Failure Localization Aware Protection in All-Optical Networks

by

Raisa Ohana da Costa Hirafuji

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Master of Applied Science
in
Electrical and Computer Engineering

Waterloo, Ontario, Canada, 2020

Author's Declaration

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Abstract

The recent development of optical signal processing and switching makes the all-optical networks a potential candidate for the underlying transmission system in the near future. However, despite its higher transmission data rate and efficiency, the lack of optical-electro-optical (OEO) conversions makes fault management a challenge. A single fiber cut can interrupt several connections, disrupting many services which results in a massive loss of data. With the ever growing demand for time-sensitive applications, the ability to maintain service continuity in communication networks has only been growing in importance. In order to guarantee network survivability, fast fault localization and fault recovery are essential.

Conventional monitoring-trail (m-trail) based schemes can unambiguously localize link failures. However, the deployment of m-trail requires extra transceivers and wavelengths dedicated to monitoring the link state. Non-negligible overhead makes m-trail schemes neither scalable nor practicable. In this thesis, we propose two Failure Localization Aware (FLA) routing schemes to aid failure localization. When a link fails, all traversing lightpaths become dark, and the transceiver at the end node of each interrupted ligthpath issues an alarm signal to report the path failure. By correlating the information of all affected and unaffected paths, it is possible to narrow down the number of possible fault locations to just a few possible locations. However, without the assistance of dedicated supervisory lightpaths, and based solely on the alarm generated by the interrupted lightpaths, ambiguity in failure localization may be unavoidable. Hence, we design a Failure Localization Aware Routing and Wavelength Assignment (FLA-RWA) scheme, the Least Ambiguous Path (LAP) routing scheme, to dynamically allocate connection requests with minimum ambiguity in the localization of a link failure. The performance of the proposed heuristic is evaluated and compared with traditional RWA algorithms via network simulations. The results show that the proposed LAP algorithm achieves the lowest ambiguity among all examined schemes, at the cost of slightly higher wavelength consumption than the alternate shortest path scheme.

We also propose a Failure Localization Aware Protection (FLA-P) scheme that is based on the idea of also monitoring the protection paths in a system with path protection for failure localization. The Least Ambiguous Protection Path (LAPP) routing algorithm arranges the protection path routes with the objective of minimizing the ambiguity in failure localization. We evaluate and compare the ambiguity in fault localization when monitoring only the working paths and when monitoring both working and protection paths. We also compare the performance of protection paths with different schemes in regards to fault localization.

Acknowledgements

I would like to thank my supervisor, Prof. Pin-Han Ho, for all his support and guidance throughout my time as a graduate student in the University of Waterloo.

I would like to thank Prof. Bingbing Li, for all the help and support she gave me these past couple years.

I would like to thank my family, for their continuous support throughout my life.

I would like to thank all my colleagues, all my instructors and the ECE staff for all the help they have been giving me.

Finally, I cannot thank enough the front-line workers that are fighting the COVID-19 pandemic.

Without the support of any of these people, this thesis would not have been possible.

Dedication

This thesis is dedicated to my beloved parents.

Table of Contents

List of Figures

List of Tables

List of Abbreviations

m-cycle monitoring cycle 11–15

m-link link-based monitoring 11

m-trail monitoring trail 14–17, 22, 23, 32, 49, 50

AFL adjacent-link failure localization 17

AR adaptive routing 6

ASP alternate shortest-path 6, 26–29, 31–34, 49

BFST breadth-first spanning-tree 12

DFS depth first searching 12

FAR fixed-alternate routing 6

FF first fit 7, 26, 38, 42

FLA failure localization aware 49, 50

FLA-P failure localization aware protection 3, 36, 37, 42

FLA-RWA failure localization aware routing and wavelength assignment 3, 22, 23, 26, 49

FR fixed routing 6

FSP fixed shortest-path 6

GBC Graph-Based Correlation 9, 10

HDFS heuristic depth first searching 12

HST heuristic spanning-tree 12, 13

ILP integer linear program 5, 10, 15

IS-IS intermediate system to intermediate system 7

KSP k-shortest paths 23–26, 37, 49

LAP least ambiguous path 3, 22–34, 49

LAPP Least ambiguous protection path 3, 37, 42–47, 49

LCP least-congested path 6, 26–28, 31–34, 49

LCPP Least congested protection path 37, 42–44, 46, 47, 50

LOL loss of light 7, 10, 35

LU least-used 7, 26

ML machine learning 5

MTA monitoring trail allocation 15, 16

MTBF mean time between failures 10, 27, 38, 42

MU most-used 7

nonsimple m-cycle *nonsimple* monitoring cycle 13, 14

OEO optical-electro-optical 1, 2, 4

OSPF open shortest path first 7

OXC optical crossconnect 21

RCA random code assignment 15

RCS random code swapping 15, 17

RF random fit 7

RWA routing and wavelength assignment 3–6, 22, 23, 26, 28

SP shortest path 22, 23

SPEM shortest path Eulerian matching 12

SPP Shortest protection path 36–38, 42–47, 50

SRLG shared risk link group 17

UFL unambiguous failure localization 11–15, 28, 39, 49, 50

WDM wavelength division multiplexing 4, 21, 22

List of Symbols

$A'_{i,j}$ Set of the links traversed by at least one path unaffected by a fault at link (i, j). 24, 25

$A_{i,j}$ Set of the links traversed by all paths affected by a fault at link (i, j). 24, 25

E' Set of links in the network traversed by at least one lightpath. 24, 25

E Set of links for a network physical topology represented as $G(V, E)$. 23, 26, 36

H^k_{sd} Number of hops in pp^i_{sd}. 36, 37

Λ_{ij} Number of free wavelength slots in link (i, j). 37

$P'_{i,j}$ Set of all paths unaffected by a failure at link (i, j). 24

PPT Routing table for protection paths. 36

PP_{sd} Set of candidate protection path for an FLA-P scheme. 36

$P_{i,j}$ Set of all paths affected by a failure at link (i, j). 24

P_{sd} Set of k-shortest alternate paths from s to d, where $s, d \in V$. 23–26

$S_{i,j}$ Set of suspect locations for a network fault in link (i, j). 24

V Set of nodes for a network physical topology represented as $G(V, E)$. 23, 26, 36

WPT Routing table for working paths. 24–26, 36

WP_{sd} Set of candidate working path for an FLA-P scheme. 36

W Set of wavelengths in a link. 23, 26, 36

bw Bandwidth demand in number of wavelength slots. 23–26, 36

d Destination node. 23–26, 36, 37

γ Cost ratio. Determines the relative importance between monitor cost and bandwidth cost. 11

λ Arrival rate. 27, 38, 42

ω_{sd}^{i} Weight for the i-th candidate protection path in the set PP_{sd}. 36, 37

p_{sd}^{i} i-th path in the set P_{sd}. 24

pp_{sd}^{i} i-th candidate protection path in the set PP_{sd}. 37

p Path. 23

ρ Network load. 27

r Connection request from source node s to destination node d with the bandwidth demand bw in number of wavelengths. 23–26, 36

s Source node. 23–26, 36, 37

$\left|A'_{i,j}\right|$ Number of links in set $A'_{i,j}$. 25

$\left|A_{i,j}\right|$ Number of links in set $A_{i,j}$. 25

$|E'|$ Number of links in set E'. 24

$\left|S_{i,j}\right|$ Number of links in set $S_{i,j}$. 24, 25

Chapter 1

Introduction

1.1 Motivations

Today's world is more connected than ever. With more and more people working from home, video-conferences and video streaming services have been growing in popularity. Designing network architectures capable of maintaining service continuity at all times is not only important, but also challenging. A common requirement for network availability is for a connection to be available 99.999% of the time [51], which is equivalent to having a downtime of less than 5 minutes per year. As faults are inevitable, and often caused by human error, it is important to design systems capable of fault localization and fault recovery. In optical networks, the most common reason for a link failure are fiber cuts. It is estimates that long-haul networks have an annually average of 3 fiber cuts per 1000 miles of fiber [20].

Most of today's data are transported through optical networks as they are capable of carrying large amounts of data. As the demand for higher bandwidths only increases, it is expected for future optical networks to transmit even more data. Thus, a single fiber cut can result in the loss of huge amounts of data, which can lead to the loss of millions of dollars for the users and network operators [33]. In order to minimize a network's downtime, it is necessary to detect, identify and locate any fault that occurs and to restore any interrupted service.

Fault detection and fault location strategies can be vastly different for distinct network architectures. An optical network architecture can be either opaque or transparent. Opaque optical networks need to do optical-electro-optical (OEO) conversions at certain

places in the network, whereas transparent optical networks only have optical components and do not need any OEO conversions [31]. Transparent optical networks have a higher flexibility and lower costs, as it eliminates expensive and useless OEO conversions. However, the OEO conversions allow a closer monitoring of the signal quality and they also allow frequent signal regeneration. Consequently, detecting and locating faults in opaque networks can be very simple [37]. Transparent optical networks, on the other hand, are more susceptible to the restrictions of fiber transmission, such as attenuation and non-linearities, and to signal degradation due to soft failures, such as fiber bending. Consequently, faults in transparent optical networks are harder to detect and locate [29].

In order to monitor the network for any faults, transparent optical networks require additional monitoring equipment, as the optical signal is only converted to the electric domain at the end of the lightpath. In general, whenever there is any unexpected event, any device capable of detecting and reporting such event will send an alarm. For a single link failure, all lightpaths traversing the failed link will be interrupted. This may trigger hundreds of alarms, most of which are redundant. It is unfeasible for the network operator to deal with so many alarms in a timely manner. Not only that, but there are also many false alarms that corresponds to no fault at all. There are several studies on how to deal with large amounts of alarms [18, 57, 56].

A solution to the aforementioned problems is to use dedicated supervisory channels to monitor the network. By carefully choosing the route of the supervisory channels, it is possible to not only reduce the amount of monitors in the network, but to also accurately locate any failed link [62, 70, 79, 80]. However, for networks with a large topology, a significant portion of the network bandwidth needs to be allocated just for monitoring.

In short, locating a network fault in transparent optical networks is not trivial, and as networks architectures grow in complexity, it will only get more difficult. In order to efficiently locate any network fault, a novel framework for fault localization is of utmost importance.

1.2 Contribution

In this work we have three main contributions. First we define the *ambiguity* in failure localization. Based on our definition, we present a set of equations to calculate the ambiguity. Secondly, we propose routing schemes based on finding the least ambiguous path for both working paths and protection paths. Finally, we carry out simulation to evaluate the gains and trade-off from the proposed schemes.

1.3 Organization

This work is organized as follows. In chapter 2 we review important concepts on routing and wavelength assignment (RWA) methods, fault localization schemes and fault recovery mechanisms. In chapter 3 we present a failure localization aware routing and wavelength assignment (FLA-RWA) scheme: the least ambiguous path (LAP) algorithm. Chapter 4 presents a failure localization aware protection (FLA-P) scheme, the Least ambiguous protection path (LAPP) algorithm. Finally, in chapter 5 we summarize and discuss our findings, and we also present an outline for future works.

Chapter 2

Background and Literature Review

2.1 Routing and Wavelength Assignment (RWA)

The wavelength division multiplexing (WDM) technology allows multiplexing several wavelength channels on the same fiber, greatly improving the network capacity. Fig. 2.1 illustrates this by showing the paths $(0 \rightarrow 2)$ and $(0 \rightarrow 2 \rightarrow 4)$ being able to traverse the link $(0, 2)$ at the same time, by using different wavelengths (λ_1 and λ_0, respectively). However, this technology also imposes a very unique constraint on transparent optical networks. Without OEO conversions or wavelength converters, a lightpath must occupy the same wavelength slot throughout all links it traverses. This is known as the wavelength-continuity constraint.

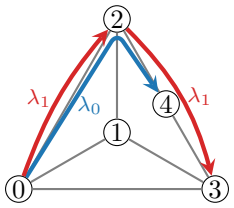
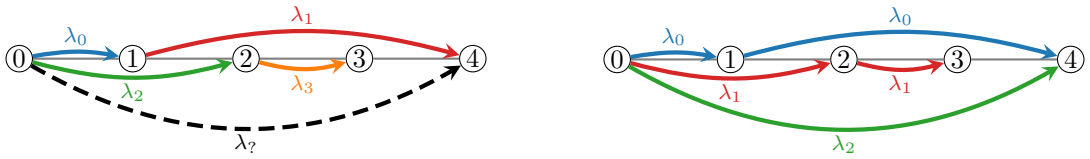


Figure 2.1: Example of distinct lightpaths using different wavelengths to traverse the same links in a WDM network.

This unique constraint imposes an extra challenge on the routing and wavelength assignment (RWA) process. Establishing a lightpath between the source and destination nodes is more than just finding a route. A poorly planned wavelength assignment can result in request being blocked even though the network has more than enough available

bandwidth. Fig. 2.2 shows a network without wavelength converters and 4 available wavelengths (λ_0, λ_1, λ_2 and λ_3). In Fig. 2.2a, the paths $(0 \to 1)$, $(1 \to 2 \to 3 \to 4)$, $(0 \to 1 \to 2)$ and $(2 \to 3)$ are each assigned to a different wavelength, and when a connection request from node 0 to node 4 arrives, there is simply no single wavelength that is available in all links between 0 and 4. Even though each link is occupied only up to half capacity, and the network has more than double of the required bandwidth available, due to a poorly planned wavelength assignment the connection request is blocked. Fig. 2.2b shows the same network with the same paths, but with a different wavelength allocation. Now the paths $(0 \to 1)$ and $(1 \to 2 \to 3 \to 4)$ are allocated to the wavelength λ_0, and the paths $(0 \to 1 \to 2)$ and $(2 \to 3)$ are allocated to the wavelength λ_1. For the connection request from node 0 to node 4, there are two wavelengths available in all links traversed by this path, λ_2 and λ_3. This example illustrates how the wavelength-continuity constraint can increase the blocking probability, and how important it is to either have wavelengths converters or to work around this constraint. There have been several studies on this subject. In [4] the author model the blocking probability with no wavelength converters, and they show that the blocking probability increases drastically for routes with many hops.



(a) Request from 0 to 4 blocked.

(b) Request from 0 to 4 allocated to λ_2.

Figure 2.2: Example of how wavelength assignment can increase or avoid blocked requests in a network without wavelength converters.

The RWA problem can be classified according to how the connection requests arrive. The request arrivals can be static, incremental or dynamic [19]. For static traffic, all requests are already known and will not be changed while the network is in operation. The static RWA problem usually deals with fitting all the connection requests while minimizing the use of network resources, such as wavelengths and number of fibers. Static traffic presents connection requests in the form of a traffic matrix, that specifies the bandwidth demands for each source-destination pair in the network. The static RWA problem can be formulated as an integer linear program (ILP), which has an NP-complete computational complexity [39]. There are several studies on solving the RWA problem via ILP [27], however, due to the high computational complexity, these solutions are only feasible for small scale networks. Recent studies tried to solve this issue by using supervised machine learning (ML) techniques to solve the optimization problem faster [34, 35].

For the incremental traffic, the connection requests arrive one at a time, and once the lightpath is established, it remains in the system indefinitely. For the dynamic traffic, the lightpaths are established as the connection requests arrive, and differently from the incremental traffic, the lightpaths are released after some finite amount of time. Usually, the goal of solving the dynamic RWA problem is to allocate the lightpaths while minimizing the chance that upcoming requests are blocked. Recent approaches to solving the dynamic RWA problem include the use of state-of-the-art reinforcement learning algorithms [48, 55, 73, 75]. In this work we will be focusing on dynamic RWA.

2.1.1 Routing

There are three basic approaches to the routing subproblem [78]:

Fixed routing (FR)

Each source-destination pair are always assigned the same fixed route. An example of this approach is the fixed shortest-path (FSP), where the shortest-path is calculated offline.

Fixed-alternate routing (FAR)

Each source-destination pair has K pre-defined routes from which only one will be chosen for a connection request. An example for these alternate routes would be using the K-shortest paths as alternate routes. The primary route is the shortest-path, and all alternate route are link-disjoint from the primary path. This scheme is known as alternate shortest-path (ASP) routing.

Adaptive routing (AR)

The route is chosen dynamically depending on the link state. An example of this approach is the least-congested path (LCP) routing [8]. Similarly to the FAR approach, the LCP has a set of pre-determined routes, and chooses one of the routes based on which route has the least-congested link. Link congestion here is determined by the number of occupied wavelengths in one link. The least-congested link is the link with most available wavelengths.

2.1.2 Wavelength Assignment

After choosing a route, the following heuristic can be used for wavelength assignment:

- Random fit (RF): Selects a random wavelength from the feasible wavelengths.
- First fit (FF): Selects the first viable wavelength from an ordered list of wavelengths.
- Most-used (MU)/PACK: Selects the most-used available wavelength.
- Least-used (LU)/SPREAD: Selects the least-used available wavelength.

These are just some examples. There are several more schemes in the literature [39].

2.2 Fault Localization

Fault localization is the process finding a fault source based on observed failure indications [32]. There are two kinds of faults: *soft* and *hard*. Soft faults, such as fiber bending, only cause degradation of the signal quality. Hard faults, such as a fiber cut, cause complete signal interruption. On this work, the focus is on hard faults, where there is complete loss of light (LOL).

Fault monitoring can be done either in the upper layers or the lower layers. The main advantage of doing it in the physical layer is that it allows faster link failure localization. In the IP layer, most routing protocols, such as the open shortest path first (OSPF) and intermediate system to intermediate system (IS-IS), can detect link failures [22].

Alarm is probably one of the most important concepts in network fault management, as such, a proper definition is of utmost importance. In [36], alarms are defined as messages that network components send to the system manager to inform of abnormal conditions. One of the challenges that may arise in fault management lies in the fact that we will not always be in the ideal scenario where all alarms are correctly generated and safely delivered. It is possible to have missing alarms and false alarms. Missing alarms, are just alarms that did not arrive to the network operator. False alarms are alarms that are sent even though there is no network fault.

