges are being shared. *RSA* consists of three important constraints.

1. Spectrum clash constraint

2. Spectrum continuity constraint

3. Spectrum contiguity constraint

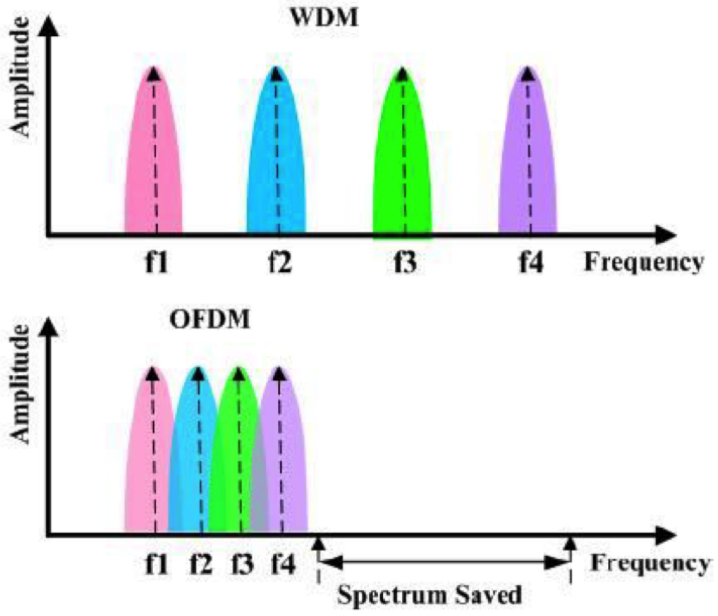

Fig. 2.8: Spectrum of *WDM* and *OFDM* signal [10]

Spectrum clash constraint: According to this constraint, any two lightpaths that share a common optical fiber must be allocated with non-overlapping spectrum or bandwidth separated by at least one guard band.

Spectrum continuity constraint: In optical networks, spectrum conversion at the optical level is not economically practical. Thus, the assigned spectrum must remain the same for all fibers along a path from source to destination. This constraint is required to establish optical lightpaths for all connections.

Spectrum contiguity constraint: This constraint ensures that the allocated subcarriers must be contiguous in the spectrum [23]. Two contiguous spectrums are separated by a guard band.

With respect to various kinds of traffic demands, the RSA problems can be classified into two types: static and dynamic. In static RSA problems, the lightpaths to be setup are known beforehand. When a static RSA lightpath establishes a connection, it remains unchanged until there is a significant change in the traffic pattern. Therefore, the lightpaths exists for sometime before the RSA algorithm is recomputed. Regarding time complexity, static RSA problems are NP-complete problems [25].

Alternately, the dynamic RSA traffic demand is not known in advance. The connection is established when the demand arrives. The main challenge in this type of traffic demand is that when a new traffic demand needs to be established, all the other existing communication must be considered. Again, when the established communication is over, the system must free the resources for future demands [24]. Thus, dynamic lightpaths are allocated when the online traffic demands arrive, and the resources are freed when the demands are finished. The dynamic RSA is considered to be a significant problem, as the demands arrive randomly and finish after varying periods of time.

Figure 2.9 and 2.10 explain the concept of RSA more elaborately:

Let, there are two lightpaths named Lightpath 1 and Lightpath 2 as shown in Figure 2.9.

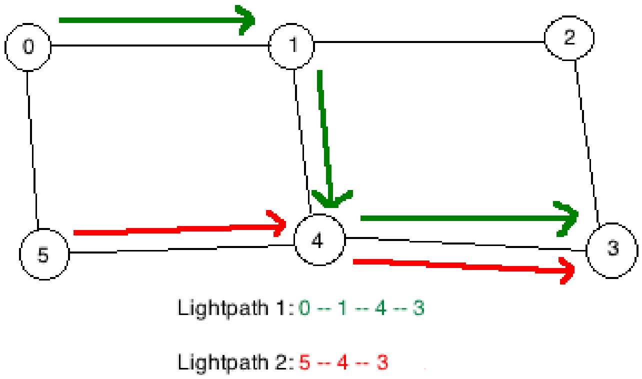

Fig. 2.9: A network with two lightpaths: Lightpath 1 and Lightpath 2

As indicated in Figure 2.10 (a), the spectrum ‘a’ is used by an ongoing connection on edge 0 - 1. By the same way, the spectrum ‘b’ on edge 1 - 4 and ‘c’, ‘d’ on edge 4 - 3 are already allocated and used by some ongoing communication. According to spectrum continuity constraint, the spectrum assigned to path 0 - 1 - 4 - 3 should remain the same for all the edges (edge 0 - 1, edge 1 - 4 and edge 4 - 3), as indicated by region P and Q. Thus, for Lightpath 1, either region P or Q can be used if the required number of subcarriers in demand are equal to or less than the subcarriers available in region P or Q. Depending on

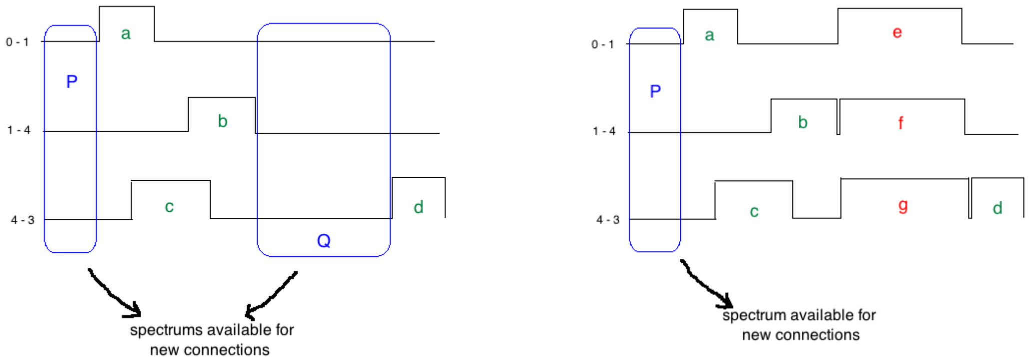
0 - 1
1 - 4
4 - 3
P
a
b
c
d
Q
spectrums available for new connections
0 - 1
1 - 4
4 - 3
P
a
e
b
f
c
g
d
spectrum available for new connections

Fig. 2.10: Examples (a) Available spectrums for Lighpath 1 (b) Available spectrum after establishing Lightpath 1

the number of subcarriers in the demand, region Q is selected, as indicated by Figure 2.10 (b), for Lightpath 1 and spectrum ‘e’ on edge 0 - 1, spectrum ‘f’ on edge 1 - 4, and spectrum ‘g’ on edge 4 - 3, each of which is used for this purpose. Region P is still available for other lightpaths like Lightpath 2.

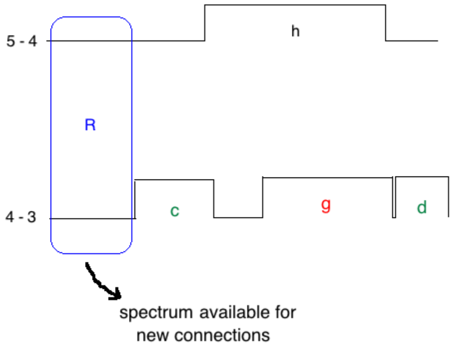

Fig. 2.11: Spectrum available for Lightpath 2

As indicated in Figure 2.9, edge 4 - 3 is common for both Lightpath 1 and Lightpath 2. According to spectrum clash constraint, spectrum g, which is used by Lightpath 1, must not be used by Lightpath 2, as indicated in Figure 2.10 (b). Thus, if possible, Lightpath 2 can use spectrums indicated by region R in Figure 2.11.

Again, with the Figure 2.10 (a), let us assume that, number of subcarriers available for region P is 11 and region Q is 24. According to spectrum contiguity constraint, if we have a new demand-request with 25 subcarriers, this can not be divided into both region P and region Q. Therefore, to accommodate this new request, a new region with 25 subcarriers or greater than 25 subcarriers is required. Otherwise this request can not be established.

2.5 Fault tolerance in OFDM network

Once an end to end path is established between the source and destination node in the optical network, a node or fiber link failure leads to the loss of data or information, which travels through the fiber link or nodes. In the case of an optical network, where Gigabits to Terabits of data are transmitting every second, this failure leads to a large amount of data loss. This conveys the concept of fault management. For this reason, the following schemes can be considered:

- Protection schemes, such as backup resources are pre-computed and reserved for each connection before a failure occurs.
- Restoration schemes, where a route and free wavelength are discovered dynamically and work for each interrupted connection after a failure occurs.

Categorization in fault management schemes are depicted in Figure 2.12.

In protection schemes, the recovery schemes are determined during the design phase and resources are reserved for each possible failure (link or path). This ensures faster and more guaranteed recovery time. The protection schemes are divided into two categories:

- Dedicated Protection
- Shared Protection

In dedicated protection, mainly there are two schemes:

- 1+1 Protection: Traffic is carried simultaneously on both the working path and the protection path. Thus, if the fault happens in the working path, data transmission is unharmed for the protection path.

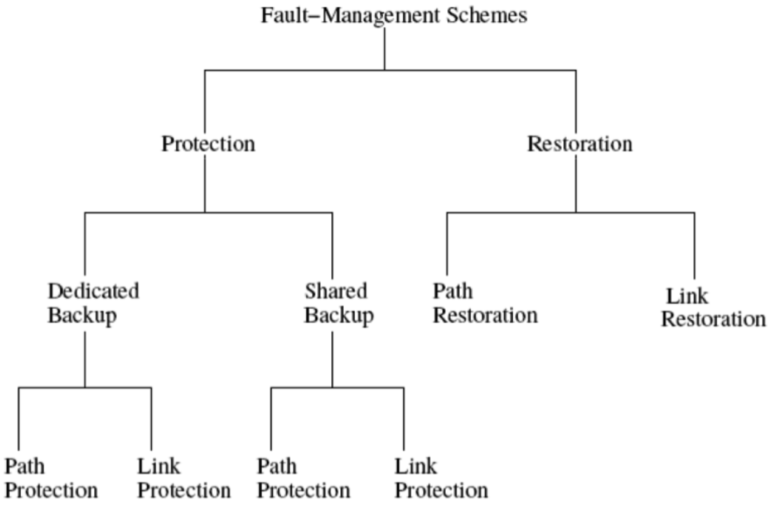

Fig. 2.12: Fault management schemes [1]

- 1:1 Protection: Traffic is carried out only on the working path and when a fault happens traffic is switched to the protected path.

In shared protection, mainly 1:N protection is used, where a fiber link can be reserved as a backup resource for multiple connections, as long as those connections do not fail simultaneously.

In a restoration scheme, recovery schemes are determined after the occurrence of a fault. Using a dynamic search for backup paths and available wavelength or subcarriers, this scheme starts recovering after failure occurrence. This kind of fault tolerance is efficient in utilizing resources and capacities.

2.5.1 Related works in fault tolerance for OFDM network

Shao et al. [3] have discussed shared path protection in *OFDM*-based optical networks with elastic bandwidth allocation. In this paper, the authors have mentioned the challenges of backup sharing in *OFDM*-based optical networks in sharing backup paths among connections efficiently with different bandwidth requests. Here, two kinds of policies, conservative sharing policy and aggressive sharing policy are discussed. In conservative sharing policy, if two backup paths have the same bandwidth and the working paths are link-disjointed, the resources can be shared. In aggressive sharing policy, two link-disjoint backup paths can share resources even if different in bandwidth. According to the authors, this kind of policy is unique and there is a benefit of efficient usage of backup resources. They have indicated that *OFDM*-based optical network is NP-complete. In this paper the authors mainly focus on developing a heuristic algorithm. After implementing this with Matlab, they examine both the blocking probability and bandwidth blocking probability for various scenarios.

Shen et al. [6] have studied shared backup path protection in *OFDM*-based elastic optical transport networks. As well, they consider 1+1 protection technique for *OFDM* optical networks. They also develop mixed *integer linear programming (MILP)* model to minimize the required protection capacity and usage of spectrum in optical networks for both shared backup path protection and 1+1 protection techniques. They have shown experimental results for 6-node, 11-node and 14-node *NFSNET* networks. Based on experimental results with working and spare capacity and used spectrum, the authors provide some comparative results between shared backup path protection and 1+1 path protection. In the conclusion, the authors mention that the proposed shared backup path protection scheme performs better than the traditional 1+1 path protection technique, and a denser network provides more opportunities for the spare capacity sharing.

Liu et al. [7] have discussed shared path protection for survivable traffic grooming in *OFDM* networks. Here the authors propose to a use the first-fit approach, by calling it *elastic separate protection at the connection (ESPAC)* to assign spectrum for the working paths and use last-fit to assign the backup path. The authors state comparisons between *WDM* and *OFDM* with respect to shared protection techniques. They propose a heuristic approach to solve *ESPAC* with dynamic traffic by exploring sharing spectrum between adjacent backup lightpaths for single fiber failure. By using a heuristic algorithm with this new back up sharing in *OFDM* network, the results indicate a significant gain in spectrum saving .

Zhang et al. [2] propose a novel shared-path protection algorithm with correlated risk against multiple failures in *OFDM* networks. In order to decrease the traffic loss caused by multiple link failures, a new parameter, called correlated risk among different connection requests is calculated for both primary and backup paths. For this purpose, they introduce two algorithms. The first algorithm works for shared-path protection algorithm with correlated risk and the second algorithm works for shared backup path protection with dynamic load balancing. They run the simulation with *NSFNET* with 14-node and *COST239* with 11-node topologies. In this simulation, they compare the performance between the proposed algorithm and traditional protection algorithms in survivable *OFDM* networks. The results show significant performance gain for the proposed algorithm. The proposed algorithm obtains smaller blocking probability than a *dedicated path protection (DPP)* algorithm. Again, by sharing a spectrum, the proposed algorithm indicates substantial usage of spectrum resources. Moreover, the level of *successful service ratio (SSR)* is higher than other algorithms. It also achieves a better *redundancy ratio (RR)* than when using other algorithms.

2.6 Disaster-resilient techniques in optical networks

The Internet has become vital to all aspects of modern life, and therefore the significances of network disruption have become increasingly serious. It is considerably recognized that the Internet is not sufficiently resilient and survivable, and thus significant research as well as development is necessary to improve the situation. The following Figure 2.13 introduces a resilient strategy for an optical network.

According to this strategy, an optical network needs to ***defend*** against challenges and threats to ensure constant and sustainable normal operations. The purpose of setting up this resilient network is to reduce the probability of occurring a fault leading to failures by reducing the impact of an adverse event on network service delivery. These defences can be identified by developing and analyzing the threats, consisting of different passive and active components. Therefore, main techniques for designing disaster-resilient optical networks are to provide geographically diverse redundant paths with alternative simultaneous wired and wireless links, so that the network is able to permit communication to be routed around the disaster-affected part. The next criterion for successfully designing a disaster-resilient optical network is to ***detect*** an adverse event or condition when it occurs. In this regard, the individual components such as routers can detect disasters and are able to understand

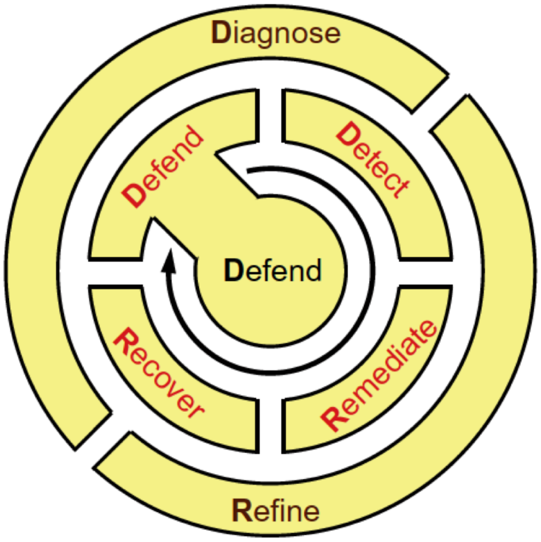

Fig. 2.13: Resilient strategy for Optical Network [20]

when and where the defence mechanisms have failed. There are different ways to determine if the network is challenged. Identifying any deviation in normal operational behaviour or by detecting service errors caused by system failures or by collecting anomalous reading can be very helpful in understanding network failures.

The next step is to ***remediate*** the effects of the detected adverse event or condition to minimize the effect on service delivery. The goal is to take the best possible action at all levels after an adverse event and during an adverse condition. In a case of disaster, the backup paths can be used to remediate the effects after detecting the disaster without direct human intervention.

Next is to use the ***recover*** technique to return to original and normal operations. When the problem is solved after a disastrous event, the network may remain in a damaged state. When the end of a challenge has been detected (e.g. disaster-affected infrastructures are recovered or a storm has passed), the system must recover to its previous optimal regular operation. As the network is possibly not to be in an ideal state, continued remediation activities may encounter additional resources. Conversely, this may take time. Moreover, it may not be clear when to revoke a remediation method that is attributed to a particular disaster because it may be designed to tackle some different kinds of problems.

After analyzing the above strategy, we must able to design a system, in which the traffic can be diverted through some backup paths to ensure a resilient network. But as we discussed before, the effects of disasters are very severe compared to other types of previously analyzed fault and path protections. Because of the effects covering a vast area with a series of cascading effects, we need to analyze and propose a solution with different perspectives. In this regard, the risk analysis of a disaster occurring and the selection of proper backup paths when a disaster happens are the two most important strategies. In the next section, we will discuss some recent works related to disaster-resilient techniques.

2.6.1 Related works in disaster resilient techniques

Habib et al. [8] have discussed a disaster-resilient optical network with uninterrupted cloud services delivered by datacenter networks. The authors have considered a circuit switched optical datacenter mesh network and formulated the problem of assigning paths to high-bandwidth connections and providing shared protection against a single disaster failure for both paths and contents using an *integer linear programming (ILP)*. They have included the content replica placement in the *ILP* as well. By using the *ILP*, the authors analyzed the characteristics of a datacenter network. The proposed two-step *ILP*, obtained by relaxing the integrity constraint of the variables, gives a lower bound on the optimal. For this purpose, the authors propose heuristics to find a feasible solution from the linear programming solution. At the same time, an algorithm for content placement is discussed. They also propose two other algorithms for computing primary and backup paths for the given request from relaxed linear programming solution for both *ILP* and heuristic solutions. Experiments are conducted with 11-node *COST239* and 14-node *NSFNET* networks. During the experiments, the wavelength usage is taken to consideration for dedicated single link failure (SLF) protection, *shared single link failure (SLF)* protection and shared *disaster-zone failure (DZF)* protection. The authors have found that shared DZF protection uses more wavelengths than shared SLF protection but fewer wavelengths than dedicated SLF protection and a probability of survivability is much higher for dedicated SLF protection. In this paper, Habib et al. have also shown the effect of the number of content replicas on wavelength usage using shared *DZF* protection in *NSFNET* and conclude that more replicas do not always provide more flexibility to choose a shorter path. More replicas use more storage for bandwidth usages for replication and synchronization. The authors have found that increasing number of datacenters does not reduce wavelength utilization and with a reasonable number of datacenters with intelligent network design can provide better survivability in case of disasters.

Savas et al. [12] have studied disaster-aware service provisioning with many-casting in the cloud network. The authors define risk, using a probabilistic model, where network equipments in a disaster zone fail with some probability. This paper considers *WDM* optical backbone network where datacenters are placed at a selected subset of network nodes. Savas et al. have developed an *integer linear programming (ILP)* model for minimizing the expected bandwidth loss when a disaster happens and at the same time minimizing the network resource usage. This is done for both *multi-path to multiple destinations (MMD)*, and a backup path to a *backup destination (BBD)*. They also consider k-shortest paths from each node to each datacenter as input. As the ILP is not applicable for large problem instances, a heuristic solution is proposed. This heuristic is used for static traffic. The authors have also used a modified version of capacity assignment algorithm. The experiments are conducted with 24-node networks. The proposed scheme provides the same level of protection by consuming 25% fewer resources than *BBD* for 50% protection and 10% fewer resources than *BBD* with full protection. In the case of heuristic algorithm, the authors demonstrate effectiveness compared to *ILP* formulation. Savas et al. have also proposed a scheme with a number of replicas per content and concluded that the number of replicas has a limited effect on the performance of many-casting when the number of replicas is fixed.

Ferdousi et al. [11] have studied disaster-aware datacenter placement and dynamic content management in cloud networks. The authors have formulated an integer linear program (ILP) for risk minimization. In this paper, a heuristic is applied per content and is divided into five phases. Cost analysis with resource utilization is performed with a dynamic content-management scheme. For experiments, the authors use a 24-node USnet topology for *weapons of mass destruction (WMD)* attack. They consider 10 *WMD* attack zones. In conclusion, the authors compare the expected loss of content with a particular network with a disaster unaware approach and achieve significant improvement in risk reduction. Moreover, after reducing risk in this dynamic approach, the authors consider the QoS constraints and the usage of the network resources with potential benefits for service providers for designing disaster-resilient cloud networks.

Dikbiyik et al. [13] have proposed a risk-minimizing scheme for disaster failures in optical backbone networks. The authors introduce a re-provisioning scheme to recover disrupted connections, which may be more severe after the initial failures. They also define a risk parameter, and introduce models for risk assessment and then formulate an *integer linear program (ILP)* as a risk-aware provisioning problem. Because of high time complexity, the authors also develop a heuristic method to calculate the risk-aware provisioning. In a small 10-node topology, the authors run experiments with both *ILP* and heuristic approaches and find out that the heuristic approach shows very close performance with *ILP* while the running time is reduced significantly. In this way, the authors have developed a disaster-risk-aware provisioning scheme for both single path and dedicated path protection. They also propose a risk aware re-provisioning scheme, which would help recover disrupted connections and take pre-cautions to protect optical backbone connections.