In [24], the authors classifies monitoring schemes in two main categories: in-band monitoring and out-of-band monitoring. In-band monitoring consists on monitoring the established lightpaths in the network [45], whereas out-of-band monitoring consists on deploying

a dedicated supervisory lightpath to monitor the network [79, 80]. It is also possible to use both operation lightpaths and out-of-band supervisory lightpaths to localize link failure.

In [45] the authors propose a minimal monitor activation with dynamic lightpaths. The monitors are initially placed in every possible location to achieve maximum coverage. Based on which lightpaths each set of monitors (referred as *Domain*) can monitor, an alarm matrix is generated, as illustrated in Table 2.1. In order to minimize the number of monitors, such that there is at least one alarm if any components fails and every component activates an unique alarm upon failure, the authors use an approximation algorithm [41]. The goal of the algorithm is to reduce the columns of the alarm matrix, maintaining all rows distinct and non-zero (see Table 2.2). Each column in the alarm matrix is assigned a weight called *hit value*, and the column with the highest value is considered a local best. The hit values are calculated as follows: (i) a given weight is assigned to a column to avoid an all 0 row; (ii) rows with the same binary pattern are grouped together.

- A weight of R1 is given to a column to avoid having an all 0 row;
- Rows with the same binary patterns are grouped together

As such, the proposed scheme not only minimizes the number of monitoring devices, but it is also capable of dealing with changes in the network topology by turning ON/OFF some monitoring equipment. It locate simultaneous faults and it is capable of dealing with missed and false alarms.

Node	M_1	M_2	M_3	M_4	M_5	M_6	M_7	M_8	M_9	M_{10}	M_{11}
ND_4	0	0	0	0	0	0	0	1	0	0	0
ND_5	1	1	0	0	0	1	0	1	1	0	0
ND_6	0	0	1	0	0	0	0	0	0	0	0
ND_7	0	0	1	0	1	0	0	0	0	1	1
ND_8	0	0	0	0	0	0	0	0	0	0	1
ND_{10}	0	1	0	1	0	1	1	1	1	0	0
ND_{13}	1	0	0	0	0	1	0	0	0	0	0

Table 2.1: Alarm matrix from [45]

2.2.1 In-Band Monitoring

In-band monitoring consists on monitoring established working lightpaths to locate failures in the network. In [57] the authors use the information from the established lightpaths to

	M_8	M_3	M_6	M_{11}	M_1
ND_4	1	0	0	0	0
ND_5	1	0	1	0	1
ND_6	0	1	0	0	0
ND_7	0	1	0	1	0
ND_8	0	0	0	1	0
ND_{10}	1	0	1	0	0
ND_{13}	0	0	1	0	1
RAL	1	0	1	0	0

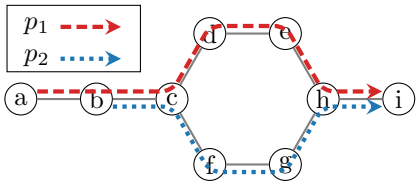
Table 2.2: Reduced alarm matrix from Table 2.1

find an optimum placement for monitors in the network. However, if there is any change in the established lightpaths, this solution would no longer be optimal.

Another approach for in-band monitoring is assuming that one has the full information of each link and each lightpath at any given time, and by monitoring the end point of the lightpath, it can correlate the generated alarms along overlapping lightpaths to narrow down the possible locations of a network fault [14].

For example, in Fig. 2.3a, we have two working lightpaths, p_1 and p_2. Lightpath p_1 connects nodes a and i via the path $(a \rightarrow b \rightarrow c \rightarrow d \rightarrow e \rightarrow h \rightarrow i)$, and an alarm from this lightpath means that a network fault could have occurred in any of the 6 links in the path. However, we also have lightpath p_2, that connects nodes b and i via the path $(b \rightarrow c \rightarrow f \rightarrow g \rightarrow h \rightarrow i)$. We can use the information from both the presence or absence of an alarm from p_2 to better locate the network fault. An alarm from both p_1 and p_2 means that the network fault is in a link shared by both lightpaths. Thus, in the example from Fig. 2.3a, it is in either link (b, c) or link (h, i). An alarm from only p_1 means that the fault is in a link in p_1 that is not in p_2. Hence, the fault could be in the links (c, d), (d, e) or (e, h). The table in Fig. 2.3b shows all possible interpretations for all combinations of alarms from p_1 and p_2.

In [46], the authors presented the Graph-Based Correlation (GBC) heuristic. It is a formal algorithm that correlates the presence or absence of alarms in order to obtain the possible locations for a network fault. Based on the received alarms, we separate the lightpaths into two categories, the affected paths and the unaffected paths. Then, we intersect the links in the affected paths in order to obtain the set of links that are present in every affected lightpath, as the failed link must be in all affected lightpaths to affect them. Next, we consider the set of all links that are in at least one unaffected path. We



(a)

p_1 ⇢	p_2 ⋯→	Possible fault locations
Alarm	Alarm	(b, c) and (h, i)
Alarm	No Alarm	(a, b), (c, d), (d, e) and (e, h)
No Alarm	Alarm	(c, f), (f, g) and (g, h)
No Alarm	No Alarm	No fault

(b)

Figure 2.3: (a) Example network topology and lightpaths from [14]; and (b) possible locations based on the presence or absence of alarms in p_1 and p_2

remove the links in the later set from the former, obtaining a set with the links that could be the fault location.

In the example in Fig. 2.3, it is impossible to accurately locate a link failure with just the alarms from p_1 and p_2. As the information from the working lightpaths may not provide enough information to find the exact location of the failed link, the authors in [14] proposes to find an optimum monitor placement via ILP [15] to further reduce the number of possible fault locations. For example, if we place a monitor in node c, the number of possible locations for the links between node c and h becomes 3, and for all other link it is 1.

Another possible approach to in-band monitoring is using the past failure information to teach a machine learning model where is the most probable location. Such approach is possible by exploiting the mean time between failures (MTBF). As such, the authors in [47], on top of using the GBC, trained a Gaussian process classifier on past data, and were able to achieve in their simulations an accuracy of 91%-99%.

2.2.2 Out-of-Band Monitoring

Out-of-band monitoring is characterized by the use of a dedicated supervisory lightpath and a network monitor. The monitor consists on an optical power detector that generates an alarm when there is LOL on the supervisory lightpath [57].

The objective when designing an out-of-band monitoring scheme, is to minimize the *monitoring cost*. The monitoring cost is given by:

$$\textit{Monitoring Cost} = \text{monitor cost} + \text{bandwidth cost} \tag{2.1}$$

where the monitor cost includes all the hardware costs, and the bandwidth cost is the cover length, i.e., the total number of supervisory wavelength-links required in the solution.

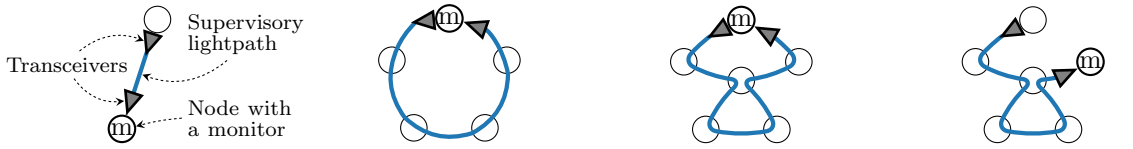
As such, we can rewrite eq. 2.1 as:

$$\textit{Monitoring Cost} = \gamma \times \text{number of monitors} + \text{cover length} \tag{2.2}$$

where γ is the *cost ratio* and determines the relative importance between monitor cost and bandwidth cost.

Link-based monitoring (*m*-link)

Link-based monitoring (*m*-link) is the most straightforward approach to out-of-band monitoring. It consists on setting a supervisory lightpath in each link, with a monitor on the receiver node (see Fig. 2.4a)[24]. Since every single link is being monitored, this scheme is always able to achieve unambiguous failure localization (UFL). The main disadvantage of this approach is the cost of having a dedicated monitor for each link in the network. For larger networks, the cost becomes prohibitive.



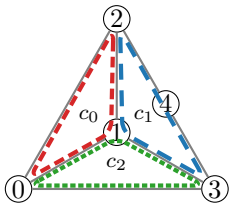
(a) An *m*-link. (b) An *m*-cycle. (c) A nonsimple *m*-cycle. (d) An *m*-trail.

Figure 2.4: Example of out-of-band monitoring schemes.

Monitoring cycle (*m*-cycle)

A *cycle* is a sequence of nodes connected by edges, in which every node connects to exactly two other nodes. A simple monitoring cycle (*m*-cycle) establishes the supervisory lightpath in the shape of a cycle, hence there are no repeated edges or nodes, and both transceivers and the monitor are on the same node (see Fig. 2.4b) [67].

For an *m*-cycle solution consisting of a set of M *m*-cycles $C = \{c_0, \ldots, c_{M-1}\}$, a link failure will disrupt every single *m*-cycle that passes through the failed link. All affected *m*-cycles will send an alarm, whereas the unaffected *m*-cycles will not send any alarm. Gathering all this information, we obtain a binary alarm code $[a_0, \ldots, a_{M-1}]$, where $a_i = 1$ if *m*-cycle c_i has been affected, and $a_i = 0$ otherwise. By comparing the obtained alarm code with the associative code for each link (see Fig. 2.5b), it is possible to determine



(a) M-cycle solution.

Link	c_2	c_1	c_0	Decimal
(0,1)	0	1	1	3
(0,2)	0	0	1	1
(0,3)	0	1	0	2
(1,2)	1	0	1	5
(1,3)	1	1	0	6
(2,4)	1	0	0	4
(3,4)	1	0	0	4

(b) Alarm code table.

Figure 2.5: Example of an m-cycle solution and its corresponding alarm code table.

which link has failed. The alarm code table, with all possible associative codes, is pre-established *offline* [81]. In order to achieve fault detection, Zeng et. al. proposed in [79] two algorithms to find the cycle cover: the Heuristic depth first searching (HDFS) and the Shortest path Eulerian matching (SPEM). Both algorithms assume that the network graph is bridgeless, i.e., it does not contain any link that when removed would disconnect the graph.

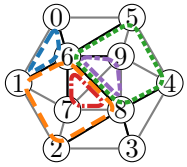
The HDFS algorithm models the network as a graph $G(V, E)$, where V is the set of vertices (network nodes) and E is the sets of edges (network links). A subgraph $G'(V', E')$ is created by traversing all links in E using the depth first searching (DFS) algorithm. While traversing the link (x, y), for $y \in E'$, there is a path $(y, \ldots, x) \in G'$. The link (x, y) and the path $(y, \ldots, x)$ forms a cycle. After traversing the graph until all links all covered by a cycle, the set of obtained cycles will form a cycle cover.

The SPEM algorithm adapts the network graph $G(V, E)$ into an Eulerian graph by finding the set V' of odd degree nodes and connecting them with the closest odd degree node. Once the network graph is an Eulerian graph, it is possible to find an Eulerian cycle that covers all links in the network. Then it is possible to form a cycle by traversing the Eulerian cycle until a node is re-visited. By removing the formed cycles and repeating this process until the Eulerian cycle is empty, the set of obtained cycles forms a cycle cover.

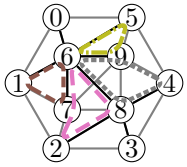
The aforementioned algorithms are able to find a cycle cover for bridgeless graphs, and although they achieve fault detection, they do not guarantee UFL. The authors in [80] propose a heuristic spanning-tree (HST) based m-cycle construction algorithm with a better performance in failure localization.

The HST algorithm consists on first constructing a spanning tree. Then, from each edge that is not in the spanning tree, we build a cycle where all other edges must be from the spanning tree. Among the several algorithms available to build a spanning tree, the authors in [80] chose the breadth-first spanning-tree (BFST) rooted from the node with

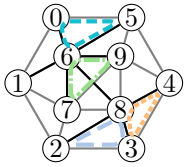
maximum degree, as it is the option that results in the use of less supervisory wavelengths per link. Fig. 2.6 shows an *m*-cycle solution for the SmallNet topology using the HST algorithm.



(a) c_0 ( ), c_1 ( ), c_2 ( ), c_3 ( ) and c_4 ( ).



(b) c_5 ( ), c_6 ( ), c_7 ( ) and c_8 ( ).



(c) c_9 ( ), c_{10} ( ), c_{11}( ) and c_{12}( ).

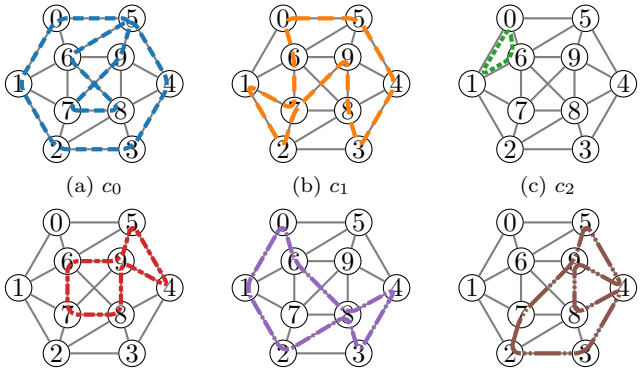
Link	c_{12}	c_{11}	c_{10}	c_9	c_8	c_7	c_6	c_5	c_4	c_3	c_2	c_1	c_0	Decimal
(0, 1)	0	0	0	0	0	0	0	0	0	0	0	0	1	1
(0, 5)	0	0	0	1	0	0	0	0	0	0	0	0	0	512
(0, 6)	0	0	0	1	0	0	0	0	0	0	0	0	1	513
(1, 2)	0	0	0	0	0	0	0	0	0	0	0	1	0	2
(1, 6)	0	0	0	0	0	0	0	1	0	0	0	1	1	35
(1, 7)	0	0	0	0	0	0	0	1	0	0	0	0	0	32
(2, 3)	0	0	1	0	0	0	0	0	0	0	0	0	0	1024
(2, 7)	0	0	0	0	0	0	1	0	0	0	0	0	0	64
(2, 8)	0	0	1	0	0	0	1	0	0	0	0	1	0	1090
(3, 4)	0	1	0	0	0	0	0	0	0	0	0	0	0	2048
(3, 8)	0	1	1	0	0	0	0	0	0	0	0	0	0	3072
(4, 5)	0	0	0	0	0	0	0	0	0	0	1	0	0	4
(4, 8)	0	1	0	0	0	1	0	0	0	0	1	0	0	2180
(4, 9)	0	0	0	0	0	1	0	0	0	0	0	0	0	128
(5, 6)	0	0	0	1	1	0	0	0	0	0	1	0	0	772
(5, 9)	0	0	0	0	1	0	0	0	0	0	0	0	0	256
(6, 7)	1	0	0	0	0	0	1	1	0	1	0	0	0	4200
(6, 8)	0	0	0	0	0	1	1	0	1	1	1	1	0	222
(6, 9)	1	0	0	0	1	1	0	0	1	0	0	0	0	4496
(7, 8)	0	0	0	0	0	0	0	0	0	1	0	0	0	8
(7, 9)	1	0	0	0	0	0	0	0	0	0	0	0	0	4096
(8, 9)	0	0	0	0	0	0	0	0	1	0	0	0	0	16

(d) Alarm code table.

Figure 2.6: The *m*-cycle solution obtained via the HST algorithm for the SmallNet topology with 13 *m*-cycles, a cover length of 43 and a monitoring cost of 108 for $\gamma = 5$.

None of the aforementioned approaches to *m*-cycle are able to guarantee UFL, and are, in general, very limited. To solve that, [70] presents the concept of *nonsimple* monitoring cycle (nonsimple *m*-cycle). Differently from the simple cycle, a nonsimple *m*-cycle can traverse the same node multiple times (see Fig. 2.4c). Fig. 2.7 shows a nonsimple *m*-cycle

solution for the same topology used in Fig. 2.6. Observe that whereas the simple m-cycle solution has a monitoring cost of 108, the nonsimple m-cycle solution has a monitoring cost of just 77. However, the cycle structure still imposes limitations, making it impossible to guarantee UFL for every network topology.



(a) c_0 (b) c_1 (c) c_2

(d) c_3 (e) c_4 (f) c_5

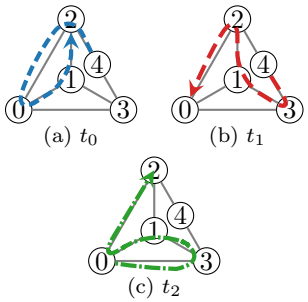
Link	$c_5c_4c_3c_2c_1c_0$	Dec.	Link	$c_5c_4c_3c_2c_1c_0$	Dec.
(0, 1)	0 1 0 1 0 1	21	(4, 5)	1 0 1 0 1 1	43
(0, 5)	0 0 0 0 1 1	3	(4, 8)	1 1 0 0 0 0	48
(0, 6)	0 1 0 1 1 0	22	(4, 9)	1 0 1 0 0 0	40
(1, 2)	0 1 0 0 1 1	19	(5, 6)	0 0 0 0 0 1	1
(1, 6)	0 0 0 1 0 0	4	(5, 9)	1 0 1 0 0 1	41
(1, 7)	0 0 0 0 1 0	2	(6, 7)	0 0 1 0 1 0	10
(2, 3)	0 0 0 0 0 1	1	(6, 8)	0 1 0 0 0 1	17
(2, 7)	1 0 0 0 1 0	34	(6, 9)	0 0 1 0 0 0	8
(2, 8)	0 1 0 0 0 0	16	(7, 8)	0 0 0 0 0 1	1
(3, 4)	1 1 0 0 1 1	51	(7, 9)	1 0 1 0 1 1	43
(3, 8)	0 1 0 0 1 0	18	(8, 9)	1 0 0 0 1 0	34

(g) Alarm code table.

Figure 2.7: A nonsimple m-cycle solution for the SmallNet topology with 6 nonsimple m-cycles, a cover length of 47 and a monitoring cost of 77 for $\gamma = 5$.