Mukherjee et al. [14] introduce network adaptability from disaster disruptions and cascading failures in their paper. Here, the authors discuss many potential threats with disasters and the aftermath. They identify the high-speed backbone optical networks that are the most vulnerable toward disasters.The authors compare the devastating effects of some recent disasters in the fields of optical networks and telecommunication. Types of backup path-based recovery techniques are not always applicable for the large scale and correlated cascading nature of disasters. In their paper, an elaborate classification of disasters is discussed. Some insights indicating risks and network preparedness are also introduced. Some comparisons between normal and enhanced preparedness are discussed as well.

Chapter 3

Approaches for designing robust OFDM networks for datacenters

This chapter reviews the topics related to the research reported in this thesis including the following topics:

- Assumptions made
- Problem statement
- Research objective
- Notations used in the proposed *ILP*
- An *ILP*-based approach for designing *OFDM* networks
- Analysis of *ILP* formulation

3.1 Introduction to the problem

A network consists of nodes (datacenters and other file requesting nodes) and edges (optical fibers). When a disaster happens, any number of nodes and edges can be destroyed. So a disaster d can be defined by a set $\mathcal{X}_d$ of members $\{m_1, m_2, ..., m_p\}$, where each member $m_i \in \mathcal{X}_d$ indicates some components (like edges and nodes) of the network which are destroyed by disaster d. We have used the region based disaster model [9] in which a disaster affects all network components within a region. In Figure 3.1, when a disaster (like an earth quake or a tsunami) happens, all network components in a region is affected. If the region is a circle of redius r, then certainly in the case of a wide area network, this r is small compared to the average distances between the nodes in the network. The area covered by a wide-area network may have an infinite number of disasters, each corresponding to a unique circle of radius r affected by a disaster. Let, d_1 (d_2) be a disaster and its corresponding affected member set be $\mathcal{X}_{d_1}$ ($\mathcal{X}_{d_1}$). If for set $\mathcal{X}_{d_2} \subset \mathcal{X}_{d_1}$, disaster d_2 is more severe than d_1 and we will say that d_2 dominates d_1.A disaster d is a dominant disaster if there is no other disaster that dominates d.

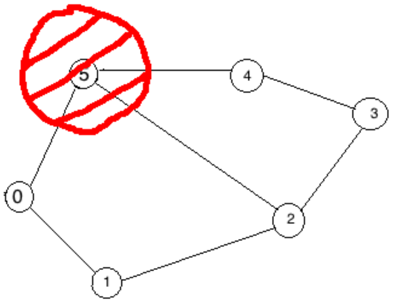

Fig. 3.1: Dominant disaster

It may be readily observed that the number of dominant disasters is always finite and can be enumerated easily. From now on, we will focus on dominant disasters only. Our algorithm does not depend on the definition of disaster and we assume that, we have a given set of dominant disasters $\mathcal{D}$ that we need to take into account.

As we are designing a disaster tolerant system, the possibility of failure of a node needs to be taken into account. if only one copy of each file f_i is stored in the network then the failure of that node containing f_i means that the file f_i is no longer available. This means that multiple copies of that file must be stored at different nodes of the network. Thus we use the term 'replication strategy' to donote how the locations of any file is determined. In our method, the replication strategy must be robust and is known in advance. Any robust replication strategy must be such that, several copies of each file must reside at multiple datacenters and for each of the dominant disaster, at least one copy of each file has a fault-free path to each node in that network that avoids that particular disaster. So if we have m copies of file f_i then we know beforehand that those copies of file f_i are saved at datacenters $\mathcal{S}_i^1, \mathcal{S}_i^2, \ldots, \mathcal{S}_i^m$. By using our proposed algorithm, appropriate optimal paths for the requested file f_i to the destination t is allocated with proper starting subcarrier c for disaster-free and the situations when disasters in $\mathcal{D}$ happen.

3.2 Assumptions made

We assume that

- we have enumerated the set $\mathcal{D}$ of dominant disasters.
- we have already determined the replication strategy for our system so that the locations for all the files $f_1, f_2, \ldots, f_n$ are known. In general, each file will be replicated at several datacenters, so that, if there are m copies of file f_i, we know that copies of file f_i are saved at datacentres $\mathcal{S}_i^1, \mathcal{S}_i^2, \ldots, \mathcal{S}_i^m$.
- the network uses *OFDM* for data communication.
- The network is currently supporting a number of on-going communication when we receive the request for transmitting file f_i to node t. The details of each existing communication are known to us, so that, for each on-going communication, we have all information about the scheme for disaster-free communication and the scheme to handle disaster d for all $d \in \mathcal{D}$.

Let there be a request to communicate file f_i to a destination node t using a communication speed that requires the use of B contiguous sub-carriers, where the network is already handling some ongoing communication. If this request can be accommodated, we have to find

- A node $\mathcal{S}_i^j$ that will be the source for communication when there is no fault.
- An appropriate path P from $\mathcal{S}_i^j$ to t and a starting sub-carrier wavelength θ for the communication. We call P the primary path.

- Path P_d for each disaster d that affects the primary path P and their corresponding starting sub-carrier wavelength θ_d. Path P_d is known as the backup path to handle disaster d that starts from a source of file f_i and ends at node t. Let, there be 5 dominant disasters in $\mathcal{D}$. Among these disasters, 3 disasters affects the primary path. Thus, in this case, our algorithm provides 3 backup paths and the corresponding starting sub-carrier wavelengths.

Here, path P could be $\mathcal{S}_i^j = a_0 \rightarrow a_1 \rightarrow \ldots a_{p-2} \rightarrow a_{p-1} = t$, where each edge $a_{i-1} \rightarrow a_i$ represents a fiber in the network. Each fiber $a_{i-1} \rightarrow a_i$ in path P should be such that sub-carriers with wavelengths $\theta, \theta + \phi, \theta + 2 \cdot \phi, \ldots, \theta + (B-1) \cdot \phi$ are available on each fiber for this new request for communication. A fiber $a_{i-1} \rightarrow a_i$, in general, is already used for several existing communication. Each existing communication uses a set of contiguous subcarrier wavelengths. As discussed in chapter 2, the spectrum of subcarrier wavelengths on fiber $a_{i-1} \rightarrow a_i$, in general, supports several communication, each requiring a particular bandwidth that consists of a number of contiguous sub-carriers. Here, we define such used contiguous subcarriers as ‘used spectrums’ or ‘slots’. For instance, in Figure 3.2 we have 2 slots. On a fiber, in general, some bandwidths are available for new requests. Here, these available bandwidths are called ‘unused spectrums’ or ‘gaps’. As a result, the total low-attenuation bandwidth on any fiber in the network can be considered as a sequence of slots and gaps, where the slots are already used by ongoing communication and the gaps are available for new communication. In Figure 3.2, A-B represents a fiber link from A to B. It contains 3 unused spectrum or gaps and 2 used spectrum or slots. Slot 1 and slot 2 are used for some ongoing communication and gap 1, gap 2, and gap 3 are available for any new communication.

3.3 Problem statement

The problem is to handle, if possible, a request for communication including

i) a specified communication rate requiring B contiguous sub-carriers,

ii) some file f_i to be communicated and,

iii) a node t requesting file f_i.

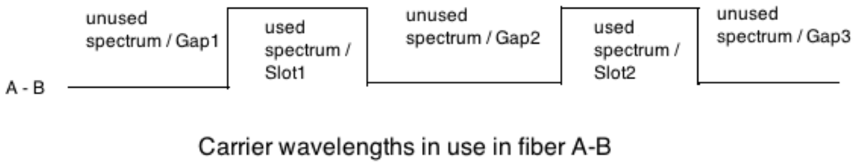

Fig. 3.2: Unused spectrum (Gaps) and used spectrum (Slots)

If we are successful in handling this request, we should be able to obtain

- details about the scheme for communication (henceforth called the scheme for disaster-free communication), which will be used to handle the disaster-free situation,
- for each disaster $d \in \mathcal{D}$, that affects the scheme for disaster-free communication, the scheme to handle disaster d. This scheme may be used to avoid all network components affected by disaster d.

We must ensure that the following conditions must be satisfied:

- the scheme for disaster-free communication will be from a node $\mathcal{S}_i^j$, where $\mathcal{S}_i^j$ $(1 \leq j \leq m)$, as explained earlier, has a copy of file f_i to node t.
- the scheme to handle disaster d will be from a node $\mathcal{S}_i^l, 1 \leq l \leq m$, where j and l are not necessarily the same node. The scheme to handle disaster d must not involve any edge affected by disaster d.
- each scheme for communication satisfies the spectrum continuity constraint.
- each scheme for communication satisfies the bandwidth clash constraint with respect to any of the existing schemes for communication.

3.4 Research objective

Bandwidth on each fiber is a scarce resource for any optical network. Assuming that only one disaster can happen at a particular time, it is highly desirable if the network is able to share the bandwidth used for different disasters. As a result, the main objective of this research is to minimize the resources needed to handle new requests for communication and at the same time, to share the bandwidth used by existing communication for disasters. We measure the resources used to handle this new request by monitoring the total number of *new* sub-carriers on each fiber used to handle this request, which was not needed by any of the existing communication. We note that, if we can handle this new request for communication,

- each fiber on the path used by the scheme for disaster-free communication must allow the same B contiguous sub-carriers. Each sub-carrier used by the scheme must not be used by any existing communication, either for disaster-free communication or for handling any disaster affecting that communication.

- each fiber on the path used by the scheme for handling disaster d must also allow the same B contiguous subcarriers. This bandwidth must not include any sub-carrier used for disaster-free communication by any existing communication. However if a subcarrier c is currently used to handle some disaster $\hat{d}, d \neq \hat{d}$ for some existing communication, the scheme for handling disaster d for the new request may use subcarrier c, since disasters d and $\hat{d}$ cannot happen at the same time.

In terms of measuring the cost of the new communication for disaster-free communication, this means we require B units of resource for each fiber in the path used by the primary path.

In the case of the scheme to handle disaster d affecting the new communication, let the scheme use sub-carrier c on a fiber, where sub-carrier c on that fiber is already reserved to handle disaster $\hat{d}, d \neq \hat{d}$ of some existing communication. Since sub-carrier c on this fiber has been reserved already for that existing communication, the use of c on this fiber does not represent an additional unused resource to be allotted to handle the new request for communication. The cost of using sub-carrier c on this fiber, for the new communication is therefore 0. We will attempt to use, to the maximum extent possible, such *free* resources when devising a scheme to handle disaster d. For each remaining subcarriers on each fiber in the backup path to handle disaster d, the cost is 1.

In this research, we have used the notion of ***virtual nodes*** and ***virtual edges*** to handle the problem of selecting one node from $\mathcal{S}_i^1, \mathcal{S}_i^2, \ldots, \mathcal{S}_i^m$. In other words, for processing a request for transmitting file f_i to a node t, it is convenient to visualize a new *virtual node* s and some new *virtual fibers* or *virtual edges* from s. For each data centre $\mathcal{S}_i^j, 1 \leq j \leq m$ containing a copy of the requested file f_i, we visualize a single *virtual fiber* from virtual node s to the node corresponding to data centre $\mathcal{S}_i^j$. A virtual node and the corresponding virtual edges do not physically exist. When considering a request, we note that

i) these virtual edges or fibers are not used for any of the existing connection, and

ii) the virtual edges or fibers do not represent any new constraints (e.g., bandwidth clash constraint).

We are considering a virtual node as a source node, which is connected with virtual edges to each of the datacenter-nodes, which has a copy of a requested file. This is shown in Figure 3.3. Once we add these virtual nodes and edges to the network, our problem is to communicate from s to t using B contiguous sub-carriers, considering the case of a disaster-free network, as well as the case of the network encountering a dominant disaster. In Figure 3.3, node 6 is a virtual node, and since we have 3 copies of the requested file at nodes 0, 1, and 5, all the edges connected to node 0, node 1, and node 5 are virtual edges.

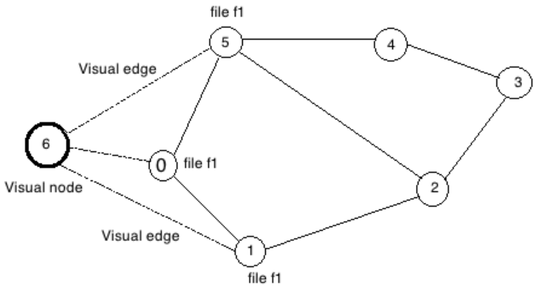

Fig. 3.3: Virtual node and virtual edges

For example, in Figure 3.4(a) and Figure 3.4(b), node 3 is the destination. Let, node 3 request file 1. Three copies of file 1 are in the datacenters situated at node 5, node 0 and node 1. Node 6 is a virtual node and is connected to node 0, node 1, and node 5 through virtual edges. In a case of disaster free situation as indicated in Figure 3.4(a),

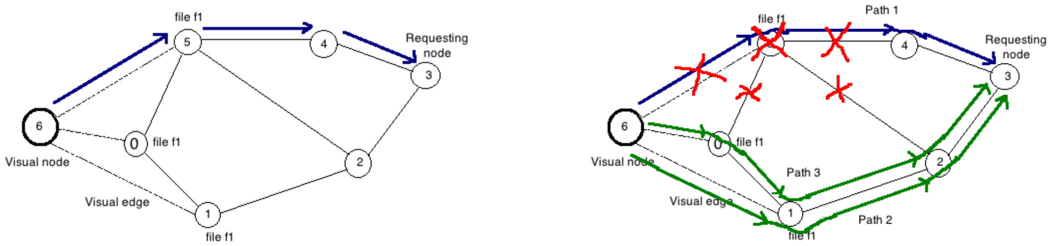

Fig. 3.4: Examples (a) Path for disaster free situation (b) Path when disaster happens

let file 1 be transmitted using path 1 from node 5 to node 3. When a dominant disaster happens to affect node 5, and all the edges connected with node 5, file 1 may no longer be communicated using path 1. In this situation, as indicated in Figure 3.4(b), file 1 is transmitted through path 2 or path 3.

In our research, we find an appropriate primary path from source s to destination t for disaster-free situation as well as backup-paths for each disaster $d \in \mathcal{D}$ that affects the primary path. We have also minimized the resources needed to handle new requests for communication by choosing appropriate paths and sharing bandwidths among the disasters. In Section 3.4.1 we have introduced the notations used in our proposed ILP formulation.In Section 3.4.2 we have described our ILP formulation. In Section 3.4.3 we have given an in-depth analysis of our proposed ILP formulation.

3.4.1 Notations used in the proposed ILP

$\boldsymbol{N}$: the set of nodes of the network including the virtual node mentioned above.

$\boldsymbol{E}$: the set of edges, each edge representing a fiber in the network, or a virtual edge as mentioned above.

$\boldsymbol{E^d}$: the set of edges of E that survive disaster d.

$\boldsymbol{\mathcal{C}}$: the ordered list of sub-carriers $[c_1, c_2, \ldots, c_p]$ that may be used on a fiber. The list is ordered, based on the wavelengths of the sub-carriers, so that the wavelength corresponding to c_1 (c_p) is the least (greatest).

$\boldsymbol{\omega_c}$: the wavelength for sub-carrier c.

$\boldsymbol{\varphi}$: the bandwidth of a sub-carrier.

$\boldsymbol{t}$: the node requesting file f_i.

$\boldsymbol{s}$: the virtual node corresponding to the file f_i.

$\boldsymbol{a_{ij}^g}$: a constant denoting the starting frequency of the g^{th} gap on link (i, j) for the scheme to handle disaster-free communication.

$\boldsymbol{b_{ij}^g}$: a constant denoting the ending frequency of the g^{th} gap on link (i, j) for the scheme to handle disaster-free communication.

$\boldsymbol{a_{ij}^{gd}}$: a constant denoting the starting frequency of the g^{th} gap on link (i, j) for the scheme to handle disaster d.

$\boldsymbol{b_{ij}^{gd}}$: a constant denoting the ending frequency of the g^{th} gap on link (i, j) for the scheme to handle disaster d.

$\boldsymbol{\theta}$: the wavelength of the first subcarrier used by the scheme to handle disaster-free communication.

$\boldsymbol{\theta^d}$: the wavelength of the first subcarrier used by the scheme to handle disaster d.

$\boldsymbol{B}$: required number of subcarriers for the signal, so that for the disaster-free case the wavelengths used will be $\theta, \theta + \phi, \theta + 2 \cdot \phi, \ldots, \theta + (B-1) \cdot \phi$. This count also includes the guard band.

$\boldsymbol{M}$: a large constant.

$\boldsymbol{f_{ij}^c}$: a constant for all on link (i,j) and subcarrier $c \in \mathcal{C}$ where

$$f_{ij}^c = \begin{cases} 1 & \text{if subcarrier } c \text{ on link } (i,j) \in E \text{ is unused by any communication} \\ & \text{currently in progress,} \\ 0 & \text{otherwise.} \end{cases}$$

$\boldsymbol{x_{ij}}$: a binary variable for all on link (i,j) where

$$x_{ij} = \begin{cases} 1 & \text{if link } (i,j) \in E \text{ is used in the path from } s \text{ to } t \text{ for the scheme to handle} \\ & \text{disaster-free communication,} \\ 0 & \text{otherwise.} \end{cases}$$

$\boldsymbol{y_{ij}^d}$: a binary variable for all on link (i,j) where

$$y_{ij}^d = \begin{cases} 1 & \text{if link } (i,j) \in E^d \text{ is used in the path from } s \text{ to } t \text{ for the scheme to handle} \\ & \text{disaster } d, \\ 0 & \text{otherwise.} \end{cases}$$

$\boldsymbol{x_{ij}^g}$: a binary variable for all edge $(i,j) \in E$ and for all gap g on fiber where

$$x_{ij}^g = \begin{cases} 1 & \text{if gap } g \text{ on link } (i,j) \text{ is used for the the scheme to handle disaster-free} \\ & \text{communication,} \\ 0 & \text{otherwise.} \end{cases}$$

$\boldsymbol{y_{ij}^{gd}}$: a binary variable for all edge $(i,j) \in E^d$ and for all gap g on fiber where

$$y_{ij}^{gd} = \begin{cases} 1 & \text{if gap } g \text{ on link } (i,j) \text{ is used for the the scheme to handle disaster } d, \\ 0 & \text{otherwise.} \end{cases}$$

$\boldsymbol{q^d}$: a binary variable for all disaster $d \in \mathcal{D}$ where

$$q^d = \begin{cases} 1 & \text{if the primary lightpath uses any edge disrupted by disaster } d, \\ 0 & \text{otherwise.} \end{cases}$$

$\boldsymbol{u^{dc}}$: a binary variable for all disaster $d \in \mathcal{D}$ and for all subcarrier $c \in \mathcal{C}$ where

$$u^{dc} = \begin{cases} 1 & \text{if subcarrier } c \text{ having wavelength } \omega_c \geq \theta^d, \\ 0 & \text{otherwise.} \end{cases}$$

$\boldsymbol{v^{dc}}$: a binary variable for all disaster $d \in \mathcal{D}$ and for all subcarrier $c \in \mathcal{C}$ where

$$v^{dc} = \begin{cases} 1 & \text{if subcarrier } c \text{ having wavelength } \omega_c \leq \theta^d + (B-1) \cdot \phi, \\ 0 & \text{otherwise.} \end{cases}$$

$\boldsymbol{z_{ij}^{dc}}$: a continuous variable for all disaster $d \in \mathcal{D}$, for all subcarrier $c \in \mathcal{C}$, and for all link $(i, j) \in E^d$, which is constrained by the conditions given below. so that

$$z_{ij}^{dc} = \begin{cases} 1 & \text{if subcarrier } c \text{ is used on link } (i,j) \text{ to handle disaster } d, \\ 0 & \text{otherwise.} \end{cases}$$

$\boldsymbol{s_{ij}^{gd}}$: a continuous variable for all gap g in all link $(i, j) \in E^d$, and all disaster $d \in \mathcal{D}$, which is constrained by the conditions given below. so that

$$s_{ij}^{gd} = \begin{cases} 1 & \text{if the primary path uses any link } (i,j) \in E^d \text{ disrupted by disaster } d, \\ 0 & \text{otherwise.} \end{cases}$$

$\boldsymbol{\epsilon}$: a very small constant (0.01).

3.5 An approach for designing OFDM networks

3.5.1 Formulation of ILP

Objective function: Minimize

$$B \cdot (\sum_{(i,j) \in E} x_{ij} + \sum_{d \in \mathcal{D}} \sum_{c \in \mathcal{C}} \sum_{(i,j) \in E^d} z_{ij}^{dc} \cdot f_{ij}^c) \tag{3.1}$$

Subject to:

1. Enforce flow conservation on the paths to be used for the scheme for disaster-free communication and the scheme to handle disaster d,

$$\sum_{j:(i,j) \in E} x_{ij} - \sum_{j:(j,i) \in E} x_{ji} = \begin{cases} 1 & \text{if } i = s, \\ -1 & \text{if } i = t, \quad \forall i \in N \\ 0 & \text{otherwise.} \end{cases} \tag{3.2}$$

$$\sum_{j:(i,j)\in E^d} y_{ij}^d - \sum_{j:(j,i)\in E^d} y_{ji}^d = \begin{cases} q^d & \text{if } i = s, \\ -q^d & \text{if } i = t, \quad \forall i \in N, \forall d \in \mathcal{D} \\ 0 & \text{otherwise.} \end{cases} \tag{3.3}$$

2. Set $q^d = 1$ if disaster d disrupts the primary lightpath. Otherwise set $q^d = 0$.

$$q^d \geq x_{ij} \quad \forall (i,j) \in E - E^d, d \in \mathcal{D} \tag{3.4}$$

$$q^d \leq \sum_{i,j:(i,j)\in E-E^d} x_{ij} \quad \forall d \in \mathcal{D} \tag{3.5}$$

3. Exactly one gap is used on each edge in the paths to be used for the scheme for disaster-free communication and for the scheme to handle disaster d,

$$\sum_g x_{ij}^g = x_{ij} \quad \forall (i,j) \in E \tag{3.6}$$

$$\sum_g y_{ij}^{gd} = y_{ij}^d \quad \forall (i,j) \in E^d, \forall d \in \mathcal{D} \tag{3.7}$$