Monitoring trail (m-trail)

Whereas m-cycles have the transceivers and monitor in the same node, monitoring trails (m-trails) do not have such restrictions (see Fig. 2.4d). An m-trail can traverse the same node multiple times, but can only traverse a link once. In an m-trail the node with the transmitter in the *sorce* of the m-trail, and the node with the receiver is the *sink* of the m-trail. The monitor is located at the sink. The source and the sink of the m-trail do



(a) t_0 (b) t_1 (c) t_2

Link	t_2	t_1	t_0	Decimal
(0,1)	1	0	1	5
(0,2)	1	1	1	7
(0,3)	1	0	0	4
(1,2)	0	1	1	3
(1,3)	1	1	0	6
(2,4)	0	0	1	1
(3,4)	0	1	0	2

(d) Alarm code table.

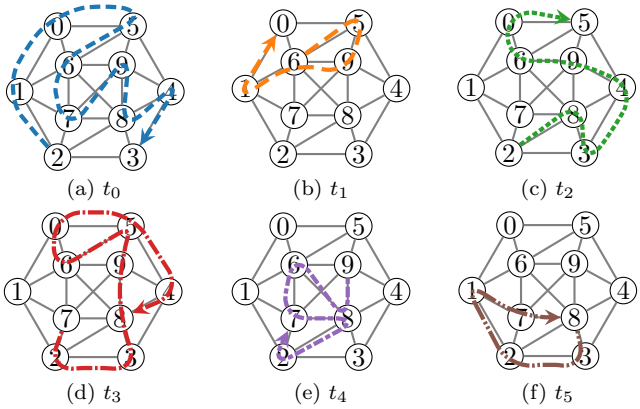
Figure 2.8: Example of an m-trail solution.

not necessarily need to be separate nodes, and can form a simple or nonsimple cycle. Such trails are called *closed trails*. When the source and sink are separate nodes, then the trail is an *open trail*. Hence, both simple and nonsimple m-cycle are a special case of m-trail.

Similarly to an m-cycle solution, an m-trail solution consists of a set of J m-trails $T = \{t_0, \ldots, t_{J-1}\}$ and a link failure will disrupt every single m-trail that traverses the failed link. The monitors at the end of each affected m-trail will send an alarm, whereas the unaffected m-trails will not send any alarm. All of this information is then represented as a binary alarm code $[a_0, \ldots, a_{J-1}]$, where $a_i = 1$ if m-trail t_i has been affected, and $a_i = 0$ if m-trail $t_i = 0$ otherwise. Fig. 2.8 shows an m-trail solution for the same network topology from Fig. 2.5. While the m-cycle solution had the same code for the links $(2, 4)$ and $(3, 4)$, the m-trail solution has a unique code for each link in the network and can unambiguously localize any link failure in the network. In fact, m-trail solutions are very effective in achieving UFL for any single failure.

In [68], the authors formulate an ILP reach an m-trail design with UFL. However, due to the computational complexity of the ILP, [62] propose an algorithm based on random code assignment (RCA) and random code swapping (RCS) to design a semi-optimal m-trail solution. The proposed algorithm first uses RCA to randomly assign an unique alarm code to each link in the network. This unique code is kept at the alarm code table. Based on these codes and the connectivity of each link in a code, the algorithm then forms the m-trails. The RCS algorithm is used to improve the solution quality, by moving the links to minimize the monitoring cost. Fig. 2.9 shows the m-trail solution obtained through the ILP formulation in [68] and Fig. 2.10 shows the solution obtained through the RCA+RCS algorithm. Both solutions outperforms the simple and nonsimple m-cycle solutions (see Figs. 2.6 and 2.7)[62]. However, the RCA+RCS algorithm has an increased number of monitors, due to the disjoint paths generated by the RCA algorithm. In order to deal with this issue, [82] propose the monitoring trail allocation (MTA) heuristic. The MTA

heuristic first puts all links in a set called ambiguity set. An ambiguity set is the set of links with the same alarm code. The algorithm then adds a new m-trail to the solution, and updates the ambiguity sets. Next, the MTA checks if all links have an unique code. If not, the algorithm return to the second step.



(a) t_0 (b) t_1 (c) t_2

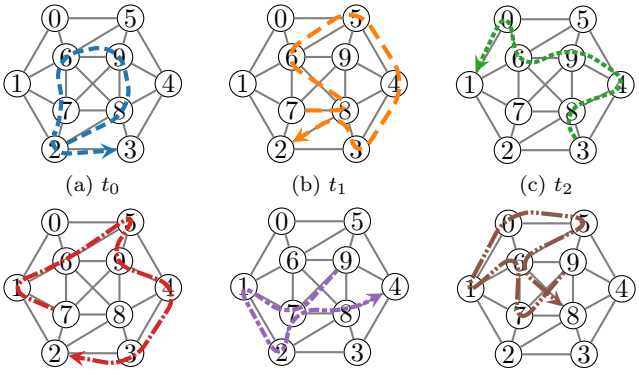
(d) t_3 (e) t_4 (f) t_5

Link	$t_5t_4t_3t_2t_1t_0$	Dec.	Link	$t_5t_4t_3t_2t_1t_0$	Dec.
(0, 1)	0 0 0 0 1 1	3	(4, 5)	0 0 1 0 0 0	8
(0, 5)	0 0 1 1 0 1	13	(4, 8)	0 0 1 0 0 1	9
(0, 6)	0 0 1 1 0 0	12	(4, 9)	0 0 0 1 0 0	4
(1, 2)	1 0 0 0 0 1	33	(5, 6)	0 0 1 0 1 1	11
(1, 6)	0 0 0 0 1 0	2	(5, 9)	0 0 1 0 1 0	10
(1, 7)	1 0 0 0 0 0	32	(6, 7)	0 1 0 0 0 1	17
(2, 3)	1 0 1 0 0 0	40	(6, 8)	0 1 0 0 0 0	16
(2, 7)	0 1 1 0 0 0	24	(6, 9)	0 0 0 1 1 0	6
(2, 8)	0 1 0 1 0 0	20	(7, 8)	1 1 0 0 0 0	48
(3, 4)	0 0 0 1 0 1	5	(7, 9)	0 0 0 0 0 1	1
(3, 8)	1 0 1 1 0 0	44	(8, 9)	0 1 1 0 0 1	25

(g) Alarm code table.

Figure 2.9: An m-trail solution for the SmallNet topology with 6 m-trails, a cover length of 42 and a monitoring cost of 72 for $\gamma = 5$ presented in [68].

In [66], the authors propose a novel framework based on m-trails in which every monitoring node is capable of localizing a single link failure using only locally available information, i.e. alarms from the m-trails traversing the node. Traditionally, an m-trail has only one node (the end) capable of detecting the status of the m-trail. Since a set of m-trails does not need to have the same end node, the monitoring nodes are usually spread throughout the network, and upon a network fault, each monitoring node reports the alarms to a remote routing entity. This generates extra delay and complexity in the electronic domain. By having all nodes capable of locating failed links, this new framework has an all-optically



(a) t_0 (b) t_1 (c) t_2

(d) t_3 (e) t_4 (f) t_5

Link	$t_5t_4t_3t_2t_1t_0$	Dec.	Link	$t_5t_4t_3t_2t_1t_0$	Dec.
(0, 1)	1 0 0 1 0 0	36	(4, 5)	0 0 0 0 1 0	2
(0, 5)	1 0 0 0 0 0	32	(4, 8)	0 1 0 1 0 0	20
(0, 6)	0 0 0 1 0 0	4	(4, 9)	0 0 1 1 0 0	12
(1, 2)	0 1 0 0 0 0	16	(5, 6)	1 0 1 0 1 0	42
(1, 6)	1 0 1 0 0 0	40	(5, 9)	0 0 1 0 0 0	8
(1, 7)	0 1 1 0 0 0	24	(6, 7)	1 0 0 0 0 1	33
(2, 3)	0 0 1 0 0 1	9	(6, 8)	1 0 0 0 1 0	34
(2, 7)	0 1 0 0 0 1	17	(6, 9)	0 0 0 1 0 1	5
(2, 8)	0 0 0 0 1 1	3	(7, 8)	0 1 0 0 1 0	18
(3, 4)	0 0 1 0 1 0	10	(7, 9)	1 1 0 0 0 0	48
(3, 8)	0 0 0 1 1 0	6	(8, 9)	0 0 0 0 0 1	1

(g) Alarm code table.

Figure 2.10: An m-trail solution for the SmallNet topology with 6 m-trail, a cover length of 39 and a monitoring cost of 69 for $\gamma = 5$ presented in [62].

fast unambiguous fault localization mechanism.

In [3], the authors focus the design of an m-trail solution that solves a failure event in a shared risk link group (SRLG). A failure of a SRLG means that all links in the SRLG have failed. They propose an algorithm called adjacent-link failure localization (AFL). The basic idea behind this algorithm is to divide the problem of SRLG failure localization into smaller subproblem that can be solved as single-link failure localization problem. This is done by partitioning the whole topology into smaller graphs, based on the SRLGs. The smaller subproblem can then be solved with the RCS algorithm.

2.3 Fault Recovery

As it has already been highlighted in Chapter 1, a single fiber cut can lead to a huge loss of data. It is possible to minimize the loss of data through fault recovery mechanisms, such as protection and restoration schemes. Protection schemes pre-configure and reserve protection resources in advance [49], whereas restoration schemes restores each interrupted connection by dynamically searching for a new available routes and wavelengths [54]. The later is usually more bandwidth efficient, but cannot guarantee service restoration, whereas the former has a faster recovery time and can guarantee service restoration, but requires more bandwidth.

Protection schemes can be designed to protect and entire path (path protection) or just a single link (link protection). In a path protection scheme, the network reserves some bandwidth to a protection path, an alternate link-disjoint path to be used in case the working path is disrupted [51]. A working path is the lightpath that transmits the traffic under normal operation. In link protection, instead of having an alternate route for the entire path, it is only around one link and each link has an alternate route reserved in advance. Fig. 2.11 shows path protection for a connection request from node 0 to node 4, and link protection for link $(0, 2)$. For a path protection scheme, when w_0 $(0 \rightarrow 2 \rightarrow 4)$ is interrupted due to a fault at any link in the path, the traffic will be switched over to the protection path p_0 $(0 \rightarrow 3 \rightarrow 4)$. For a link protection scheme, each link has a protection path. In Fig. 2.11b, link $(0, 2)$ has the protection path p_0 $(0 \rightarrow 1 \rightarrow 2)$ to protect just this one link. When link $(0, 2)$ fails, only the segment of the path w_0 that corresponds to the link $(0, 2)$ is replaced by p_0, switching the traffic over to a path $(0 \rightarrow 1 \rightarrow 2 \rightarrow 4)$. There are also schemes to protect just a segment of a path (sub-path protection) [44].

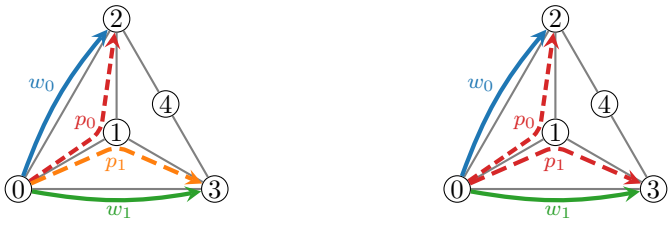
(a) Path protection. (b) Link protection.

Figure 2.11: (a) Path and (b) Link protection.

This work mainly focus on path protection, since compared to link protection, it requires less network resources.

The aforementioned protection schemes offer two distinct approaches in how it reserves

bandwidth for protection: dedicated protection, also known as $1 + 1$ protection, assigns for each working path its own dedicated bandwidth for the protection path; and shared protection, where disjoint working paths can have protection paths traversing the same link while occupying the same wavelength. Shared protection paths assumes that all working connections will not fail at the same time and reduces the amount of bandwidth dedicated to protection. With shared protection we can also use the protection bandwidth to carry some low-priority traffic, which will be discarded if the working path fails. Fig. 2.12 shows an example of both dedicated and shared protection paths. The working paths w_0 and w_1 have the protection paths p_0 and p_1, respectively. In Fig. 2.12a, the protection paths occupy different wavelengths, and if w_0 or w_1 fail, their traffic will switch to their respective protection paths. Since p_0 and p_1 have their own dedicated wavelength in link $(0, 1)$, then even though they traverse the same link, both protection paths can co-exist at the same time and restore the traffic flow even if both w_0 and w_1 are in a failed state at the same time. On the other hand, shared protection paths, illustrated in Fig. 2.12b, share the same wavelength at link $(0, 1)$, so they cannot function at the same time.



(a) Dedicated protection path. (b) Shared protection paths.

Figure 2.12: Protection schemes.

When establishing new working and protection paths, the following shared path protection constraints regarding the existing lightpaths must be followed [44]:

- A working path and its protection path must be link-disjoint;
- The working paths do not share links within the same wavelength;
- The established lightpath does not share any wavelength with any of the established backup protection paths for any common link they may share;
- Backup protection paths can only share links within the same wavelength if their respective working paths are link disjoint.

Protection paths can also be revertive or nonrevertive. In case of a failure, the traffic from the working path is rerouted to the protection path. A protection scheme is considered revertive if, after the route for the working path is fixed, the traffic returns to the original path. In a nonrevertive scheme, the traffic stays in the protection path, until it is manually moved back to the original working path. Dedicated protection schemes may be either revertive or nonrevertive, while shared protection is usually revertible. Since the protection bandwidth is shared, it is important to free it as soon as possible.

Chapter 3

Failure Localization Aware Working Paths (FLA-RWA)

3.1 Network Model

In this work, we consider the single-link failure localization problem in all-optical IP over WDM network, which consists of two layers: IP layer and optical physical layer. The electronic layer is formed by an IP router at each network node with an electronic control unit sending control signals to configure the optical switching fabric. The IP routers generate and drop IP traffic, serving as the source and destination nodes. Network data flows are done by establishing transparent lightpaths between pairs of transceivers equipped at the source and destination nodes, without any electronic processing at the intermediate nodes on the routing path. Two adjacent optical crossconnects (OXCs) are interconnected by an optical fiber link and are responsible for switching lightpaths entirely in the optical domain. The optical layer is basically the set of OXCs and optical fibers in the system.

With the recent development and commercialization of signal processing technologies, it is possible to maintain continuous monitoring of physical layer in real-time. Light probe technology allows the link state to be continuously monitored and analyzed [42]. Since we consider the failure in the granularity of link level, a small portion of the bandwidth on a lightpath can be used to send control signals for actively probing for the status of all lightpaths. When a link traversed by the lightpath fails, the probing signal will be disrupted and become dark, indicating an "OFF" state. The signal processing module of the coherent optical transceiver at the end node of the lightpath will detect the "OFF" state, and subsequently it will generate alarm codes to report the failure event. The alarms

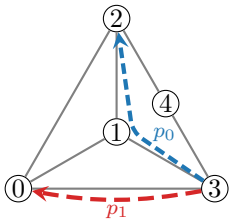
are forwarded to a centralized network management center in charge of failure localization. Since multiple lightpaths from different source nodes and/or with different routes may share the same destination node, failure localization can be a highly complicated and challenging task, but crucial to guarantee availability and reliability in all-optical networks.

3.2 Failure Localization by Probing Working Lightpaths

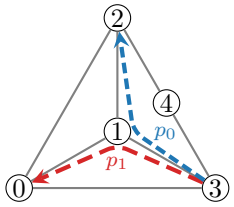
Based on the all-optical IP over WDM network and in-band active probing technology, we can abandon the use of additional supervisory lightpaths, like m-trail. However, directly exploiting working lightpaths for monitoring creates new problems. Routing and wavelength assignment schemes, such as the shortest path method and load balancing schemes, usually aim to minimize the number of occupied wavelengths, the end-to-end latency or the blocking probability. To the best of our knowledge, no previous study has taken failure localization into consideration when allocating network resource to establish lightpaths. Since we propose the use of the working paths for monitoring, the failure localization issue needs to be included in the RWA process in a FLA-RWA scheme, where the goal to reduce the ambiguity in failure localization.

Fig. 3.1 shows two different solution for the allocation of two connection requests, one from node 3 to node 2 and the second from node 3 to node 0. In Fig. 3.1a we have the classic shortest path (SP) approach to the connection requests. For the SP approach, we have that if link $(1, 3)$ fails, then the management center will receive the codes "1" and "0" for the working paths p_0 and p_1, respectively. However, this is the same code for a fault in link $(1, 2)$. Since both links have the same code, whenever the management center receives this code, there are two possible locations for the failed link, which mean that there is ambiguity in the failure localization. Fig. 3.1b shows a different solution for the same connection requests. Here, the route for the request from node 3 to node 0 is different. Now, in case of a link failure at link $(1, 3)$, we will have the codes "1" and "1" for the working paths p_0 and p_1, which is different from the codes "0" and "1" for link $(0, 1)$, and "1" and "0" for link $(1, 2)$. Compared with the solution from Fig. 3.1a, there is less ambiguity for failure localization at the cost of 1 extra hop for the working path p_1.

This simple example illustrates the least ambiguous path (LAP) routing scheme. Note that by monitoring the network through working paths, instead of dedicated supervisory lightpaths, we save a lot of network resources. The cover length, as a measurement of monitoring cost, is defined as the total number of wavelength links used for supervisory



(a) Shortest path (SP).



(b) Least ambiguous path (LAP).

Figure 3.1: Comparison between the shortest path and the least ambiguous path for the paths p_0 from node 3 to node 2, and p_1 from node 3 to node 2.

lightpaths for a failure localization solution [67]. The m-trail solution for the topology in Fig. 3.1 is illustrated in Fig. 2.8 and has a cover length of 12 wavelengths. In contrast, both the SP and LAP, illustrated in Fig. 3.1, do not require any additional wavelength for monitoring. Hence, the cover length for both schemes are negligible. Moreover, the establishment of three m-trails requires six extra optical transceivers, which is expensive and a limited network resource, since the number of ports in an IP router is finite. Thirdly, once the m-trails are established, the monitoring operation starts without interruptions, leading to a higher complexity in the control plane.

When comparing two routing schemes from 3.1, we realize that the LAP scheme may choose a longer route to gather more information on the link state. In other words, we can significantly improve the fault location accuracy at the cost of an increased wavelength usage. Inspired by this example, it is possible to notice that the core issue in using a working path monitoring scheme is to design an efficient failure localization aware routing and wavelength assignment (FLA-RWA) method to reduce the ambiguity in failure localization.