4. The starting frequency for the scheme for disaster-free communication (handling disaster d) must be greater than or equal to the starting frequency of some gap g.

$$\theta \geq a_{ij}^g \cdot x_{ij}^g \quad \forall (i,j) \in E \tag{3.8}$$

$$\theta^d \geq a_{ij}^{gd} \cdot s_{ij}^{gd} \quad \forall (i,j) \in E^d, \forall d \in \mathcal{D} \tag{3.9}$$

5. The ending frequency for the scheme for disaster-free communication (handling disaster d) must be less than or equal to the ending frequency of the same gap g.

$$\theta + (B-1) \cdot \varphi \leq b_{ij}^g + M \cdot (1 - x_{ij}^g) \quad \forall (i,j) \in E \tag{3.10}$$

$$\theta^d + (B-1) \cdot \varphi \cdot q^d \leq (b_{ij}^{gd} + M) \cdot q^d - M \cdot s_{ij}^{gd} \quad \forall (i,j) \in E^d, \forall d \in \mathcal{D} \tag{3.11}$$

6. Compute the value of z_{ij}^{dc}.

$$u^{dc} \cdot M \geq \omega_c - \theta^d + \epsilon \quad \forall d \in \mathcal{D}, \forall c \in \mathcal{C} \tag{3.12}$$

$$(1 - u^{dc}) \cdot M \geq \theta^d - \omega_c \quad \forall d \in \mathcal{D}, \forall c \in \mathcal{C} \tag{3.13}$$

$$v^{dc} \cdot M \geq \theta^d + (B-1) \cdot \varphi - \omega_c + \epsilon \quad \forall d \in \mathcal{D}, \forall c \in \mathcal{C} \tag{3.14}$$

$$(1 - v^{dc}) \cdot M \geq \omega_c - \theta^d - (B-1) \cdot \varphi \quad \forall d \in \mathcal{D}, \forall c \in \mathcal{C} \tag{3.15}$$

$$z_{ij}^{dc} \leq y_{ij}^{d} \quad \forall d \in \mathcal{D}, \forall c \in \mathcal{C}, \forall (i,j) \in E^d \tag{3.16}$$

$$z_{ij}^{dc} \leq u^{dc} \quad \forall d \in \mathcal{D}, \forall c \in \mathcal{C}, \forall (i,j) \in E^d \tag{3.17}$$

$$z_{ij}^{dc} \leq v^{dc} \quad \forall d \in \mathcal{D}, \forall c \in \mathcal{C}, \forall (i,j) \in E^d \tag{3.18}$$

$$z_{ij}^{dc} \geq v^{dc} + u^{dc} + y_{ij}^{d} - 2 \quad \forall d \in \mathcal{D}, \forall c \in \mathcal{C}, \forall (i,j) \in E^d \tag{3.19}$$

7. Compute the value of s_{ij}^{gd}.

$$s_{ij}^{gd} \leq y_{ij}^{gd} \quad \forall d \in \mathcal{D}, \forall c \in \mathcal{C}, \forall (i,j) \in E^d \tag{3.20}$$

$$s_{ij}^{gd} \leq q^{d} \quad \forall d \in \mathcal{D}, \forall c \in \mathcal{C}, \forall (i,j) \in E^d \tag{3.21}$$

$$s_{ij}^{gd} \geq y_{ij}^{gd} + q^d - 1 \quad \forall d \in \mathcal{D}, \forall c \in \mathcal{C}, \forall (i,j) \in E^d \tag{3.22}$$

3.5.2 Justification of the ILP

The objective function in equation (3.1) has two parts - the cost of the scheme for disaster-free communication, and the cost to handle the disasters. To account for the first part, we note that each sub-carrier on each fiber on the path used by the scheme for disaster-free communication has a cost of 1. In the second part, the cost would also be counted once for each subcarrier for disaster situation. This happens because, the subcarriers shared by other different disasters will not cause any extra cost.

Constraint (3.2) corresponds to the flow balance constraint [16] for disaster-free communication. This means to specify the difference between the sum of outgoing and incoming flows to be:

- 1, if node i is the source.
- -1, if node i is the destination.
- 0, if node i is any other intermediate node in the path from the source to the destination.

Constraint (3.3) corresponds to flow balance constraint [16] to determine the path when when disaster d happens. This is to specify the difference between the sum of outgoing and incoming flows for the communication when disaster happens:

- q^d, if node i is the source. If $q^d = 0$ (i.e. disaster d does not affect the primary path), the flow is 0.
- -q^d, if node i is the destination.
- 0, if node i is any other intermediate node in the path from the source to the destination.

Constraint (3.4) and (3.5) ensure that, if disaster d disrupts the primary path, then q^d is 1. Otherwise, the value of q^d would be 0.

Constraint (3.6) ensures that one gap on each link in the path is used for disaster-free communication.

Constraint (3.7) ensures that, exactly one gap on each link in the backup path is used when disaster d happens.

Constraints (3.8) and (3.10) state that, if gap g on link $(i, j) \in E$ is used (i. e., $x_{ij}^{g} = 1$) for the scheme for disaster-free communication, the sub-carriers used for the communication must have wavelengths that are within the g^{th} gap. If $x_{ij}^{g} = 1$, constraints (3.8) and (3.10) become $\theta \geq a_{ij}^{g}$ and $\theta + (B - 1) \cdot \varphi \leq b_{ij}^{g}$, so that $a_{ij}^{g} \leq \theta < \theta + (B - 1) \cdot \varphi \leq b_{ij}^{g}$ which satisfies the requirements. If $x_{ij}^{g} = 0$, $\theta \geq 0$ and $\theta + (B - 1) \cdot \varphi \leq M$ then both are trivially true. Explanations for constraints (3.9) and (3.11) are similar.

Constraints (3.12) - (3.19) are used to define the value of z_{ij}^{dc}. Variable z_{ij}^{dc} has a value of 1 if the following conditions are satisfied:

1. Edge (i, j) is on the path from the source s to the destination t in the scheme to handle disaster d.

2. The bandwidth corresponding to sub-carriers starting with carrier wavelength θ^{d} and ending with the subcarrier with carrier wavelength $\theta^{d} + (B - 1) \cdot \varphi$ includes sub-carrier ω_c.

The first condition means that $y_{ij}^{d} = 1$. The second condition is equivalent to the condition $\theta^{d} \leq \omega_c \leq \theta^{d} + (B - 1) \cdot \varphi$. This condition may be restated as $\omega_c \geq \theta^{d}$ and $\theta^{d} + (B - 1) \cdot \varphi \geq \omega_c$. In other words, the condition to be satisfied is $u^{dc} = 1$ and $v^{dc} = 1$. Variables y_{ij}^{d}, u^{dc} and v^{dc} are all binary variables. Thus $z_{ij}^{dc} = 1$, if and only if $y_{ij}^{d} = 1$, $u^{dc} = 1$ and $v^{dc} = 1$.

Constraints (3.12) and (3.13) define the value of u^{dc}. Constraints (3.14) and (3.15) define the value of v^{dc}. Constraints (3.16), (3.17), (3.18) and (3.19) define the value of z_{ij}^{dc}.

The product $z_{ij}^{dc} \cdot f_{ij}^{c}$ is 1 if sub-carrier c on edge (i, j) is used to handle disaster d where sub-carrier c on edge (i, j) represents a new resource that has not been used by any other communication. This explains the second term.

y_{ij}^d	u^{dc}	v^{dc}	z_{ij}^{dc}
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	0
1	0	0	0
1	0	1	0
1	1	0	0
1	1	1	1

Table 3.1: Table for constraints (3.16), (3.17), (3.18) and (3.19)

When, $y_{ij}^d = 0$, $u^{dc} = 0$ and $v^{dc} = 0$ then Constraints (3.16) becomes $z_{ij}^{dc} \leq 0$, Constraints (3.17) becomes $z_{ij}^{dc} \leq 0$, Constraints (3.18) becomes $z_{ij}^{dc} \leq 0$ and Constraints (3.19) becomes $z_{ij}^{dc} \geq -2$. However, the value of z_{ij}^{dc} can not be negative as we know that z_{ij}^{dc} only takes 0 or positive values. Thus, Constraints (3.19) becomes $z_{ij}^{dc} \geq 0$. By Constraints (3.16), (3.17) and (3.17), $z_{ij}^{dc} \leq 0$. As a result the value of z_{ij}^{dc} becomes 0. When, $y_{ij}^d = 0$, $u^{dc} = 0$ and $v^{dc} = 1$, then Constraints (3.16) becomes $z_{ij}^{dc} \leq 0$, Constraints (3.17) becomes $z_{ij}^{dc} \leq 0$, Constraints (3.18) becomes $z_{ij}^{dc} \leq 1$ and Constraints (3.19) becomes $z_{ij}^{dc} \geq -1$. Again, the value of z_{ij}^{dc} can not be negative. Thus, Constraints (3.19) becomes $z_{ij}^{dc} \geq 0$. By Constraints (3.16) and (3.17) $z_{ij}^{dc} \leq 0$. Thus, the value of z_{ij}^{dc} is 0. All other combinations where, any one or two of the variables y_{ij}^d, u^{dc} and v^{dc} are 1, then by the same way as explained before, $z_{ij}^{dc} = 0$. When, $y_{ij}^d = 1$, $u^{dc} = 1$ and $v^{dc} = 1$ then Constraints (3.16) becomes $z_{ij}^{dc} \leq 1$, Constraints (3.17) becomes $z_{ij}^{dc} \leq 1$, Constraints (3.18) becomes $z_{ij}^{dc} \leq 1$ and Constraints (3.19) becomes $z_{ij}^{dc} \geq 1$. Thus, $z_{ij}^{dc} = 1$.

y_{ij}^{gd}	q^d	s_{ij}^{gd}
0	0	0
0	1	0
1	0	0
1	1	1

Table 3.2: Table for constraints (3.20), (3.21) and (3.22)

Constraints (3.20) - (3.22) are used to define the value of s_{ij}^{gd}. When, $y_{ij}^{gd} = 0$ and $q^d = 0$ then constraints (3.22) becomes $s_{ij}^{gd} \geq -1$. However, the value of s_{ij}^{gd} in constraint (3.22) can not be negative. Thus, $s_{ij}^{gd} \geq 0$. The value of s_{ij}^{gd} in constraint (3.21) is less than or equal to 0. As a result, s_{ij}^{gd} is 0. If $y_{ij}^{gd} = 0$ and $q^d = 1$, then constraint (3.22) becomes $s_{ij}^{gd} \geq 0$. The value of s_{ij}^{gd} in the constraint (3.20) is less than or equal to 0. As a result, the value of s_{ij}^{gd} is 0. Again, if $y_{ij}^{gd} = 1$ and $q^d = 0$, then Constraint (3.22) becomes $s_{ij}^{gd} \geq 0$. Howerer, the value of s_{ij}^{gd} in the constraint (3.21) is less than or equal to 0. Hence, the value of s_{ij}^{gd} is 0. When, $y_{ij}^{gd} = 1$ and $q^d = 1$, then Constraint (3.22) becomes $s_{ij}^{gd} \geq 1$. Though, the value of s_{ij}^{gd} in the constraint (3.20) and (3.21) are less than or equal to 1. Therefore, the value of s_{ij}^{gd} is 1.