3.3 Least Ambiguous Path (LAP)

For the sake of simplicity, a network physical topology is represented as $G(V, E)$ consisting of node set V and edge set E. Each link contains a wavelength set W. The network traffic, $r(s, d, bw)$, denotes a connection request from source node s to destination node d with the bandwidth demand bw in number of wavelengths, where s, $d \in V$. To save the computation time of the RWA in a dynamic environment, a set of candidate routing paths can be precomputed offline and stored in the set of the k-shortest paths (KSP), which contains $P_{sd} = [p^1_{sd}, p^2_{sd}, \ldots, p^k_{sd}]$ for every source-destination pair (s, d). P_{sd} represent the set of k-shortest alternate paths from s to d, where s, $d \in V$. In addition, in order to keep

record of ongoing working paths in the current network, centralized management center dynamically manages a routing table, WPT.

On the arrival of a connection request $r(s, d, bw)$, the LAP scheme attempts to select the routing path $p_{sd}^{i} \in P_{sd}$ in the KSP set that leads to a minimum failure localization ambiguity among all k candidates. If such path p_{sd}^{i} exists, then the second phase will be initialized to assign a common available wavelength on all physical links along the selected path p_{sd}^{i} (due to the wavelength-continuity constraint). If a viable routing path and/or available wavelength cannot be found after checking all candidate paths and wavelength channels, request $r(s, d, bw)$ will be blocked. The ambiguity in failure localization is defined as the number of physical links which are possibly failed, according to the alarm code received by network operation and management center, averaged by the number of non-idle links in the network. It can be calculated by Eq. 3.1 as follows:

$$\text{Ambiguity} = \frac{1}{|E'|} \sum_{(i,j) \in E'} \left|S_{i,j}\right| \tag{3.1}$$

where: $S_{i,j}$ is the set of suspected locations for a network failure in link (i, j); $\left|S_{i,j}\right|$ is the number of elements in set $S_{i,j}$; E' is the set of links in the network traversed by at least one lightpath; $|E'|$ is the number of links in set E'.

To calculate $S_{i,j}$, for each link $(i, j) \in E'$ we first separate all paths $p_w \in WPT$ into two sets: the affected paths sets, $P_{i,j}$, and the unaffected paths, $P'_{i,j}$. The paths in the $P_{i,j}$ set are all paths that traverse link (i, j), i.e. $(i, j) \in p_w$. The paths on the $P'_{i,j}$ set, on the other hand, are all paths that do not traverse link (i, j), i.e. $(i, j) \notin p_w$. For a single link failure, the fault location must be traversed by every single affected path. Hence, we calculate the set of all links that are traversed by every single affected path, $A_{i,j}$, as:

$$A_{i,j} = \bigcap P_{i,j} \tag{3.2}$$

We also have that every link traversed by any of the unaffected paths cannot be a possible location for the link failure. We then calculate the set of all links that are traversed by at least one unaffected path, $A'_{i,j}$, as:

$$A'_{i,j} = \bigcup P'_{i,j} \tag{3.3}$$

Now we can obtain the set $S_{i,j}$ by just removing from the set $A_{i,j}$ any link that is also in set $A'_{i,j}$. We can calculate the number of suspect locations, denoted as $\left|S_{i,j}\right|$, with Eq. 3.4.

$$|S_{i,j}| = |A_{i,j}| - \left|\left(A_{i,j} \bigcap A'_{i,j}\right)\right| \tag{3.4}$$

where $|A_{i,j}|$and $\left|A'_{i,j}\right|$ are the number of links in the sets $A_{i,j}$ and $A'_{i,j}$, respectively. $\left|\left(A_{i,j} \bigcap A'_{i,j}\right)\right|$ is the number links that are in both sets $A_{i,j}$ and $A'_{i,j}$.

To better illustrate how to calculate the ambiguity, we can calculate the simple example from Fig. 3.1. In Fig. 3.1b we have that $WPT = [p_0, p_1]$, where $p_1 = [(3,1),(1,2)]$ and $p_0 = [(3,1),(1,0)]$. Hence, $E' = [(1,0),(1,2),(3,1)]$. For a fault at link $(1,0)$, the set of affected paths is $P_{1,0} = [p_1]$ and the set of unaffected paths is $P'_{1,0} = [p_0]$. From equations 3.2 and 3.3, we have that $A_{1,0} = [(3,1),(1,0)]$ and $A'_{1,0} = [(3,1),(1,2)]$. By removing the only link $A_{1,0}$ and $A'_{1,0}$ have in common from the set $A_{1,0}$, we have that $S_{1,0} = [(1,0)]$ and $\left|\begin{matrix}S_{1,0}\\S_{3,1}\end{matrix}\right| = 1$. Following the same calculation for links $(1,2)$ and $(3,1)$ we have $\left|S_{1,2}\right| = 1$ and $\left|S_{3,1}\right| = 1$. The final ambiguity for Fig. 3.1b is 1. If we do the same calculation for Fig. 3.1a, we will obtain an ambiguity of 1.67.

Based on the above definition of ambiguity, we develop an LAP algorithm with the objective to choose a path among all candidates path in the KSP with minimum ambiguity in failure localization. Since when and where the next link failure will occur cannot be known in advance, all possible single-link failure events need to be examined. The listed pseudocode *Algorithm* 1 depicts the proposed LAP algorithm, which attempts to find viable routing path with available wavelength for each incoming connection request $r(s,d,bw)$.

In *Algorithm* 1, the LAP heuristic first selects the shortest of the feasible candidates in $P_{sd} \in KSP$ sorted in ascending order by the number of hops (Line 2). Secondly, for a certain candidate path, the ambiguity is calculated assuming the candidate path is in the network (Line 3). Observe that since the ambiguity is calculated without any a priori knowledge of the next link failure, its calculations includes every active link in the network. This procedure will be repeated for all alternate routing paths by considering all possibilities of link failure in set E'. The alternate path with the least value of ambiguity will be chosen as the routing solution for the current connection request (Line 5). In case of a tie, where the same ambiguity is achieved among different alternate paths, a random path is selected out of the competing paths. After successfully determining a routing path, the heuristic searches on all available wavelengths in each physical link along the path to find a common wavelength (Line 9). If not successful, the alternate path with the next lowest ambiguity will be checked, until either a viable path is found or there are no more paths and the request is blocked. Finally, the procedure *Update* WPT establishes a

Algorithm 1: Least ambiguous path (LAP)

input : $G(V, E), r(s, d, bw), KSP, WPT$
output: updated WPT'

```
foreach arriving connection requests do
    foreach p^i_sd ∈ P_sd from KSP do
        Calculate Ambiguity_p^i_sd assuming p^i_sd ∈ WPT
        if Ambiguity_p^i_sd = Min_Ambiguity then
            r(s, d, bw) ← p^i_sd
    if p^i_sd = ∅ then
        Block r(s, d, bw)
    else if w ∈ W is common on p^i_sd then
        r(s, d, bw) ← w
    else
        Block r(s, d, bw)
    WPT' ← Update(WPT)
```

working lightpath for the current connection request. Lastly, the information of the newly established working lightpath will be recorded and inserted into the set WPT.

3.4 Performance Evaluation and Discussion

In this section, we examine the proposed FLA-RWA scheme via a discrete event-driven network simulator. It is anticipated that the LAP algorithm can achieve the lowest localization ambiguity. We evaluate the effectiveness of the proposed scheme with performance metrics related to fault localization, network resource usage and blocking probability. For the fault localization metrics, we consider the accuracy in which the heuristic was able to determine unambiguously the fault location and the number of possible fault locations. For the resource usage metrics, we consider the average path length and cover length. Since we are using the working path to monitor the network, the cover length in this case refers to the total wavelength occupancy in the network by the working paths. We also implement two other commonly used RWA heuristic algorithms, the ASP and LCP schemes, for comparison. We use the well known FF scheme for wavelength allocation for the ASP and LAP schemes, and the LU scheme for the LCP scheme. We use Yen's algorithm [77] to find the set of alternate paths for 3 alternate paths.

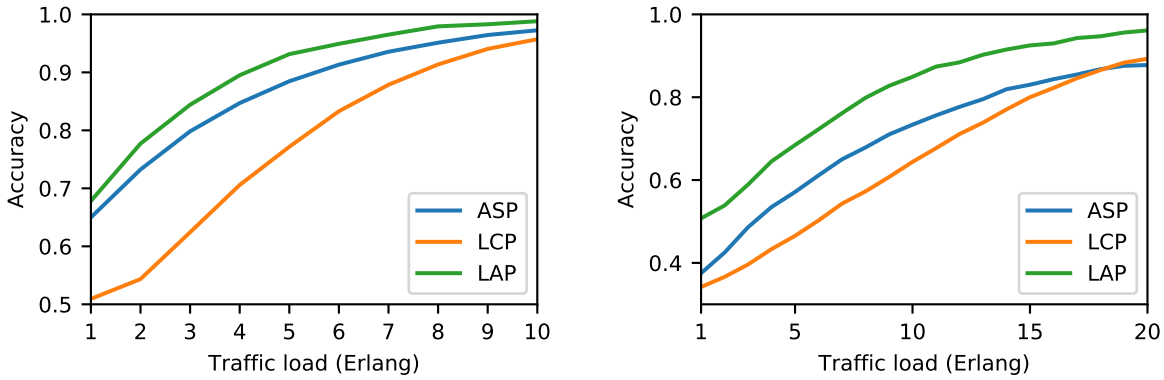
All three schemes are examined based on the two network topologies illustrated in Fig. 3.2, a small sized 5N7L network (see Fig. 3.2a) and the SmallNet topology (see Fig. 3.2b). Each link contains 16 wavelengths. In the simulations, connection requests are generated under network load ρ. Each connection request arrives dynamically in the network according to a Poisson process, with an average arrival rate of λ requests per time unit. The holding times of connection requests are exponentially distributed with the average of 1 time unit. To simulate the link failure in networks, $10,000$ single-link failures are generated for each run. We considered that the MTBF follows an exponential distribution with an average of 12 time units.

(a) 5N7L network. (b) SmallNet network.

Figure 3.2: Considered network topologies.

Fig. 3.3 shows the accuracy in which we are able to locate the failed link for both networks under a traffic load ranging from 1 to 10 Erlangs for the 5N7L network, and from 1 to 20 Erlangs for the SmallNet network. This range is chosen because there are no blocked requests for these traffic load intervals. In this metric we consider that only when there is just one possible fault location that we have found a correct solution, all cases that have more than one possible fault location are considered inaccurate. Observe that the accuracy increases with the traffic load and eventually, with a traffic load high enough, the accuracy for all three schemes will converge to approximately 1. For the 5N7L network, the LAP outperforms the other two schemes, and although the difference between LAP and LCP can be as big as 16.9%, there is not much difference between the LAP and ASP schemes. For the SmallNet network, on the other hand, the LAP scheme greatly outperforms the other two schemes. Even for extremely small traffic loads, with a very limited number of paths to gather information from, the LAP is able to maintain an accuracy superior to 50%, while the other two schemes have an accuracy below 40%. For a network load of 10 Erlangs, the LAP scheme has around 85% accuracy, while the ASP scheme has only around 73% and the LCP scheme is just a little bit over 64%. For 20 Erlangs, the ASP and LCP scheme have an accuracy close to 90%, while the LAP accuracy is over 95%. Once again the LAP outperforms all other schemes, and the difference only increases for bigger networks. Table 3.1 shows the numeric values (in percentage) for the fault location

accuracy under different traffic loads.



(a) 5N7L network.

(b) SmallNet network.

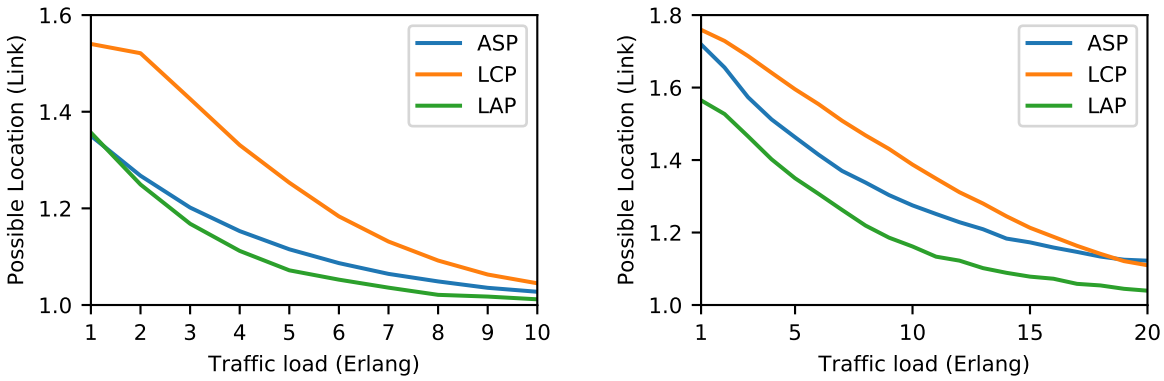
Figure 3.3: Fault location accuracy for (a) 5N7L network and (b) SmallNet network for the ASP, LCP and LAP schemes.

RWA	5N7L			SmallNet		
	1 Erlang	5 Erlangs	10 Erlangs	1 Erlang	10 Erlangs	20 Erlangs
ASP	65%	88.5%	97.3%	37.5%	73.4%	87.8%
LCP	50.9%	77.2%	95.7%	34.2%	64.4%	89.2%
LAP	67.8%	93.1%	98.9%	50.7%	84.9%	96%

Table 3.1: Fault location accuracy in percentage for ASP, LCP and LAP routing.

From Fig. 3.3 we observe that the tendency is for the accuracy to only increase with the traffic load, however, with no prior knowledge of future connection requests, it may be impossible to guarantee unambiguous failure localization (UFL). Decreasing the ambiguity in fault localization does not just increase the accuracy in which we can unambiguously locate a network fault, but it also reduces the number of possible fault locations for a given network fault. Fig. 3.4 shows the average number of possible fault locations. As expected, the LAP achieves the lowest number of possible fault locations among all three schemes for both networks. For the 5N7L network, the LCP values are between 4% to 23% larger than the LAP, and the ASP values are 2-4% larger. Although the ASP and LAP have a very similar performance for the 5N7L network, for the SmallNet network the LAP routing performs significantly better than all other schemes. For the SmallNet network, the LCP values are up to 22% larger than the LAP, and the ASP values are up to 12% larger.

The ASP scheme performance for both the fault location accuracy and average number of possible fault locations is similar to the LAP performance for the 5N7L network mainly because of the network size. When the shortest distance between a source-destination is just 1 hop, both the shortest path and least ambiguous path will be the 1 hop path. Since 70% of the source-destination pairs in the 5N7L network have a shortest possible distance of just 1 hop, then most of the routing for the ASP and LAP schemes will be the same. When the percentage of source-destination pairs with a minimum distance of 1 hop decreases to less than 50% for the SmallNet network, the difference in the performance between the ASP and LAP schemes increases. The gain in the failure localization performance for the LAP scheme becomes more significant for bigger network.

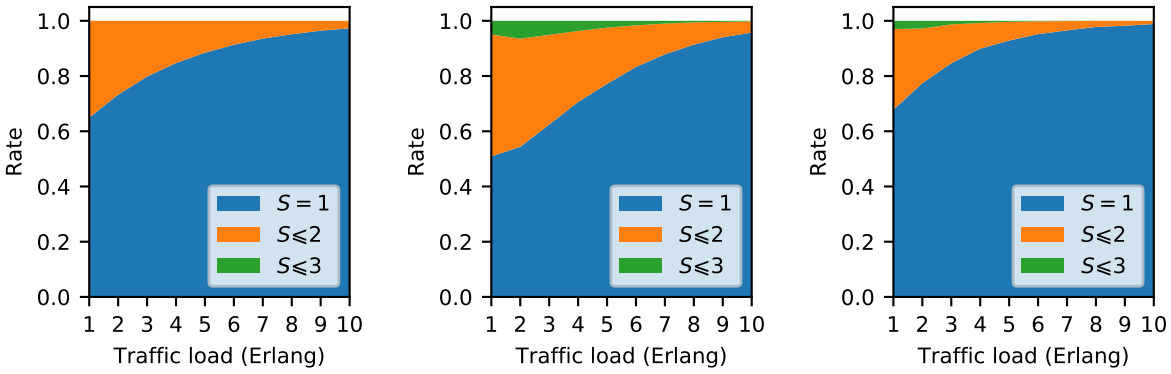


(a) 5N7L network.

(b) SmallNet network.

Figure 3.4: Average number of possible fault locations for (a) 5N7L network and (b) SmallNet network for the ASP, LCP and LAP schemes.

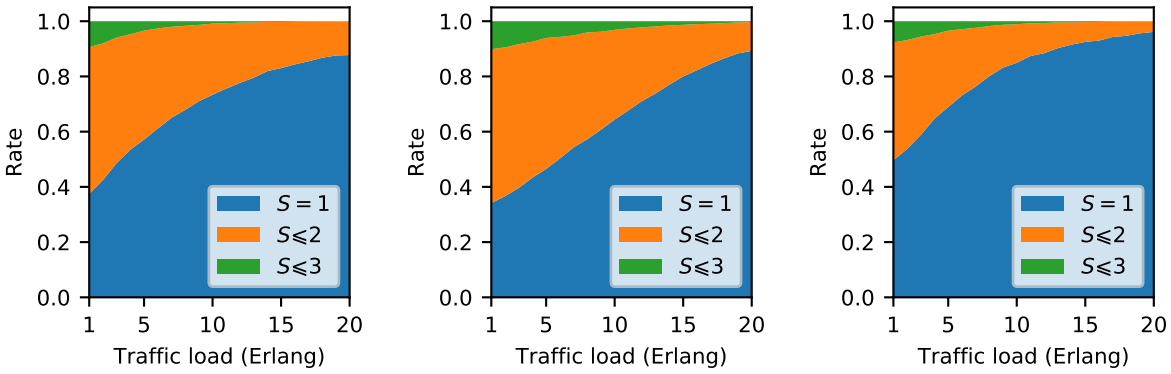
The average number of possible fault locations alone can give us an estimate on how many locations we may need to check in order to find the network fault. However it does not provide a full picture of how the number of possible fault locations is distributed. Figs. 3.5 and 3.6 show the rate in which the number of possible fault location S is less or equal to $1, 2$ and 3 for the networks 5N7L and SmallNet, respectively. Observe that $S = 1$ is the fault location accuracy from Fig. 3.3. For the 5N7L network, less than 5% of the network faults have more than 2 possible fault locations. In fact, for the ASP routing, none of the $10,000$ simulated network faults had over 2 possible fault locations. This is mainly due to the fact that the shortest path for the 5N7L between any source-destination pair is always less or equal to 2 hops, and the ASP always allocate the shortest available path. The maximum number of possible fault locations is the number of hops of the longest



(a) ASP. (b) LCP. (c) LAP.

Figure 3.5: Rate in which the number of possible fault locations is $S = 1$, $S \leqslant 2$ and $S \leqslant 3$ for the ASP, LCP and LAP schemes for the 5N7L network.

path allocated to a connection request. The LAP scheme has up to 2% of cases where the the number of fault locations is bigger than 2, because it allocates paths longer than the shortest possible path when necessary. At the cost of some cases having over 2 possible fault locations, the LAP scheme is able to increase the fault location accuracy and decrease the average number of possible fault locations.



(a) ASP. (b) LCP. (c) LAP.

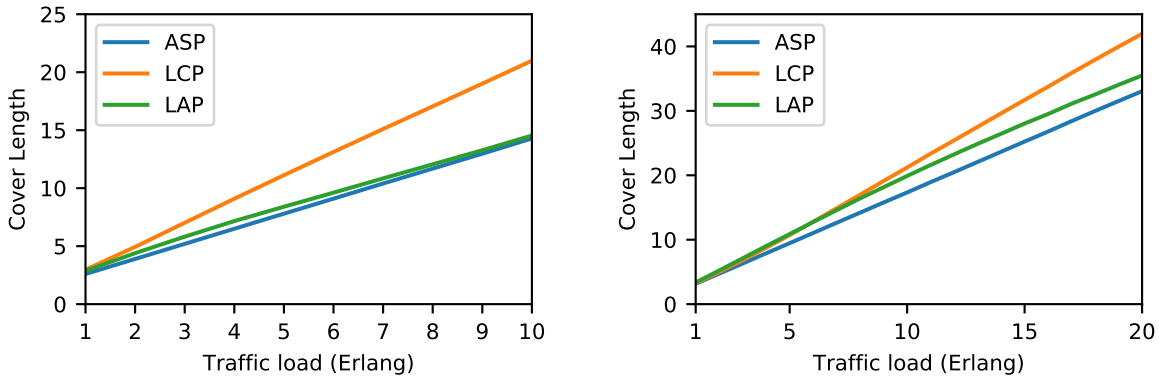
Figure 3.6: Rate in which the number of possible fault locations is $S = 1$, $S \leqslant 2$ and $S \leqslant 3$ for the ASP, LCP and LAP schemes for the SmallNet network.

For the SmallNet network (see Fig. 3.6), we have that less than 12% of the network

faults have over 2 possible fault locations. Differently from the 5N7L network, the ASP has over 2 possible fault locations more frequently than the LAP scheme for the SmallNet network. Although the size of the network has a huge impact on the number of possible fault locations, the LAP scheme is able to outperform the other two scheme in regards to failure localization for both networks.

The LCP scheme has a poor performance in failure localization due to the fact that this routing scheme prioritizes paths with the least congested links. This results in having the paths more spread throughout in the network. At first, this may seem like a better way to monitor the network, as there will be less lightless links. However, when we have a fault on a link not traversed by any lightpath, it does not interrupt any connection and does not trigger any alarm within the working paths. A failed link that does not affect any service in the network is not a priority, hence, we do not care for such faults in this work. When the LCP spreads the paths, it can monitor more links, but it gather less information from each link.

We have shown that for failure localization the LAP scheme is able to outperform both the ASP and LCP schemes. However, we also need to discuss the cost of prioritizing fault localization over any other performance metric. Fig. 3.7 shows the cover length for the three scheme for both networks. We consider here that cover length is total occupied wavelengths in the network.



(a) 5N7L network.

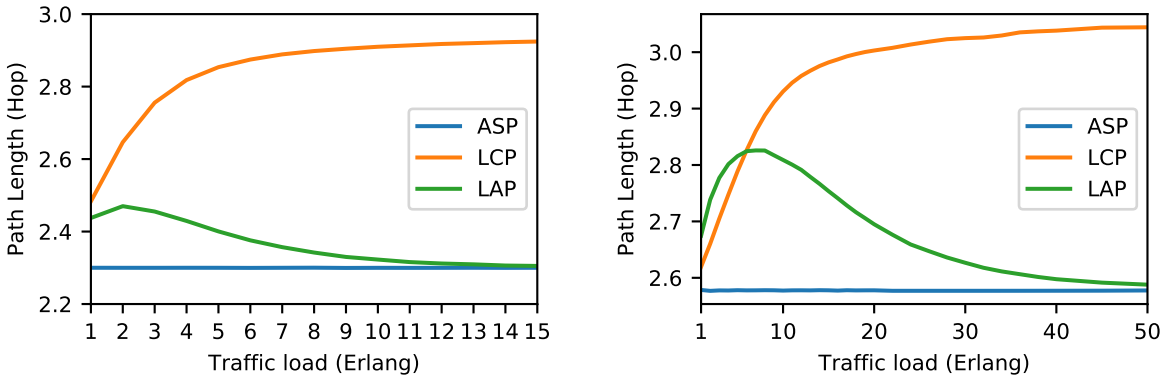
(b) SmallNet network.

Figure 3.7: Cover length for (a) 5N7L network and (b) SmallNet network for the ASP, LCP and LAP schemes.

In Fig. 3.7, the ASP scheme has the lowest cover length as expected, since it is a scheme that always assigns the shortest available path. Compared to the ASP scheme, the LCP

has an increase of up to 6.7 wavelengths and the LAP scheme has an increase of up to 0.65 wavelengths for the 5N7L network within the observed traffic load interval. It is worth remembering that the m-trail solution alone for the 5N7L network has a cover length of 12 wavelengths (see Fig. 2.8). For the SmallNet network, the LCP scheme has an increase of up to 9 wavelengths, and the LAP schemes has an increase of up to 2.82 wavelengths. The m-trail solution presented in [62] for the SmallNet has a cover length of 39 (see Fig. 2.10). Even though the LAP scheme increases the bandwidth usage in the network, it is a considerably smaller increase than if we were to deploy a full m-trail solution.

Fig. 3.8 shows the average path length for the three schemes for both networks. Although it is not a relevant metric for the schemes' performance, it is a better representation than the cover length on the difference in bandwidth usage for the three schemes. In this figure we use different intervals for the traffic load. For the 5N7L network, we consider a traffic range from 1 to 15 Erlangs, and for the SmallNet network, we consider a traffic range from 1 to 50 Erlangs. There are still no blocked requests for both traffic ranges.



(a) 5N7L network.

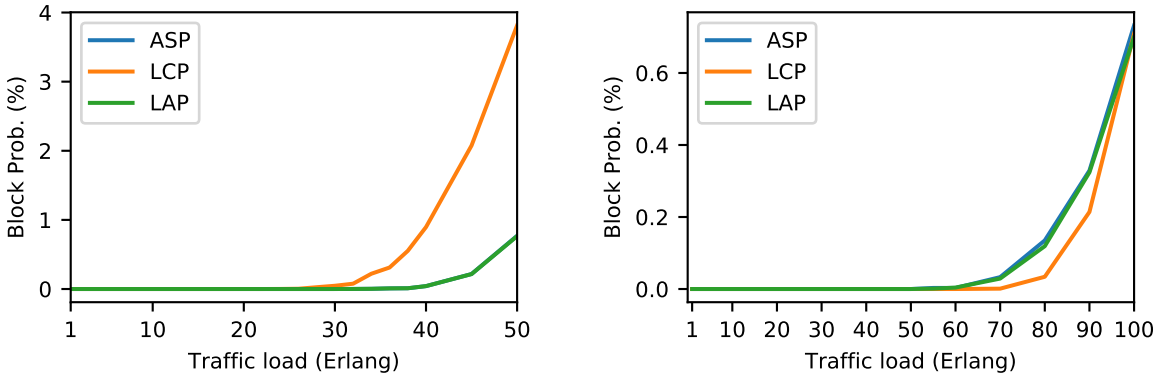
(b) SmallNet network.

Figure 3.8: Path length for (a) 5N7L network and (b) SmallNet network for the ASP, LCP and LAP schemes.

The ASP always chooses the shortest path, and as such, even for higher traffic loads, the values for the average path length in hops are almost constant. The LCP spreads the traffic throughout the network, and as the traffic load increases, this scheme starts choosing longer paths to avoid congested links. The LAP scheme starts by choosing longer paths, to gather more information on the links states, and, as the traffic load increases and there are more paths to gather information from, the paths start getting shorter and eventually we have an average path length similar to the ASP scheme. Observe that we

did not run 10,000 faults for traffic loads above 20 Erlangs, due to the computational time required for simulations with heavier traffic loads. For the results over 20 Erlangs we ran the simulations for 100,000 connection requests.

A direct consequence of a high usage of network resources is the probability of a connection request being blocked due to the lack of available wavelengths. Although a higher cover length and path length may result in more blocked request, if the network load is better distributed throughout the network, we may have a reduced blocking probability. In Fig. 3.9 we have the blocking probability for the three schemes under a traffic load of 1 to 50 Erlangs to the 5N7L network, and from 1 to 100 Erlangs for the SmallNet network. Due to the fact that for heavy traffic loads, with many active connections in the network, the LAP scheme assigns basically the same paths as the ASP schemes, we have that the blocking probability for both schemes is almost the same for both the 5N7L network and the SmallNet network. For the 5N7L network, we have that the blocking probability for the LCP can be as big as four times the blocking probability of the other two schemes. This is due to the very small size of the 5N7L network. The LCP is usually capable of distributing the traffic load throughout the network such that the blocking probability is reduced when compared to a shortest path scheme. For a sightly bigger network, such as the SmallNet network, the blocking probability for the LCP scheme is lower than the other two schemes.



(a) 5N7L network.

(b) SmallNet network.

Figure 3.9: Blocking probability for (a) 5N7L network and (b) SmallNet network for the ASP, LCP and LAP schemes.

Although the LAP prioritizes the failure localization at the cost of a higher cover length, the increased wavelength occupancy is only necessary when there are plenty of available

wavelengths. In the end, there is no increase in the LAP blocking probability compared to the ASP scheme. Even when the LCP scheme has a better blocking probability than the LAP scheme, the difference is less than 0.1%.

Chapter 4

Failure Localization Aware Protection (FLA-P)

4.1 Network Model

We consider here basically the same network model described in Section 3.1, with the inclusion of path protection for the working paths. In path protection, when establishing the working paths the resources for a link-disjoint protection path are reserved and can either be dedicated to that one working path or shared with other protection paths. In dedicated protection, each established working path has its own dedicated protection path, whereas in shared protection, several disjoint working paths can share the same wavelengths for the protection paths. The bandwidth reserved for protection can be equal or even bigger than the bandwidth used by the working paths. We propose to exploit the established protection paths by establishing supervisory lightpaths in the paths to aid the failure localization. Now, when a link fails, the probing signal in all traversing working and protection paths will be disrupted, and this LOL will be detected by the signal processing module from the coherent optical transceiver at the end node of each affected path.

4.2 Failure Location Aware Protection (FLA-P)

A protection path is usually chosen as the shortest disjoint-path from the working path, obtained with an algorithm such as the one presented in [59]. However, as it has been

shown in Section 3.4, it is possible to choose routes that reduces the ambiguity of failure localization.

For the proposed FLA-P scheme, we precompute offline all candidate working and protection paths and store them in the sets WP_{sd} and PP_{sd}, respectively. The set $WP_{sd} = [wp^1_{sd}, wp^2_{sd}, \ldots, wp^k_{sd}]$ contains all candidate working paths and the set $PP_{sd} = [pp^1_{sd}, pp^2_{sd}, \ldots, pp^k_{sd}]$ contains all candidate protection paths. In order to keep record of both ongoing working and protection paths in the network, all ongoing working paths are stored in the routing table WPT and their respective protection path is stored in PPT. Algorithm 2 depicts the proposed FLA-P scheme, which attempts to find the best route for the protection path for a connection request $r(s, d, bw)$ after an appropriate working path wp^i_{sd} has been chosen from the set WP_{sd} (Line 2).

Algorithm 2: Failure localization aware protection (FLA-P) scheme

input : $G(V, E), r(s, d, bw), PP_{sd}, WPT, PPT$
output: updated PPT'

```
1  foreach arriving connection requests do
2      Chose an appropriate wp^i_sd from WP_sd
3      foreach pp^i_sd ∈ PP_sd disjoint from wp^i_sd do
4          Calculate weight ω^i_sd for pp^i_sd
5          if ω^i_sd = Min_Weight then
6              r(s, d, bw) ← pp^i_sd
7      if pp^i_sd = ∅ then
8          Block r(s, d, bw)
9      else if w ∈ W is viable for pp^i_sd then
10         r(s, d, bw) ← w
11     else
12         Block r(s, d, bw)
13     PPT' ← Update(PPT)
```

After a proper working path has already been chosen, we calculate the weight ω^i_{sd} for each candidate protection path disjoint from the chosen working path (Line 4). The weight calculation depends on what we want to prioritize. We considered three different calculations for ω^i_{sd}:

1. Shortest protection path (SPP):

$$\omega^i_{sd} = H^k_{sd} \tag{4.1}$$

where H_{sd}^{k} is the number of hops in the path pp_{sd}^{i}.

2. Least congested protection path (LCPP):

$$\omega_{sd}^{i} = \max_{i,j \in pp_{sd}^{i}} \Lambda_{ij} \tag{4.2}$$

where Λ_{ij} is the number of free wavelengths for link (i, j)

3. Least ambiguous protection path (LAPP):

$$\omega_{sd}^{i} = \text{Ambiguity}_{sd}^{i} \tag{4.3}$$

where $\text{Ambiguity}_{sd}^{i}$ is calculated using Eq. 3.1, with the assumption that the paths wp_{sd}^{i} and pp_{sd}^{i} have been established in the network.

After we assign the weights for each candidate protection path, we choose the path with the least weight and a viable wavelength. If no candidate path has any available wavelength for all links, then the working path is not established (Line 12). The wavelength can be chosen using any wavelength allocation scheme.

4.3 Performance Evaluation and Discussion

Similarly to Section 3.4, we evaluate the performance of the proposed FLA-P scheme via discrete event-drive network simulations. First we compare the failure localization accuracy between monitoring and not monitoring the protection paths. Next, we compare the performance of the three different schemes: SPP, LCPP and LAPP.

4.3.1 Monitoring Protection Paths

In Chapter 3, we use the working paths to monitor the network and we do not consider protection paths. In this section, we will compare the performance when monitoring only the working paths and when monitoring both working and protection paths. For the sake of simplicity, we consider the set of candidate working paths to be just the shortest path from source s to destination d. Therefore, the working path is always the shortest path. We precalculate the shortest path via Djikstra's shortest path algorithm [10]. The set of candidate working paths for each source-destination pair is the k-shortest paths (KSP)

(obtained via Yen's algorithm [77]) from the residual network obtained by removing all links traversed by the shortest path. We consider 3 alternate paths for the candidate protection paths.

We examine both cases under the two network topologies illustrated in Fig. 3.2, the 5N7L network and the SmallNet network. Each link contains 16 wavelengths. The connection request follow a Poisson process, with an arrival rate of λ. The holding time are exponentially distributed, with an average of 1 time unit. We simulate $10,000$ single-link failures for each run. We considered that the MTBF follows an exponential distribution with an average of 12 time units.

The protection paths are chosen using the SPP scheme, which will prioritize the protection path with the least hop count, i.e. the shortest path. The deployed wavelength allocation is FF, where we select the first viable wavelength from an ordered list of wavelengths. The working paths and protection paths use the same ordered wavelength list, however, the protection paths consider a reverse order for the list of wavelengths.

Observe that a protection path is always disjoint from its corresponding working path. When calculating the ambiguity according to Eq. 3.1, two disjoint paths may have a higher ambiguity than just one path. Fig. 4.1 shows an example of two disjoint paths for a connection request from node 0 to node 2. Observe that if we consider only the working path, we have only one active link, and a failure in this one link has only one possible location. Hence, the ambiguity for the working path is 1. When we consider both the working path (w_0) and protection path (p_0), we have three active links, and a fault in links $(0,1)$ and $(1,2)$ have two possible locations. The overall ambiguity for this case is 1.67. Although having more paths in the network usually decreases the ambiguity, two disjoint paths increases the ambiguity. However, notice that the ambiguity is increased only for the protection paths. The working paths have either the same ambiguity, or a reduced ambiguity. For service interrupting faults, the monitoring of the protection paths always improve the accuracy fault location accuracy. Hence, we will consider in our results only faults that affect working paths.

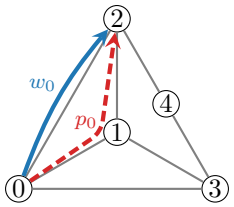
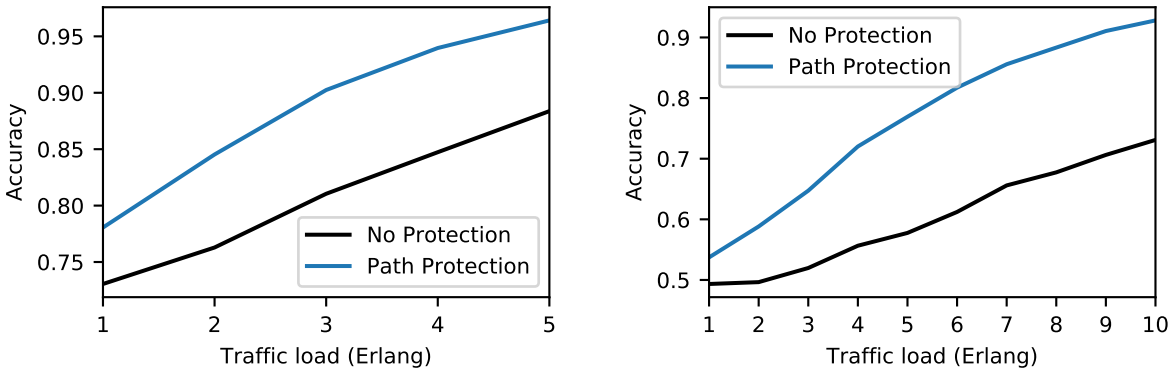


Figure 4.1: Example of two disjoint paths, p_0 and w_0 in the 5N7L network.