3.6 Analysis of the ILP formulation

There are two kinds of variables in the ILP: binary variables and continuous variables. *ILP* formulation contains seven binary (0/1) variables, x_{ij}, y_{ij}^d, x_{ij}^g, y_{ij}^{gd}, q^d, u^{dc} and v^{dc}. In the network, there is $|E|$ number of edges or links. Therefore, the number of binary variable is $|E|$ for x_{ij}. As the number of binary variable, y_{ij}^d depends on number of disasters $|D|$ and number of edges $|E|$, the number of binary variables is $|E|.|D|$. If the number of gaps per edge or link is $|G|$ and there is $|E|$ edges, the number of binary variable x_{ij}^g would be $|G|.|E|$. The number of variables for y_{ij}^{gd} depends on the number of gaps($|G|$), the number of disasters ($|D|$) and the number of edges ($|E|$). Thus, the number of binary variable for y_{ij}^{gd} is $|G|.|D|.|E|$. By the same way, q^d depends on the number of disaster, $|D|$. So, q^d

has $|D|$ variables. u^{dc} and v^{dc} depend on the number of disaster D and the subcarriers C. Thus, both contain $|D|.|C|$ variables. Consequently, the total number of binary variables is $|E|$ + $|E|.|D|$+$|G|.|E|$+$|G|.|D|.|E|$+$|D|$+ 2.$|D|.|C|$.

There are two continuous variables; z_{ij}^{dc} and s_{ij}^{dg}. Both of these variables depend on the number of edges $|E|$, the number of disasters $|D|$, the number of gaps $|G|$ and the number of subcarriers $|C|$. Thus, the total number of variables are 2.$|E|.|D|.|G|.|C|$.

The number of constraints for equation (3.2) is the number of nodes $|N|$ in the network. The number of constraints for equation (3.3) is $|N|.|D|$. By this way, the total number of constraints for equation (3.2) to equation (3.22) is $|N|$ + $|D|$ + $|E|$ + $|N|.|D|$ + 2.$|E|.|D|$ + 2.$|E|.|G|$ + 2.$|E|.|G||D|$ + 4.$|D|.|C|$ + 7.$|D|.|C|.|E|$.

For example, let there is a network with 6 nodes, 18 edges and, 50 subcarriers and 5 gaps in each edge. Then 3 files are there in the replication strategy. There are 4 disasters. Thus, for x_{ij} the number of binary variable is 18, for y_{ij}^{d}, the number of variables is 72, and so on. The total number of binary variables is 18 + 72 + 90 + 360 + 4 + 400 = 944 and the total number of continuous variables is 36000. By the same way, the total number of constraints is 6 + 4 + 18 + 24 + 144 + 180 + 720 + 900 + 25200 = 27196.

Again, if the number of subcarriers is increased to 200, keeping all the other information the same as before, then the number of binary variables for x_{ij} is 18, for y_{ij}^{d}, the number of variables is 72, and so on. The total number of binary variables is 18 + 72 + 90 + 360 + 4 + 1600 = 2144 and the total number of continuous variables is 144000. Again, the total number of constraints is 6 + 4 + 18 + 24 + 144 + 180 + 720 + 3200 + 100800 = 105096.

Chapter 4

Experimental Results

In computer networking, simulation is an efficient technique that can be used to study and analyze the performance of a system. By using simulation, one does not need to set up the network physically. For evaluating the *ILP* formulation proposed in this thesis, we developed a suite of simulation tool including proper interfaces, which will be used to input files; and a script file, written in Python, which was used to automatically run repeated experiments.

As per our knowledge, no research work has been done to solve disaster resilient technique for *OFDM* networks. The primary objective of this simulation study was to evaluate our proposed ILP formulation. We have included several sets of experiments to study the efficiency of our formulation. For our experimental purposes, we worked with 6-node, 14-node, and 20-node networks. In a network, nodes are connected by edges. In our experiments, an edge between two nodes consists of two separate unidirectional optical fibers. For a given size of the network, we have generated 5 sets of random lists of requests for communication and have run all these lists with our simulation tools. We have utilized 50, 100, 150, 200, 250 and 300 as the number of subcarriers that can be handled by each fiber. Each of the connection requests consists of the file to be retrieved, the destination node (i.e. the requesting node) and the number of subcarriers required by that connection request. An example of a list of four requests is shown in the following table.

$FileNumber$	$DestinationNode$	$NumberofSubcarriers$
1	11	4
0	9	3
2	10	4
1	12	5

Table 4.1: A list of 4 requests

According to Table 4.1, the first row indicates that node 11 requested file number 1, and for such file transmission, 4 subcarriers would be required. Similarly, the second row indicates that file 0 was requested by node 9, and for this transmission, 3 subcarriers would be required. Each of the tests was considered subsequently with this pattern.

For a given size of the network and a given set of requests for communication, we have solved the problem of processing each request using our formulation. As a result, for each request for communication, we have received output results from *CPLEX*, which we used to update the corresponding network database. This database includes information about all existing communication, including the bandwidth used by the set of subcarriers corresponding to each communication in progress.

4.1 Experimental setups

We carried out experiments with *IBM ILOG CPLEX*. *CPLEX* [15] is a tool developed by IBM, which can be used to solve linear optimization problems, commonly known as *Linear Programming (LP)* problems, including integer linear programming. *CPLEX* can also be used for solving network flow problems, *quadratic programming (QP)* problem, *quadratically constrained programming (QCP)* and *mixed integer programming (MIP)* problems.

Figure 4.1 shows a flow diagram of the experimental setup. Before processing a list of requests for communication, we must initialize the program with the following input:

- The topology of the network (network information),
- Disaster information (nodes and edges affected by each disaster),

- Replication information (datacenter locations of each file), and
- Requests for communication

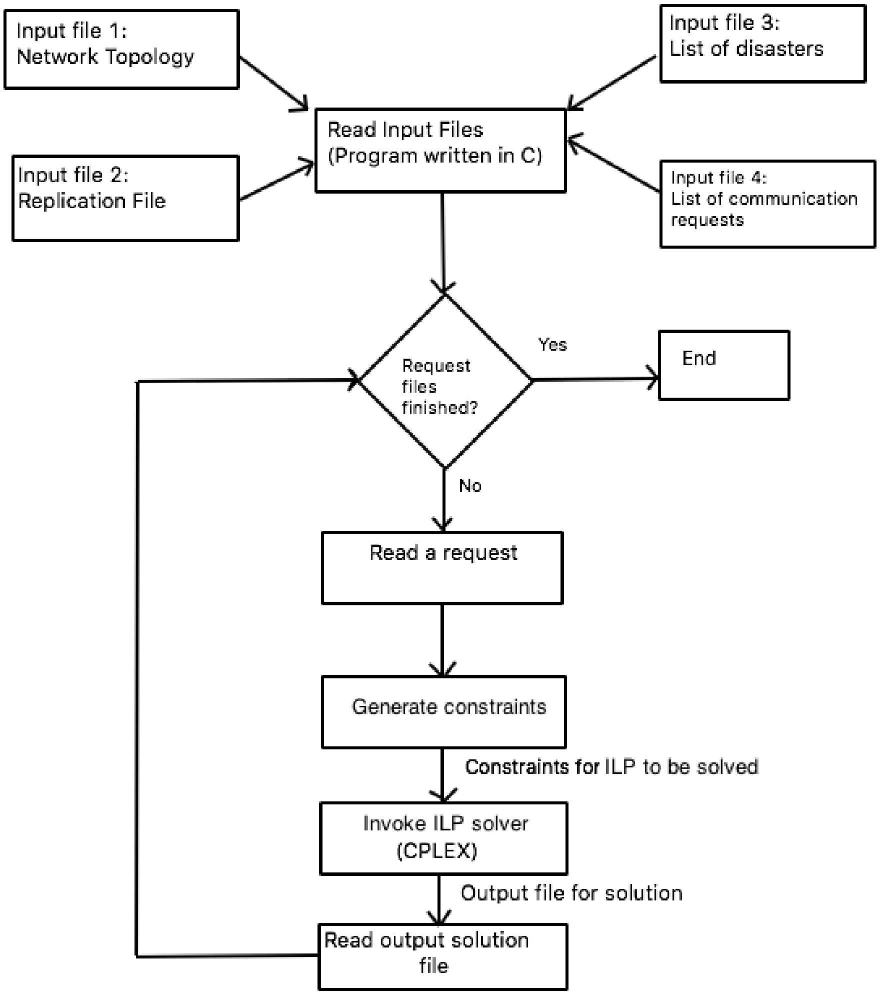

Fig. 4.1: Flow diagram for experimental setup

The file containing the requests for communication has many requests and the program continues to execute until all the requests are tried. This is indicated by the decision block, where 'no' indicates that the simulation will continue and 'yes' indicates the end of the experiment. If the decision is 'no', then an LP file containing all the constraints are generated for each request for communication. This *LP* file is sent to the *CPLEX LP* solver for processing, and the output file with the solution is created if possible. Thus, after a particular number of successfully completed requests, if there are not enough unused subcarriers available, the solution cannot be created by *CPLEX* for that particular request. Based on our experiments, we have realized that if the number of subcarriers increases, the average number of successful requests increases as well. In this way, as shown in the flow diagram in Figure 4.1, the process would go on until all the requests are tried.

4.2 Performance study

In the following Table 4.3, a summary of the input values for the variables is stated.

Variable name	Values
Number of nodes	6, 14, 20
Number of disasters	2, 3, 4
Number of subcarriers	50, 100, 150, 200, 250, 300
Number of files	3, 5, 7

Table 4.2: Summary of the input values for variables

During the experiments, we considered 6-node, 14-node and 20-node networks. For each network, the experiments were conducted where the number of subcarriers were increased from 50 to 300. When considering 6-node networks, we conducted our experiments by varying the number of disasters. In every experiment, we took 5 lists of randomly created requests for communication and calculated the averages of the time, the maximum number of successful requests and the blocking probability. Within any request-list, the number of requested files were distributed equally.

At the beginning of our experiments, we calculated the average times for a number of disasters. For this purpose, we conducted the experiments with a different numbers of disasters with 5 lists of 50 requests and calculated the following average times as output. During these experiments, we used a 6-node network, 3 files, and 50 subcarriers in each edge. The graph shown in Figure 4.2 indicates a linear relationship between these two variables.

From this graph, we found out that if the number of disasters increases, the average time also increases.