Fig. 4.2 shows the fault location accuracy for both networks under a traffic load ranging from 1 to 5 Erlangs for the 5N7L network, and from 1 to 10 Erlangs for the SmallNet network. This range was chosen mainly because there are no blocked request in this range. Similarly to Fig. 3.3 from section 3.4, the accuracy increases with the traffic load, and for a traffic load big enough, the accuracy will be approximately 1. By monitoring more paths we have a better accuracy for fault localization, however, it is still not possible to guarantee UFL. Table 4.1 shows the exact accuracy in percentage for specific traffic loads. There is a significant increase in accuracy, that can be a big as 9% for the 5N7L network and almost 20% for the SmallNet network. The increased accuracy is not exclusively due to having more paths to monitor. The accuracy for the SmallNet network under a traffic load of 10 Erlangs without monitoring the protection paths is 73.1%. When monitoring the the protection paths under a traffic load of 5 Erlangs, the accuracy is 76.9%. Even though both cases may have a similar number of monitored paths, the protection paths are usually longer than the working paths and disjoint from the main working path, which spreads the monitoring without having to accurately locate any fault at the protection paths.



(a) 5N7L network.

(b) SmallNet network.

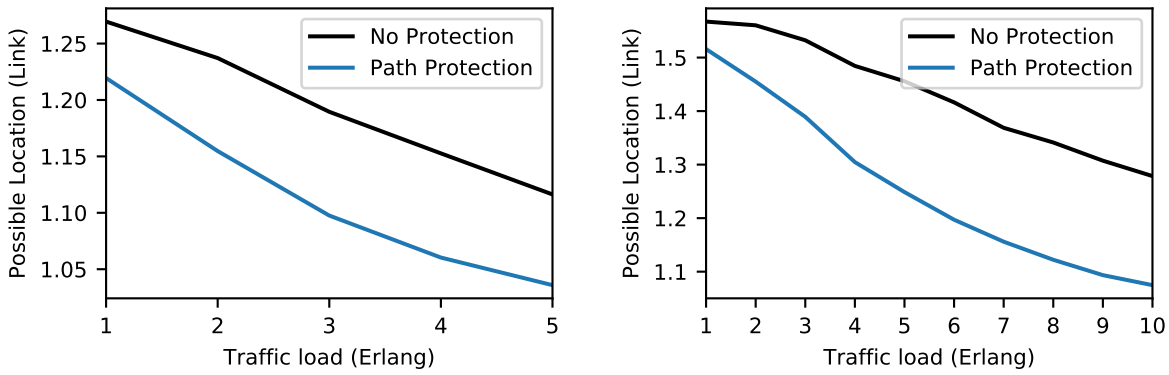
Figure 4.2: Fault location accuracy when not monitoring the protection paths and when monitoring the protection paths.

Next we have Fig. 4.3, which shows the average number of possible fault locations. The number of possible fault locations reduces as the traffic load increases. The ideal number of possible fault locations is just 1 location, as it implies we were able of unambiguously locating the network fault. If we keep increasing the traffic load, eventually we will reach for both cases values very close to 1. However, it is preferable for the network to work under a traffic loads in which either there are no blocked requests, or the blocking probability is negligible. For the considered network load, with no blocked requests, there is a significant

Monitoring	5N7L			SmallNet		
	1 Erlang	3 Erlangs	5 Erlangs	1 Erlang	5 Erlangs	10 Erlangs
No Protection	73.1%	81%	88.4%	49.3%	57.8%	73.1%
Path Protection	78.1%	90%	96.4%	53.7%	76.9%	92.8%

Table 4.1: Fault location accuracy in percentage when not monitoring the protection paths and when monitoring the protection paths.

improvement in the number of possible fault locations when monitoring the protection paths. For both networks, monitoring the protection paths can reduce the average number of possible fault locations by over 10%.



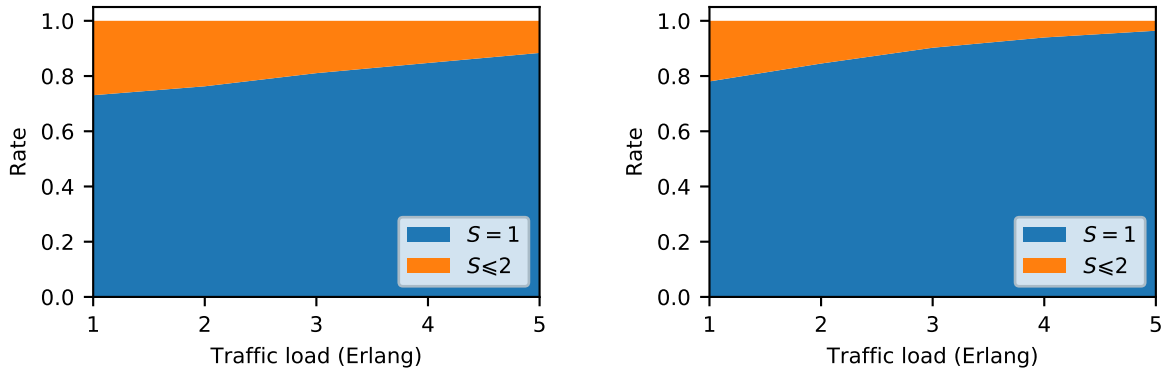
(a) 5N7L network.

(b) SmallNet network.

Figure 4.3: Average number of possible fault locations when not monitoring the protection paths and when monitoring the protection paths.

Besides just the average number of possible fault locations, it is important to also analyse the full distribution for the number of possible fault locations. We have in Figs. 4.4 and 4.5 the rate in which there are up to S possible fault locations for the 5N7L network and the SmallNet network, respectively. Notice that for $S = 1$ the curve is the same as the fault location accuracy shown in Fig. 4.2.

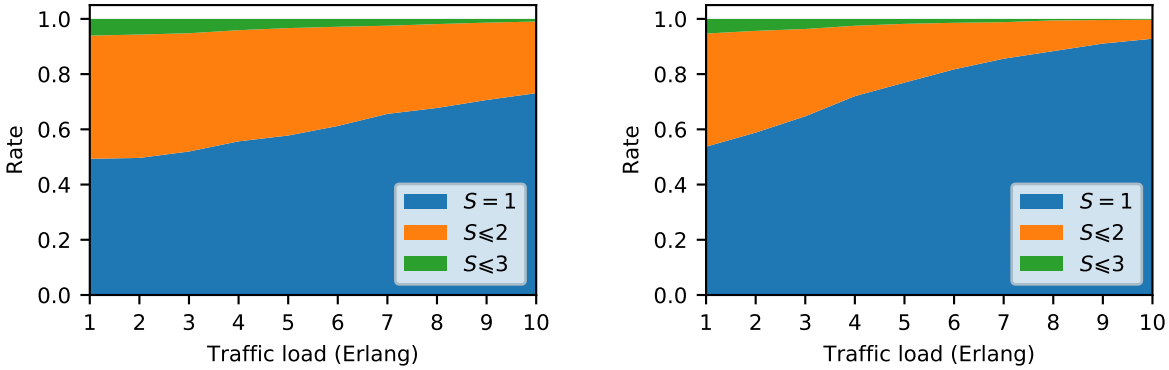
For the 5N7L network (Fig. 4.4), we have that the number of possible fault locations is always below $S = 2$, which is mainly due to the network size. We fixed the working path to be always the shortest path, and for the 5N7L topology, the minimum distance between any source-destination pairs always less or equal to 2 hops. This means that for any fault in this network we are able to always gather enough information to narrow the number of



(a) No protection.

(b) Path protection.

Figure 4.4: Rate in which the number of possible fault locations is $S = 1$ and $S \leqslant 2$ for the cases where we are not monitoring the protection paths and where we are monitoring the protection paths for the 5N7L network.



(a) No protection.

(b) Path protection.

Figure 4.5: Rate in which the number of possible fault locations is $S = 1$, $S \leqslant 2$ and $S \leqslant 3$ for the cases where we are not monitoring the protection paths and where we are monitoring the protection paths for the SmallNet network.

possible fault locations to just 2 links.

For the SmallNet network (Fig. 4.5), we have that it is very rare to have 3 possible fault locations and for the 10,000 simulated faults, and not even a single case has over 3 possible fault locations. Observe that when we monitor the protection paths, we have less

variance in the number of possible fault locations. By monitoring the protection paths, we are able to further reduce the frequency in which $S = 3$, however, it is unavoidable to have a few cases with 3 fault locations.

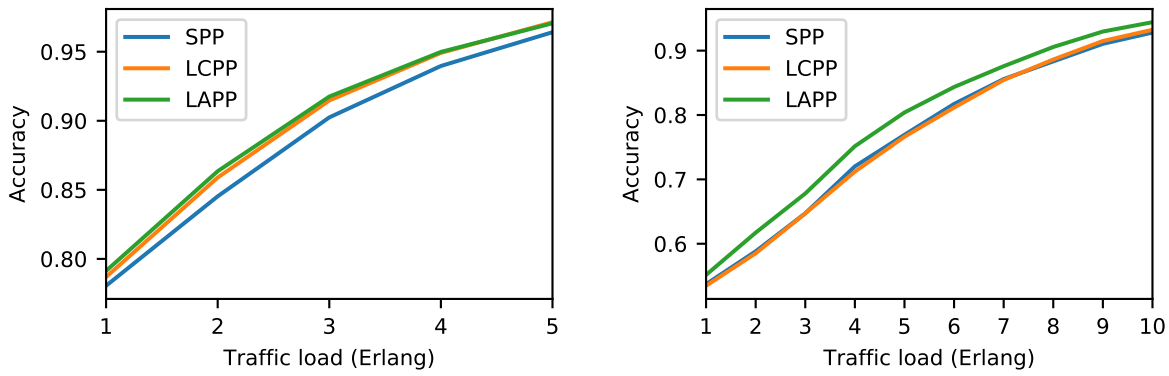
Monitoring the protection paths greatly improved the failure localization performance. However, the use of protection path comes with a cost. Since a protection path is usually longer than its working path, the number of wavelength reserved for protection can easily surpass the wavelengths used by the working paths. Since we cannot allocate the reserved wavelengths to new connection requests, there is also an increase in the blocking probability. The costs of using protection path is discussed with more detail in the next section.

4.3.2 Comparing Different Protection Routing Schemes

In this section, we will analyse the FLA-P under three different schemes, the SPP, LCPP and LAPP. We use the same set of candidate working paths and protection paths from the previous part. For the wavelength allocation we use the FF scheme for all cases. We examine the three schemes for the 5N7L network and the SmallNet network. Each link contains 16 wavelengths. The connection request follow a Poisson process, with an arrival rate of λ. The holding time are exponentially distributed, with an average of 1 time unit. We simulate $10,000$ single-link failures for each run. We considered that the MTBF follows an exponential distribution with an average of 12 time units. For most of the results, the traffic loads range from 1 to 5 Erlangs for the 5N7L network, and 1 to 10 Erlangs for the SmallNet network. This traffic range was chosen, mainly because there are no blocked requests in this range.

In Fig. 4.6 we have the fault location accuracy for both networks. The accuracy tends to increase with the network load. Differently from the results presented in section 3.4, focusing on minimizing the ambiguity does not result in a huge improvement in the performance. In fact, for the 5N7L the LCPP has almost the same performance as the LAPP, and for the SmallNet network the difference between both schemes is around 1% (see Table 4.2).While spreading the working paths resulted in a worse fault localization accuracy, spreading the protection paths actually improves it, as faults that interrupts only the protection paths are not considered when calculating the fault location accuracy. For the SmallNet, on the other hand, the LCPP scheme has the same performance of the SPP scheme, whereas the LAPP scheme outperforms the other two scheme by $1 - 4\%$. This difference is only expected to increase for bigger networks.

Fig. 4.7 shows the average number of possible fault locations. The number of possible fault location decreases as the traffic load increases. The 5N7L is a very small network,



(a) 5N7L network.

(b) SmallNet network.

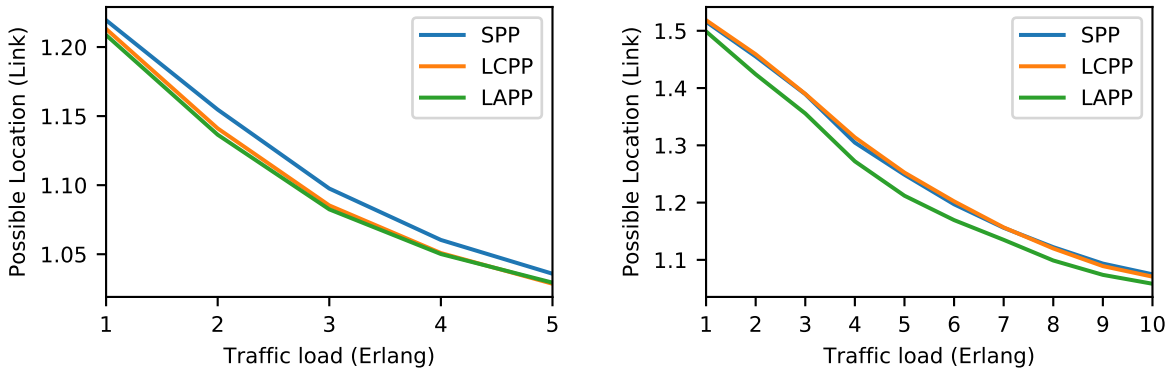
Figure 4.6: Fault location accuracy for (a) 5N7L network and (b) SmallNet network for the SPP, LCPP and LAPP schemes.

Scheme	5N7L			SmallNet		
	1 Erlang	5 Erlangs	10 Erlangs	1 Erlang	10 Erlangs	20 Erlangs
SPP	78.1%	90%	96.4%	53.7%	76.9%	92.8%
LCPP	78.7%	91.5%	97.1%	53.5%	76.6%	93.2%
LAPP	79.1%	91.8%	97.1%	55.2%	80.4%	94.4%

Table 4.2: Fault location accuracy in percentage for SPP, LCPP and LAPP.

and there are not many alternate routes disjoint from the main working path from which a protection path can choose from. As such, although the SPP curve is a little bit worse than the other schemes for the 5N7L network, there is little to no difference between the curves. For a bigger network, such as the SmallNet, there is a more significant improvement for the LAPP scheme compared to the other schemes.

Figs. 4.8 and 4.9 show the rate in which there are up to S possible fault locations for the 5N7L network and the SmallNet network, respectively. For the 5N7L network (see Fig. 4.8), we have a very similar result to the one shown in Fig. 4.4b. Once again the maximum number of possible fault location is 2, due to the network topology. Similarly, for the SmallNet network (see Fig. 4.9), we have a very similar result to the one shown in Fig. 4.5b. Once again the maximum number of possible fault location is 3, however, it is very rare. Less than 5% of the cases have over 2 possible fault locations. The maximum number of possible fault locations is mainly determined by the length of the working path. Even though monitoring the protection path can reduce the average number of possible

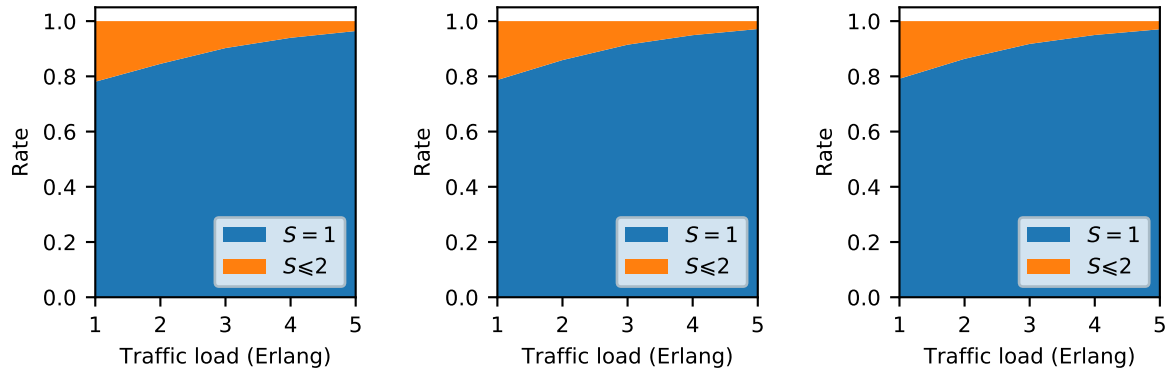


(a) 5N7L network.

(b) SmallNet network.

Figure 4.7: Average number of possible fault locations for (a) 5N7L network and (b) SmallNet network for the SPP, LCPP and LAPP schemes.

fault locations, only the working paths affects the maximum.



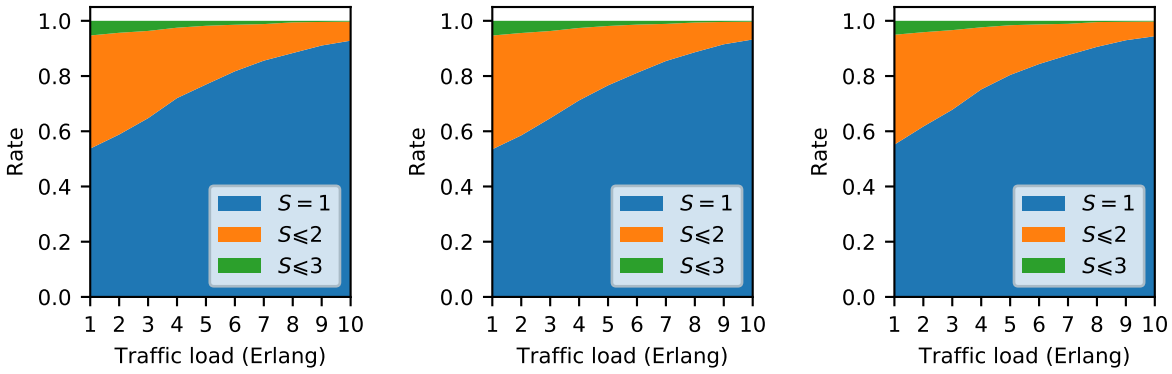
(a) SPP.

(b) LCPP.

(c) LAPP.

Figure 4.8: Rate in which the number of possible fault locations is $S = 1$ and $S \leqslant 2$ for the SPP, LCPP and LAPP schemes for the 5N7L network.

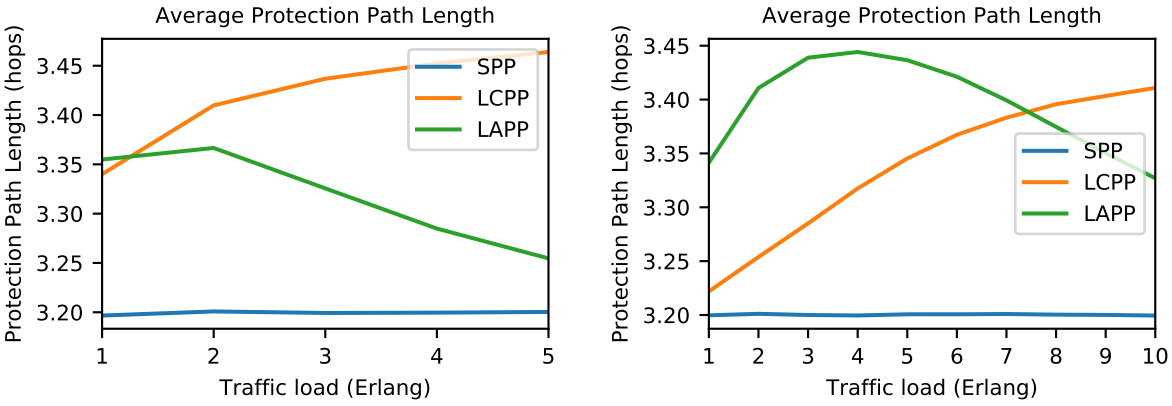
Fig. 4.10 shows the average length in hops for the protection paths. This figure is very similar to Fig. 3.8. The LAPP scheme, that prioritizes minimizing the ambiguity, has long paths for lower network loads, and as the traffic load increase the average path length decreases, until it is similar to the length of the paths from the SPP scheme. The LCPP scheme deploys longer paths for increased network loads, as it always tries to choose



(a) SPP. (b) LCPP. (c) LAPP.

Figure 4.9: Rate in which the number of possible fault locations is $S = 1$, $S \leqslant 2$ and $S \leqslant 3$ for the SPP, LCPP and LAPP schemes for the 5N7L network.

the least congested path. The SPP is constant, as it always chooses the shortest available path.



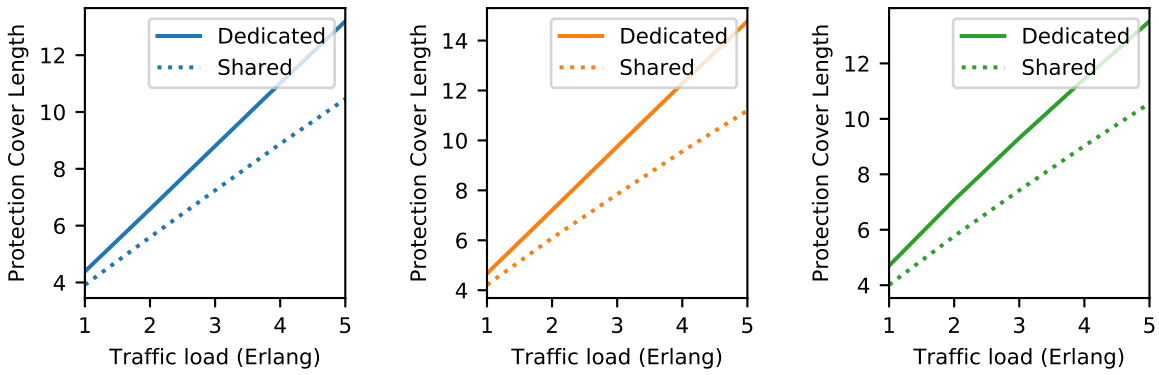
(a) 5N7L network. (b) SmallNet network.

Figure 4.10: Average protection path length for (a) 5N7L network and (b) SmallNet network for the SPP, LCPP and LAPP schemes.

The above results show that there is an increase in the failure localization performance with the LAPP scheme. However, the use of protection paths have a cost. Observe that when reserving bandwidth for the protection paths, we can either reserve a dedicated wave-

length slot for each link the protection path traverses, or we can share some wavelengths that are reserved for other protection paths, i.e. we can use either dedicated protection or shared protection. For all previous analysed results we considered dedicated protection, and the results for the failure localization metrics are the same when using either dedicated protection or shared protection. The difference in the performance of a shared protection scheme and a dedicated protection scheme is in the cover length and blocking probability. A shared protection scheme requires less bandwidth, since the protection paths can share some wavelengths whenever their respective working paths are disjoint. Since we did not consider wavelength sharing during the routing process nor during the wavelength allocation, the number of occupied wavelengths by the protection paths could be further reduced. The cover length for both dedicated and shared protection is over twice as big that the cover length for the working paths.

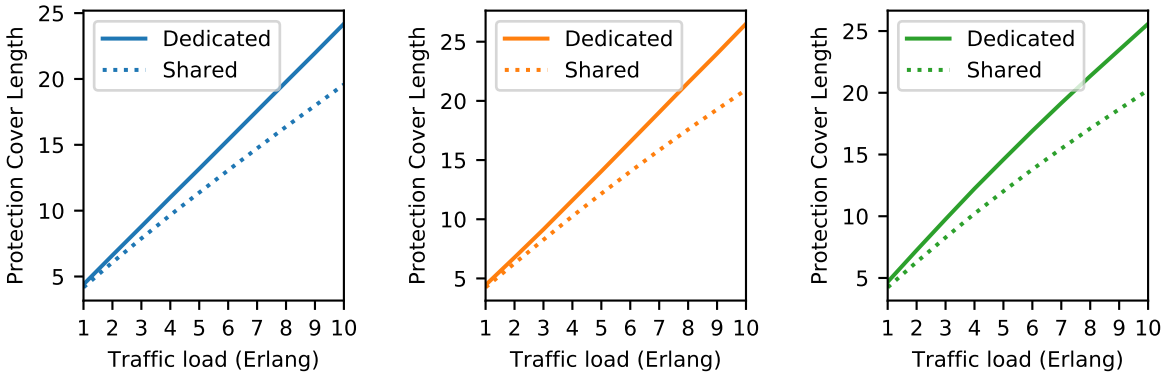
Figs. 4.11 and 4.12 show a comparison in the protection cover length for dedicated and shared protection. Protection cover length refers to the wavelengths reserved for protection paths. The LCPP scheme has the highest protection cover length between the three schemes for both networks, however, the difference between the SPP, LCPP and LAPP is very small when compared to the difference between dedicated and shared protection schemes.



(a) SPP. (b) LCPP. (c) LAPP.

Figure 4.11: Protection cover length comparison for dedicated and shared protection schemes for the 5N7L network.

For the 5N7L network (Fig. 4.11), shared protection is around 20% smaller than the dedicated protection for 5 Erlangs, and this difference will only increase with the traffic load. For the SmallNet network, we also have a decrease of around 20% for the shared



(a) SPP. (b) LCPP. (c) LAPP.

Figure 4.12: Protection cover length comparison for dedicated and shared protection schemes for the SmallNet network.

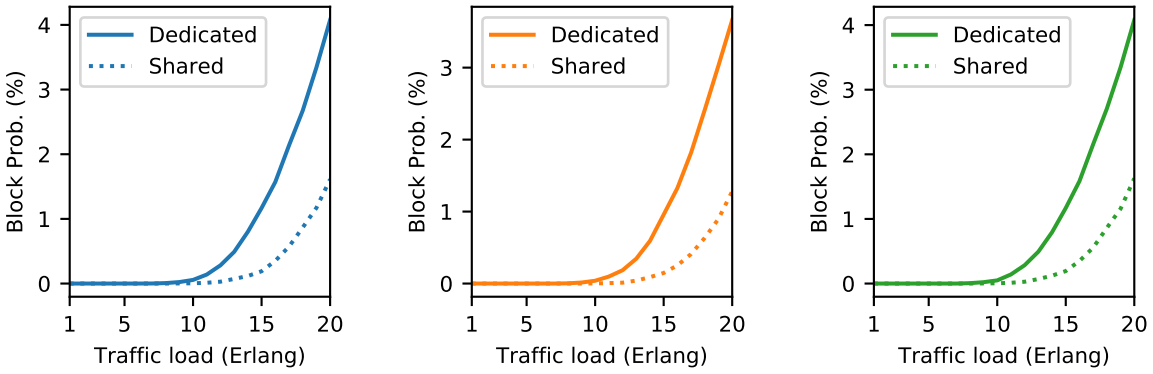
protection under a traffic load of 10 Erlangs.

Shared protection has a much better cover length than the dedicated protection, which ultimately results in a reduced blocking probability. Figs. 4.13 and 4.14 show the blocking probability the the SPP, LCPP and LAPP schemes for the 5N7L network and the SmallNet network, respectively. When comparing the blocking probability for the dedicated protection and shared protection schemes, we have that the blocking probability for the shared protection scheme is a fraction of the blocking probability for the dedicated protection schemes. For both networks we have that the blocking probability for the shared protection scheme can be less than half of the blocking probability for the dedicated protection scheme.

Notice that the LCPP scheme had an increased cover length compared to the SPP and LAPP schemes, however, it has the lowest blocking probability out of all three schemes, while the SPP and LAPP schemes have almost the same blocking probability. For dedicated protection in the 5N7L network, the blocking probability for the LCPP was around 0.4% smaller than for the other two schemes for 20 Erlangs, whereas for the SmallNet network the blocking probability for the LCPP is 0.8% smaller than the blocking probability of the SPP and LAPP schemes for 50 Erlangs.

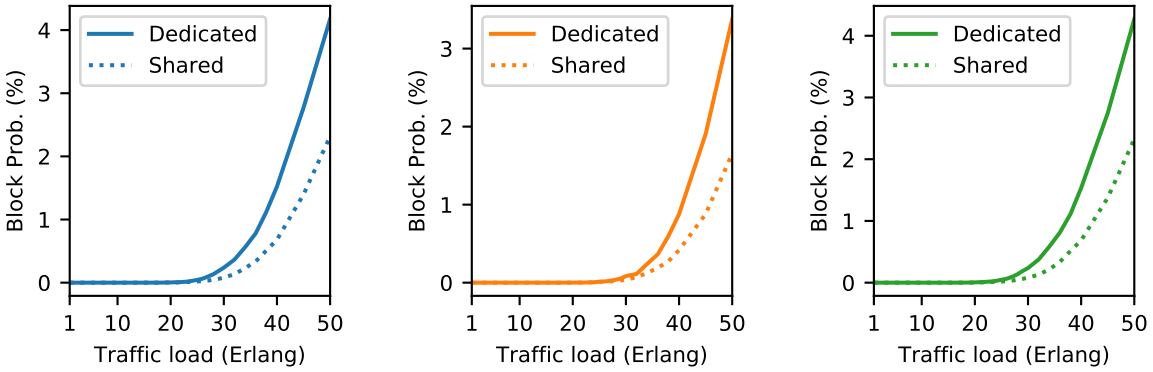
In general, the proposed LAPP is capable of outperforming both SPP and LCPP in regards to failure localization at a cost of a small increase in the blocking probability when compared to the LCPP scheme. The use of either dedicated protection or shared protection does not affect the failure localization performance, however, using shared protection does

reduce wavelength occupancy and blocking probability at the cost of not being able to restore traffic in case of multiple link failures at the same time.



(a) SPP. (b) LCPP. (c) LAPP.

Figure 4.13: Blocking Probability for dedicated and shared protection schemes for the 5N7L network.



(a) SPP. (b) LCPP. (c) LAPP.

Figure 4.14: Blocking Probability for dedicated and shared protection schemes for the SmallNet network.

Chapter 5

Conclusions and Future Work

5.1 Conclusions

In this work, we present two failure localization aware (FLA) schemes based on in-band monitoring. When probing the established lightpaths and a links fails, based on the presence and absence of alarms from the affected and unaffected paths, it is possible to either locate the fault or find a small set of possible fault locations. As the information obtained exclusively from the established lightpaths is usually not enough to achieve UFL, we introduce a metric for failure localization called *ambiguity*. Based on the concept of ambiguity, we propose a FLA-RWA scheme called LAP. The LAP algorithm precomputes offline the KSP, and for each connection request it calculates which of the pre-determined paths can service the connection request with the least ambiguity in failure localization. We then evaluated the performance of the LAP routing, compared to two classic routing schemes, the ASP and the LCP. From a failure localization perspective, the LAP scheme outperforms both ASP and LCP schemes. Compared to the ASP, the LAP scheme uses more bandwidth, but it is a negligible increase when compared to traditional out-of-band monitoring schemes, such as m-trail. Not only that, but the increased bandwidth usage is only necessary when most of the network is idle. Under heavy traffic loads, the LAP scheme has the same blocking probability as the ASP scheme.

Alternatively, we can also extend the probing from just the working paths to the protection paths. By also monitoring the protection paths, we can greatly improve the failure localization for faults in the working paths, specially in bigger networks. In order to further improve the failure localization accuracy, we propose an ambiguity based scheme to assign the routes for the protection paths, the LAPP scheme. We once again compare

the proposed scheme with two other schemes, the SPP and LCPP schemes, and we obtain similar conclusions from the previous set of routing schemes. We also compare the use of dedicated protection and shared protection for the three considered protection path monitoring schemes. From our results, we observe that the use of shared protection paths do not affect the failure localization accuracy.

5.2 Future Works

The presented FLA schemes can improve in-band failure localization, however, there are several limitations and aspects from these schemes that needs more work:

- None of the algorithms proposed in this work can guarantee UFL. One way of improving the fault localization accuracy would be to deploy some dedicated supervisory lightpaths for monitoring, similarly to an m-trail. For dynamic traffic arrivals, it may be impossible to guarantee UFL, but we may be able to get very close to it at a fraction of the cost of a full m-trail solution.

- The equation for the ambiguity (Eq. 3.1) is very complex, and its computation time increases drastically for bigger networks. To use it in real time operations for real world networks, as it is proposed here, is just unfeasible. Ideally, we should be able to define a simple heuristic to pick the least ambiguous path without having to calculate the ambiguity.

- For our simulations we obtained the candidate protection paths disjoint from the working path out of residual networks. This creates the possibility of not being to find a disjoint path due to a trap topology. There are better ways to generate a pair of path-disjoint routes, such as using Suurballe's algorithm [59]. Although the design of the protection paths presented in this work did show a significant improvement from just using the pair of the shortest available disjoint-paths as the working and protection path, an algorithm that configured the routes of both working and protection paths should be able to easily surpass the results presented here.

- There are several works in the literature that uses a machine learning algorithm to predict traffic arrivals. To use such predictions to design an optimal route allocation for fault detection could improve the fault localization accuracy.

References

[1] Mohamed Al-Kuwaiti, Nicholas Kyriakopoulos, and Sayed Hussein. A comparative analysis of network dependability, fault-tolerance, reliability, security, and survivability. *IEEE Communications Surveys & Tutorials*, 11(2):106–124, 2009.

[2] Vishal Anand, Sunit Chauhan, and Chunming Qiao. Sub-path protection: A new framework for optical layer survivability and its quantitative evaluation. 2002.

[3] Péter Babarczi, János Tapolcai, and Pin-Han Ho. Adjacent link failure localization with monitoring trails in all-optical mesh networks. *IEEE/ACM transactions on networking*, 19(3):907–920, 2011.

[4] Richard A Barry and Pierre A Humblet. Models of blocking probability in all-optical networks with and without wavelength changers. In *Proceedings of INFOCOM'95*, volume 2, pages 402–412. IEEE, 1995.

[5] Bela Bollobas. *Graph theory: an introductory course*, volume 63. Springer Science & Business Media, 2012.

[6] Paul A Bonenfant. Optical layer survivability: a comprehensive approach. In *OFC'98. Optical Fiber Communication Conference and Exhibit. Technical Digest. Conference Edition. 1998 OSA Technical Digest Series Vol. 2 (IEEE Cat. No. 98CH36177)*, pages 270–271. IEEE, 1998.

[7] Anastasios T Bouloutas, Seraphin Calo, and Allan Finkel. Alarm correlation and fault identification in communication networks. *IEEE Transactions on communications*, 42(234):523–533, 1994.

[8] Kit-man Chan and Tak-shing Peter Yum. Analysis of least congested path routing in wdm lightwave networks. In *Proceedings of INFOCOM'94 Conference on Computer Communications*, pages 962–969. IEEE, 1994.

[9] Xiaoliang Chen, Shilin Zhu, Liu Jiang, and Zuqing Zhu. On spectrum efficient failure-independent path protection p-cycle design in elastic optical networks. *Journal of Lightwave technology*, 33(17):3719–3729, 2015.

[10] Edsger W Dijkstra et al. A note on two problems in connexion with graphs. *Numerische mathematik*, 1(1):269–271, 1959.

[11] Bharat T Doshi, Subrahmanyam Dravida, P Harshavardhana, Oded Hauser, and Yufei Wang. Optical network design and restoration. *Bell Labs Technical Journal*, 4(1):58–84, 1999.