Number of disasters	Average time
2	4.02
3	10.02
4	16.43

Table 4.3: Relation between number of disaster and average time

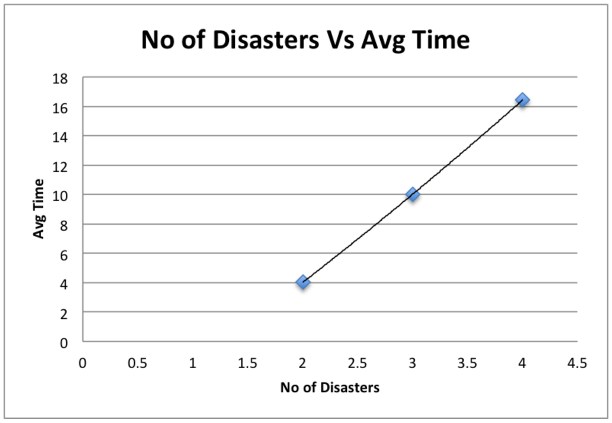

Fig. 4.2: Number of disaster vs average time

Figures 4.3, 4.4, 4.5 show how the number of requests affects the average time for successfully complete each request for communication when the number of subcarriers is 50, 100, 150, 200, 250 and 300. In this study, we took 20-node networks, with 5 possible disasters, 4 datacenters and 5 lists of requests with 50 requests per list. In Figure 4.3 (a), the average time to calculate both the primary path for disaster-free situation and the backup paths for the disaster situation varied from 35 second to 70 seconds. In Figure 4.3 (b), the average times varied from 100 seconds to 200 seconds. In Figure 4.4 (a), the average times varied from 200 seconds to 400 seconds. In Figure 4.4 (b), the average times varied from 300 seconds to 500 seconds. In Figure 4.5 (a), the average times varied from 400 seconds to 800 seconds, and in Figure 4.5 (b), the average times varied from 600 seconds to 1200 seconds. From all these 6 Figures, we can conclude that with the increase of number of subcarriers, the corresponding average times also increases.

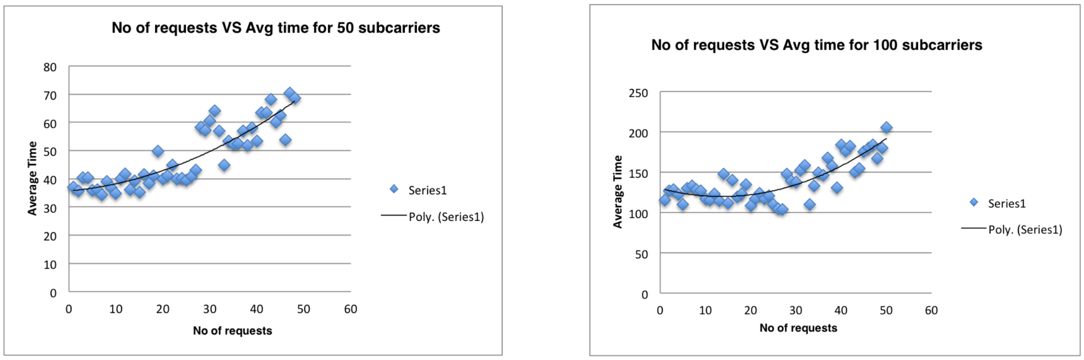

Fig. 4.3: Number of requests vs average time for (a) 50 subcarriers (b) 100 subcarriers

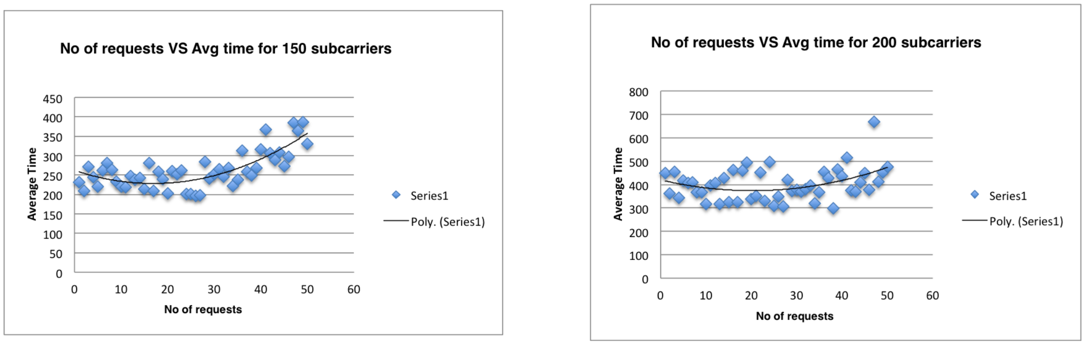

Fig. 4.4: Number of requests vs average time for (a)150 subcarriers (b) 200 subcarriers

Again, from Table 4.4 and Figure 4.6, the graphs show that the average times increase as the corresponding number of subcarriers increases. Therefore, we can conclude that, if the network nodes and a number of datacenters are fixed, then the average time increases considerably if the number of subcarriers increases. Moreover, in our subsequent experiments, we increased the number of files from 3 to 5 and 7 and computed the average as indicated in the Table 4.5.

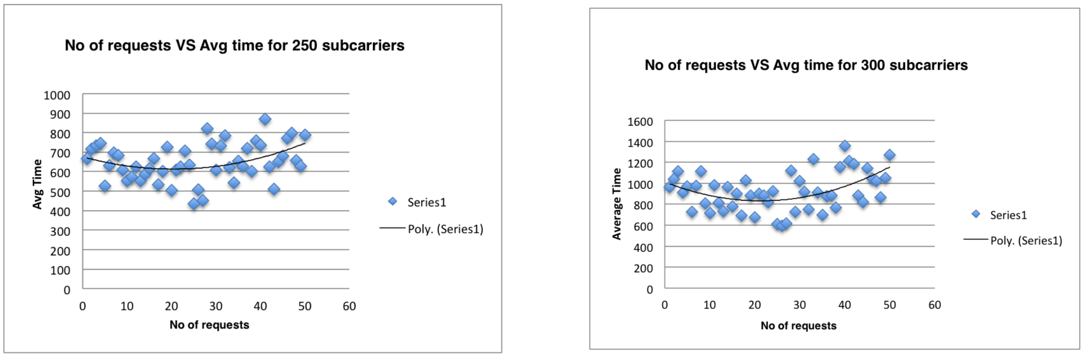

Fig. 4.5: Number of requests vs average time for (a)250 subcarriers (b) 300 subcarriers

Number of subcarriers	Average time
50	47.77
100	138.8
150	261.77
200	400.38
250	648.23
300	921.31

Table 4.4: Average time and number of subcarriers for number of file 3

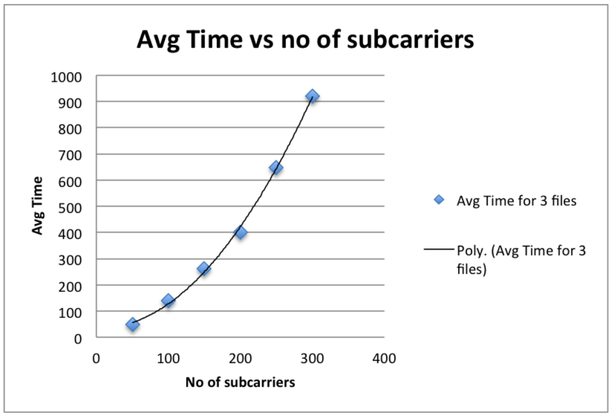

Fig. 4.6: Average time vs no of subcarriers for number of files, 3

We also conducted experiments by varying the number of files (i.e. 5, and 7). During these experiments with 3, 5, and 7 files, we made sure that, in the list of requests in all 5 request-files, all requesting files were distributed in such a way that the probability of appearing these files in our experiments were equal. For example, in 5 request-files, the average number of file 0 was 16, file 1 was 17 and file 2 was also 17. That indicated that the probability of appearing these request-files were equal for number of files 3. This is also true for files 5 and 7. Thus, we calculated the overall average times by considering the average times computed with number of file 3, 5, and 7 (see Table 4.5). Again, the relationship between these overall average times and number of subcarriers were shown in Figure 4.7.

No of subcarriers	Average time
50	61.17
100	144.52
150	251.11
200	374.59
250	576.44
300	730.6

Table 4.5: Average times by considering number of files 3, 5 and 7

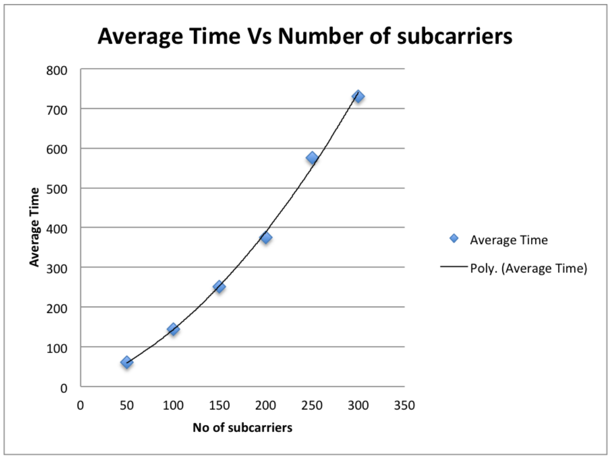

Fig. 4.7: Average time vs number of subcarriers

As indicated in Table 4.6, we calculated the maximum number of requests handled successfully when the number of subcarriers was 50, 100, 150, 200, 250 and 300. Here, we indicated a maximum number of successful requests as a threshold value. After this value, no other request was handled successfully. In other words, after this threshold point, no more subcarriers was allocated and it became ‘saturated’. During these experiments, we considered a list of 70 requests for communication when each fiber or link could handle 50 subcarriers, 120 requests for 100 subcarriers on each link, 170 requests for 150 subcarriers on each link, 220 requests for 200 subcarriers on each link, 270 requests for 250 subcarriers on each link and 320 requests for 300 subcarriers on each link. For each of these experiments, we took 5 lists of requests and calculated the average maximum number of requests or requests to get more accurate results. Figure 4.8 indicates a linear increase of the maximum number of successful requests. As expected, if the number of subcarriers on each link increases, the total maximum number of successful requests also increase.

Number of subcarriers	Max number of requests
50	56
100	104
150	164
200	211
250	263
300	318

Table 4.6: Number of subcarriers vs Max number of requests

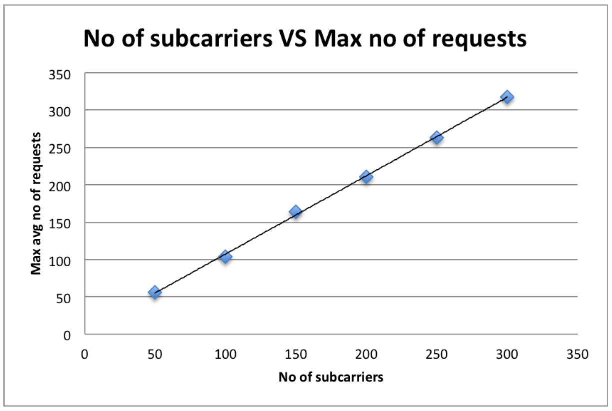

Fig. 4.8: Number of subcarriers vs Max number of requests

In dynamic lightpath allocation in optical networks, one of the key performance metrics is the blocking probability [22]. The blocking probability is the probability that a connection request would be denied due to unavailable resources. In the case of the *OFDM* network, this blocking probability can also be used for performance evaluation. Therefore, in the *OFDM* network, if we have total n requests and within those requests, $n1$ requests are rejected because of scarcity of subcarriers, then the blocking probability(P) is: $P = (\frac{n1}{n})$. When the number of subcarriers on each link was 50, we took 60 requests to calculate the blocking probability. In the same way, we took 110 requests for 100 subcarriers, 160 requests for 150 subcarriers and 210 requests for 200 subcarriers as shown in Table 4.7. We plotted these blocking probabilities with respect to number of subcarriers and obtained the results shown in Figure 4.9. Thus, we can conclude that, if the number of subcarriers increases, the blocking probability decreases.