[12] Georgios Ellinas, Eric Bouillet, Ramu Ramamurthy, Jean-Francois Labourdette, Sid Chaudhuri, and Krishna Bala. Routing and restoration architectures in mesh optical networks. *Optical Networks Magazine*, 4(1):91–106, 2003.

[13] Georgios Ellinas, Aklilu Gebreyesus Hailemariam, and Thomas E Stern. Protection cycles in mesh wdm networks. *IEEE Journal on Selected Areas in Communications*, 18(10):1924–1937, 2000.

[14] Alex Ferguson, Barry O'Sullivan, and Dan Kilper. Impact of wavelength route correlation on the optimal placement of optical monitors in transparent mesh networks. In *2008 34th European Conference on Optical Communication*, pages 1–2. IEEE, 2008.

[15] Alex Ferguson, Barry O'Sullivan, and Daniel C Kilper. Transparent path length optimized optical monitor placement in transparent mesh networks. In *Optical Fiber Communication Conference*, page OThI3. Optical Society of America, 2008.

[16] Andrea Fumagalli, Isabella Cerutti, and Marco Tacca. Optimal design of survivable mesh networks based on line switched wdm self-healing rings. *IEEE/ACM Transactions on networking*, 11(3):501–512, 2003.

[17] Ruoxuan GAO, Lei LIU, Xiaomin LIU, Huazhi LUN, Lilin YI, Weisheng HU, and Qunbi ZHUGE. An overview of ml-based applications for next generation optical networks. *Information Sciences*, 63(160302):1–160302, 2020.

[18] Robert D Gardner and David A Harle. Pattern discovery and specification techniques for alarm correlation. In *NOMS 98 1998 IEEE Network Operations and Management Symposium*, volume 3, pages 713–722. IEEE, 1998.

[19] Ori Gerstel and Shay Kutten. Dynamic wavelength allocation in all-optical ring networks. In *Proceedings of ICC'97-International Conference on Communications*, volume 1, pages 432–436. IEEE, 1997.

[20] Ornan Gerstel and Rajiv Ramaswami. Optical layer survivability: a services perspective. *IEEE Communications magazine*, 38(3):104–113, 2000.

[21] Mukul Goyal, Guangzhi Li, and Jennifer Yates. Shared mesh restoration: a simulation study. In *Optical Fiber Communication Conference*, page ThO2. Optical Society of America, 2002.

[22] Mukul Goyal, KK Ramakrishnan, and Wu-chi Feng. Achieving faster failure detection in ospf networks. In *IEEE International Conference on Communications, 2003. ICC'03.*, volume 1, pages 296–300. IEEE, 2003.

[23] CG Gruber. Resilient networks with non-simple p-cycles. In *10th International Conference on Telecommunications, 2003. ICT 2003.*, volume 2, pages 1027–1032. IEEE, 2003.

[24] Ahmed Haddad, Elias A Doumith, and Maurice Gagnaire. A fast and accurate metaheuristic for failure localization based on the monitoring trail concept. *Telecommunication Systems*, 52(2):813–824, 2013.

[25] José Alberto Hernández. Learning from data: Applications of machine learning in optical network design and modeling. In *2020 International Conference on Optical Network Design and Modeling (ONDM)*, pages 1–6. IEEE, 2020.

[26] Pin-Han Ho and Hussein T Mouftah. A framework for service-guaranteed shared protection in wdm mesh networks. *IEEE Communications Magazine*, 40(2):97–103, 2002.

[27] Brigitte Jaumard, Christophe Meyer, and Babacar Thiongane. Comparison of ilp formulations for the rwa problem. *Optical Switching and Networking*, 4(3-4):157–172, 2007.

[28] Irene Katzela and Mischa Schwartz. Schemes for fault identification in communication networks. *IEEE/ACM Transactions on networking*, 3(6):753–764, 1995.

[29] Yousef S Kavian, Yousef S Kavian, and Mark S Leeson. *Resilient Optical Network Design: Advances in Fault-tolerant Methodologies*. IGI Publishing, 2011.

[30] Sunggy Koo and Suresh Subramaniam. Trade-offs between speed, capacity, and restorability in optical mesh network restoration. In *Optical Fiber Communication Conference*, page ThO1. Optical Society of America, 2002.

[31] Jean-Franćois Labourdette and Z Zhang. Opaque and transparent networking. *Optical Networks Magazine*, 4(3), 2003.

[32] Ma łgorzata Steinder and Adarshpal S Sethi. A survey of fault localization techniques in computer networks. *Science of computer programming*, 53(2):165–194, 2004.

[33] Mari W Maeda. Management and control of transparent optical networks. *IEEE Journal on Selected Areas in Communications*, 16(7):1008–1023, 1998.

[34] Ignacio Martín, José Alberto Hernández, Sebastian Troia, Francesco Musumeci, Guido Maier, and Oscar González de Dios. Is machine learning suitable for solving rwa problems in optical networks? In *2018 European Conference on Optical Communication (ECOC)*, pages 1–3. IEEE, 2018.

[35] Ignacio Martín, Sebastian Troia, José Alberto Hernández, Alberto Rodríguez, Francesco Musumeci, Guido Maier, Rodolfo Alvizu, and Óscar González de Dios. Machine learning-based routing and wavelength assignment in software-defined optical networks. *IEEE Transactions on Network and Service Management*, 16(3):871–883, 2019.

[36] Carmen Mas, Olivier Crochat, and Jean-Yves Le Boudec. Fault localization for optical networks. In *All-Optical Networking: Architecture, Control, and Management Issues*, volume 3531, pages 408–419. International Society for Optics and Photonics, 1998.

[37] Carmen Mas, Ioannis Tomkos, and Ozan K Tonguz. Failure location algorithm for transparent optical networks. *IEEE Journal on Selected Areas in Communications*, 23(8):1508–1519, 2005.

[38] Gurusamy Mohan, C Siva Ram Murthy, and Arun K Somani. Efficient algorithms for routing dependable connections in wdm optical networks. *IEEE/ACM transactions on Networking*, 9(5):553–566, 2001.

[39] Hussein T Mouftah and Pin-Han Ho. *Optical Networks: Architecture and Survivability*. Springer Science & Business Media, 2003.

[40] Hussein T Mouftah and Pin-Han Ho. *Optical networks: architecture and survivability*. Springer Science & Business Media, 2012.

[41] Puspendu Nayek, Sayan Pal, Buddhadev Choudhury, Amitava Mukherjee, Debashis Saha, and Mita Nasipuri. Optimal monitor placement scheme for single fault detection in optical network. In *Proceedings of 2005 7th International Conference Transparent Optical Networks, 2005.*, volume 1, pages 433–436. IEEE, 2005.

[42] Yasuko Nozu, Yasuhiko Aoki, Kosuke Komaki, and Satoru Okano. 'conscious optical network'with reliability and flexibility. *Fujitsu Sci. Tech. J.*, 52(2):75–82, 2016.

[43] Canhui Ou, Hui Zang, Narendra K Singhal, Keyao Zhu, Laxman H Sahasrabuddhe, Robert A MacDonald, and Biswanath Mukherjee. Subpath protection for scalability and fast recovery in optical wdm mesh networks. *IEEE Journal on Selected Areas in Communications*, 22(9):1859–1875, 2004.

[44] Canhui Sam Ou and Biswanath Mukherjee. *Survivable optical WDM networks*. Springer Science & Business Media, 2005.

[45] Amitangshu Pal, Amitava Mukherjee, Mrinal K Naskar, and Mita Nasipuri. Minimal monitor activation and fault localization in optical networks. *Optical Switching and Networking*, 8(1):46–55, 2011.

[46] Tania Panayiotou, Sotirios P Chatzis, and Georgios Ellinas. A probabilistic approach for failure localization. In *2017 International Conference on Optical Network Design and Modeling (ONDM)*, pages 1–6. IEEE, 2017.

[47] Tania Panayiotou, Sotirios P Chatzis, and Georgios Ellinas. Leveraging statistical machine learning to address failure localization in optical networks. *IEEE/OSA Journal of Optical Communications and Networking*, 10(3):162–173, 2018.

[48] Tania Panayiotou, Konstantinos Manousakis, Sotirios P Chatzis, and Georgios Ellinas. A data-driven bandwidth allocation framework with qos considerations for eons. *Journal of Lightwave Technology*, 37(9):1853–1864, 2019.

[49] Senthil Ramamurthy and Biswanath Mukherjee. Survivable wdm mesh networks. part i-protection. In *IEEE INFOCOM'99. Conference on Computer Communications. Proceedings. Eighteenth Annual Joint Conference of the IEEE Computer and Communications Societies. The Future is Now (Cat. No. 99CH36320)*, volume 2, pages 744–751. IEEE, 1999.

[50] Sumathi Ramamurthy, Laxman Sahasrabuddhe, and Biswanath Mukherjee. Survivable wdm mesh networks. *Journal of Lightwave Technology*, 21(4):870, 2003.

[51] Rajiv Ramaswami, Kumar Sivarajan, and Galen Sasaki. *Optical networks: a practical perspective*. Morgan Kaufmann, 2009.

[52] Rajiv Ramaswami and Kumar N Sivarajan. Routing and wavelength assignment in all-optical networks. *IEEE/ACM Transactions on networking*, 3(5):489–500, 1995.

[53] Dominic A Schupke, Claus G Gruber, and Achim Autenrieth. Optimal configuration of p-cycles in wdm networks. In *2002 IEEE International Conference on Communications. Conference Proceedings. ICC 2002 (Cat. No. 02CH37333)*, volume 5, pages 2761–2765. IEEE, 2002.

[54] BR Lu Shen and Xi Yang. Survivable WDM mesh networks, Part II - restoration. In *IEEE ICC*, volume 3, pages 2023–2030, 1999.

[55] Ryuta Shiraki, Yojiro Mori, Hiroshi Hasegawa, and Ken-ichi Sato. Dynamically controlled flexible-grid networks based on semi-flexible spectrum assignment and network-state-value evaluation. In *Optical Fiber Communication Conference*, pages M1B–4. Optical Society of America, 2020.

[56] Sava Stanic, Gokhan Sahin, Hongsik Choi, Suresh Subramaniam, and Hyeong-Ah Choi. Monitoring and alarm management in transparent optical networks. In *2007 Fourth International Conference on Broadband Communications, Networks and Systems (BROADNETS'07)*, pages 828–836. IEEE, 2007.

[57] Sava Stanic, Suresh Subramaniam, Hongsik Choi, Gokhan Sahin, and Hyeong-Ah Choi. On monitoring transparent optical networks. In *Proceedings. International Conference on Parallel Processing Workshop*, pages 217–223. IEEE, 2002.

[58] Sava Stanic, Suresh Subramaniam, Gokhan Sahin, Hongsik Choi, and Hyeong-Ah Choi. Active monitoring and alarm management for fault localization in transparent all-optical networks. *IEEE Transactions on Network and Service Management*, 7(2):118–131, 2010.

[59] JW Suurballe. Disjoint paths in a network. *Networks*, 4(2):125–145, 1974.

[60] János Tapolcai, Pin-Han Ho, Lajos Rónyai, Péter Babarczi, and Bin Wu. Failure localization for shared risk link groups in all-optical mesh networks using monitoring trails. *Journal of Lightwave Technology*, 29(10):1597–1606, 2011.

[61] János Tapolcai, Pin-Han Ho, Lajos Rónyai, and Bin Wu. Network-wide local unambiguous failure localization (nwl-ufl) via monitoring trails. *IEEE/ACM Transactions on Networking*, 20(6):1762–1773, 2012.

[62] János Tapolcai, Bin Wu, Pin-Han Ho, and Lajos Rónyai. A novel approach for failure localization in all-optical mesh networks. *IEEE/ACM Transactions on Networking*, 19(1):275–285, 2010.

[63] Dongmei Wang, Guangzhi Li, Jennifer Yates, and Chuck Kalmanek. Efficient segment-by-segment restoration. In *Optical Fiber Communication Conference*, page TuP2. Optical Society of America, 2004.

[64] Jian Wang, Laxman Sahasrabuddhe, and Biswanath Mukherjee. Fault monitoring and restoration in optical wdm networks. In *National Fiber Optic Engineers Conference*. Citeseer, 2002.

[65] Jian Wang, Laxman Sahasrabuddhe, and Biswanath Mukherjee. Path vs. subpath vs. link restoration for fault management in ip-over-wdm networks: performance comparisons using gmpls control signaling. *IEEE Communications Magazine*, 40(11):80–87, 2002.

[66] Bin Wu, Pin-Han Ho, Janos Tapolcai, and Xiaohong Jiang. A novel framework of fast and unambiguous link failure localization via monitoring trails. In *2010 INFOCOM IEEE Conference on Computer Communications Workshops*, pages 1–5. IEEE, 2010.

[67] Bin Wu, Pin-Han Ho, and Kwan L Yeung. Monitoring trail: a new paradigm for fast link failure localization in wdm mesh networks. In *IEEE GLOBECOM 2008-2008 IEEE Global Telecommunications Conference*, pages 1–5. IEEE, 2008.

[68] Bin Wu, Pin-Han Ho, and Kwan L Yeung. Monitoring trail: On fast link failure localization in all-optical wdm mesh networks. *Journal of Lightwave Technology*, 27(18):4175–4185, 2009.

[69] Bin Wu, Pin-Han Ho, Kwan L Yeung, János Tapolcai, and Hussein T Mouftah. Optical layer monitoring schemes for fast link failure localization in all-optical networks. *IEEE Communications Surveys & Tutorials*, 13(1):114–125, 2010.

[70] Bin Wu, Kwan L Yeung, and Pin-Han Ho. Monitoring cycle design for fast link failure localization in all-optical networks. *Journal of lightwave technology*, 27(10):1392–1401, 2009.

[71] Bin Wu, Kwan L Yeung, Bing Hu, and Pin-Han Ho. M2-cycle: An optical layer algorithm for fast link failure detection in all-optical mesh networks. *Computer Networks*, 55(3):748–758, 2011.

[72] Bin Wu, Kwan L Yeung, and Shizhong Xu. Ilp formulation for p-cycle construction based on flow conservation. In *IEEE GLOBECOM 2007-IEEE Global Telecommunications Conference*, pages 2310–2314. IEEE, 2007.

[73] LUO Xiao, SHI Chen, CHEN Xue, LI Yang, and Tao Yang. Comprehensive performance study of elastic optical networks for distributed datacenter with survivability. In *Optical Fiber Communication Conference*, pages Th2A–23. Optical Society of America, 2019.

[74] Dahai Xu, Yizhi Xiong, and Chunming Qiao. Novel algorithms for shared segment protection. *IEEE Journal on Selected areas in Communications*, 21(8):1320–1331, 2003.

[75] Boyuan Yan, Yongli Zhao, Yajie Li, Xiaosong Yu, Jie Zhang, Ying Wang, Longchun Yan, and Sabidur Rahman. Actor-critic-based resource allocation for multi-modal optical networks. In *2018 IEEE Globecom Workshops (GC Wkshps)*, pages 1–6. IEEE, 2018.

[76] Jennifer M Yates, Michael P Rumsewicz, and Jonathan PR Lacey. Wavelength converters in dynamically-reconfigurable wdm networks. *IEEE Communications Surveys*, 2(2):2–15, 1999.

[77] Jin Y Yen. Finding the k shortest loopless paths in a network. *management Science*, 17(11):712–716, 1971.

[78] Hui Zang, Jason P Jue, Biswanath Mukherjee, et al. A review of routing and wavelength assignment approaches for wavelength-routed optical wdm networks. *Optical networks magazine*, 1(1):47–60, 2000.

[79] Hongqing Zeng and Changcheng Huang. Fault detection and path performance monitoring in meshed all-optical networks. In *IEEE Global Telecommunications Conference, 2004. GLOBECOM'04.*, volume 3, pages 2014–2018. IEEE, 2004.

[80] Hongqing Zeng, Changcheng Huang, and Alex Vukovic. A novel fault detection and localization scheme for mesh all-optical networks based on monitoring-cycles. *Photonic Network Communications*, 11(3):277–286, 2006.

[81] Hongqing Zeng and Alex Vukovic. The variant cycle-cover problem in fault detection and localization for mesh all-optical networks. *Photonic Network Communications*, 14(2):111–122, 2007.

[82] Yangming Zhao, Shizhong Xu, Xiong Wang, and Sheng Wang. A new heuristic for monitoring trail allocation in all-optical wdm networks. In *2010 IEEE Global Telecommunications Conference GLOBECOM 2010*, pages 1–5. IEEE, 2010.

Glossary

cover length Total number of wavelengths dedicated to fault localization. 10, 22, 23, 26, 31, 33, 46, 47

cycle cover A set of cycles that covers every node and edge of the network at least once. 12

dedicated protection Each protection path has its own dedicated bandwidth. 19, 46, 47, 50

Eulerian cycle A cycle that passes through every node at least once. 12

Eulerian graph A connected graph where each node has an even degree, i.e., each node connects to an even number of nodes [5]. 12

hard fault Faults that completely interrupts the signal. 7

in-band monitoring Monitoring established lightpaths to locate failures in the network. 7–10, 49

lightpath All optical WDM-channel that may span through multiple links. Two lightpaths cannot occupy the same wavelength in the same link because they will interfere with each other. 2, 4, 8–11, 18, 19, 21–23, 26, 31, 35, 49

out-of-band monitoring Monitoring scheme that deploys a dedicated supervisory lightpath with a monitor at the end node. 7, 10, 11, 49

protection path Lightpath with an alternate route that carries the traffic in case the main path fails. 2, 18–20, 35–46, 49, 50

shared protection Protection paths from disjoint working paths can traverse the same link while occupying the same wavelength, i.e. protection paths can share wavelengths with other protection paths. 19, 46, 47, 50

soft fault Faults that degrades signal quality. 7

spanning tree A tree that contains all vertices (nodes) on the graph [5]. 12

wavelength-continuity constraint A lightpath must occupy the same wavelength throughout all links it passed through, unless there are wavelengths converters. 4, 5, 24

working path Lightpath that carries the traffic during normal operation. 2, 18–20, 31, 35–40, 42–44, 46, 49, 50