Number of subcarriers	Total number of requests	Avg blocking probability
50	60	0.14
100	110	0.07
150	160	0.04
200	210	0.02

Table 4.7: Blocking probability

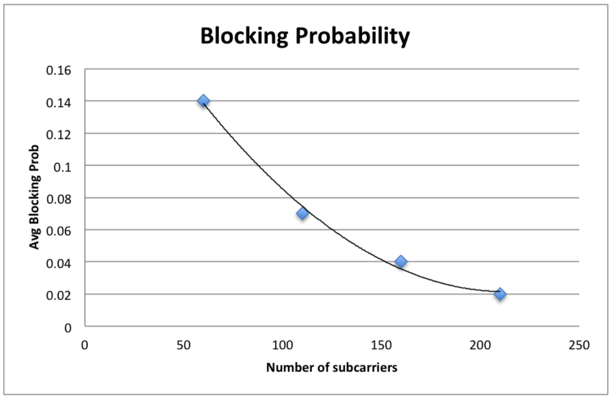

Fig. 4.9: Blocking probability

Chapter 5

Conclusions and Future Works

5.1 Conclusions

In this thesis, we have introduced a novel formulation to find a solution to minimize the resources needed to handle requests dynamically for communication in both disaster-free situations and when a disaster happens. We measured the resources used to handle the new request by the total number of remaining subcarriers, which are not needed by any of the existing communication. In the case of all the subcarriers already used by any existing communication for disaster free situations, no other communication including disaster-free situations and disaster situations can use these subcarriers any more. In case a disaster happens, the bandwidth cannot be used by any subcarriers for disaster-free communication. However, as we take the initial assumption that no two disasters can happen at the same time, if a subcarrier is used to handle some other disasters, this subcarrier can also be used to handle this disaster. As a result, by sharing the subcarriers, our proposed formulation is efficient in minimizing the resources needed to handle requests for *OFDM* networks.

We have analyzed our ILP formulation with respect to the size and the number of binary and continuous variables. We carried out an extensive study and analysis of the performances depending on different types of variables are performed in this research. We have performed the analysis with respect to the following experiments:

- Conducted experiments with 6-node, 14-node, and 20-node networks

- Studied the effects of various numbers of files in datacenters with respect to average time

- Analyzed the average time change varying the number of subcarriers

- Evaluated the average time change varying the number of nodes

- Explored the average time change varying the number of disasters

- Calculated and analyzed the blocking probabilities

By conducting the above experiments, we demonstrated the feasibility of the formulation and measured the performance with respect to average time and blocking probabilities. As we mentioned before, to the best of our knowledge, no prior work is done in our field of research; our work would be a good start for designing disaster-resilient networks and analyzing the performances.

5.2 Future Works

Disaster protection techniques are most important for current datacenters and above all cloud computing. At the same time, *OFDM* networks offer a huge efficiency gain in terms of spectrum utilization. Considerable work has been done covering RSA in *OFDM* networks. To the best of our knowledge, we are the first to introduce this disaster protection technique in *OFDM* networks for datacenters. Our ILP formulation is unable to handle networks having more than 20 nodes. Moreover, as we discussed in Chapter 3, the average time required to solve our ILP formulation increases with the increase in number of subcarrriers. As indicated in Chapter 4, we have conducted experiments with at most 300 subcarriers. But for any practical environment, the number of subcarriers would be substantially higher than 300. As a result, it could be a good future direction for exploration to develop fast heuristics for practical-sized subcarrier-numbers.

The average time for our work directly linked with average time required for *RSA* in *OFDM* network. As the network size increases, it also increases the time for managing *RSA*. Thus, this could be another possible future avenue of study in this field.

Bibliography

[1] Bandyopadhyay, S.: Disssemination of Information in Optical Networks: From Technology to Algorithms. Springer, 2008.

[2] Zhang, J., Lv, C., Zhao, Y., Chen, B., Li, X., Huang, S., Gu, W.:. A novel shared-path protection algorithm with correlated risk against multiple failures in flexible bandwidth optical networks. Optical Fiber Technology 18 (2012) 532-540.

[3] Shao, X., Yeo, Y., Xu, Z., Cheng, X., Zhou, L.: Shared-Path Protection in OFDM-based Optical Networks with Elastic Bandwidth Allocation. OFC/NFOEC Technical Digest (2012).

[4] Wikipedia: Datacenter wikipedia, the free encyclopedia (2016) [Online: accessed 3rd July 2016]. $[https://en.wikipedia.org/wiki/Data_center]$

[5] Wikipedia: 2008 Sichuan earthquake wikipedia, the free encyclopedia (2016) [Online: accessed 1rd July 2016]. $[https://en.wikipedia.orgwiki2008_Sichuan_earthquake]$

[6] G. Shen, Y. Wei, Q. Yang, Shared Backup Path Protection (SBPP) in Elastic Optical Transport Networks. Asia Communications and Photonics (2012).

[7] Liu, M., Tornatore, M., and Mukherjee, B.: Survivable traffic grooming in elastic optical networks Shared path protection, 2012 IEEE International Conference on Communications (ICC), (June, 2012), 6230-6234.

[8] Habib, M. F., Tornatore, M., Leenheer M. De, Dikbiyik, F. and Mukherjee, B.: Design of Disaster-Resilient Optical Datacenter Networks, Journal of Lightwave Technology, vol 30, number 16 (Aug, 2012), 2563-2573.

[9] Banerjee, S., Shirazipourazad, S., and Sen, A.,: ?Design and analysis of networks with large components in presence of region-based faults,? in Communications (ICC), 2011 IEEE International Conference on, pp. 1?6, IEEE, 2011.

[10] Zhang, G., Leenheer, M., Morea, A., Mukherjee, B.:. A survey on OFDM-based elastic core optical networking. IEEE communications surveys & tutorials (First 2013) 65-87.

[11] Ferdousi, S., Dikbiyik, F., Leenheer, Habib, M. F., Tornatore, M., Mukherjee, B.:. Disaster-aware datacenter placement and dynamic content management in cloud networks. IEEE/OSA Journal of Optical Communications and Networking, vol 7, issue 7 (July, 2015) 681-694.

[12] Savas, S. S., Dikbiyik, Habib, M. F., Tornatore, M., Mukherjee, B.:. Disaster-aware service provisioning with manycasting in cloud networks. Photonic Network Communications, Volume 28, Issue 2, October 2014, 123-134.

[13] F. Dikbiyik, F., Tornatore, M. and Mukherjee, B.,: Minimizing the Risk From Disaster Failures in Optical Backbone Networks, Journal of Lightwave Technology, vol. 32, no. 18, (Sept, 2014), pp. 3175-3183.

[14] Mukherjee, B., Habib, M. F., and Dikbiyik, F.,: Network adaptability from disaster disruptions and cascading failures. IEEE Communications Magazine, vol. 52, no. 5, (May 2014), pp. 230-238.

[15] IBM: Ilog cplex: High-performance software for mathematical programming and optimization. http://www-01.ibm.com/software/commerce/optimization/cplex-optimizer/. [Online: Accessed on 2nd of July, 2016].

[16] Ahuja, R.K., Magnanti, T.L., Orlin, J.B.: Network flows: theory, algorithms, and applications, 1993.

[17] Yuan, S., Jue, J.: Dynamic lightpaht protection in WDM mesh networks under wavelength-continuity and risk-disjoint constraints. Elsevier, Computer Networks 48, pp 91-112, (2005).

[18] Christodoulopoulos, K., Tomkos, I., and Varvarigos, E. A.: Routing and Spectrum Allocation in OFDM-Based Optical Networks with Elastic Bandwidth Allocation. Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE, Miami, FL, 2010, pp. 1-6.

[19] Christodoulopoulos, K., Tomkos, I., and Varvarigos, E. A.: Elastic Bandwidth Allocation in Flexible OFDM-Based Optical Networks. Journal of Lightwave Technology (2011), Vol. 29, Issue 9, pp. 1354-1366 (2011).

[20] Sterbenz, J. P. G., Hutchison, D, Çetinkaya, E. K., Jabbar, A and Rohrer, J. P. and Schöller, M. and Smith, P.: Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines. Computer Networks: The International Journal of Computer and Telecommunications Networking archive vol 54 issue 8, June, 2010,pp 1245-1265

[21] International Telecommunications Union: The world in 2013: ICT facts and figures. [https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2013-e.pdf] [Online: Accessed on 7th of July, 2016].

[22] Lu, K., Xiao, G. and Chlamtac, I.: Blocking analysis of dynamic lightpath establishment in wavelength-routed networks. ICC 2002. IEEE International Conference on Communications, 2002, (2002), pp. 2912-2916 vol.5.

[23] Velasco, L., Castro, A., Ruiz, M. and Junyent, G.: Solving Routing and Spectrum Allocation Related Optimization Problems: From Off-Line to In-Operation Flexgrid Network Planning. Journal of Lightwave Technology, vol. 32, no. 16, pp. 2780-2795, Aug.15, 15 2014.

[24] Takagi, T., Hasegawa, H., Sato, K., Sone, Y., Kozicki, B., Hirano, A., Jinno, M.: Dynamic routing and frequency slot assignment for elastic optical path networks that adopt distance adaptive modulation. Optical Fiber Communication Conference and Exposition (OFC/NFOEC), 2011 and the National Fiber Optic Engineers Conference. (March 2011) pp. 1-3.

[25] Shirazipourazad, S., Zhou, C., Derakhshandeh, Z., Sen, A.: On routing and spectrum allocation in spectrum-sliced optical networks. INFOCOM, 2013 Proceedings IEEE. (April 2013) 385-389.

VITA AUCTORIS

Sayeed Ahmed completed his Bachelors Degree in Computer Science and Engineering from the Bangladesh University of Engineering and Technology, Bangladesh, in the year 2002. He completed a masters degree from University of Wollongong, Australia in 2004. He was a Lecturer at Stamford University, Bangladesh and also later, held the position of Assistant Professor at University of Asia Pacific, Bangladesh. He worked in numerous positions as software engineer in Bangladesh, Australia and Canada. He also worked as a computer engineer at the Ministry of Interior, Kuwait. His research interests include Computer Networking, Optical fiber networks, Sensor Networking, Pattern Recognition, Machine Learning, and Artificial Intelligence. He is currently a candidate for the Masters degree in Computer Science at the University of Windsor, Ontario and hopes to graduate in Spring 2016.