Study of the mechanisms associated with the preventive network restoration in fiber optic core networks

Jelena Pesic

N° d'ordre : 2012telb0228

Sous le sceau de l'Université européenne de Bretagne

Télécom Bretagne

En habilitation conjointe avec l'Université de Bretagne-Sud

Ecole Doctorale – Sicma

Etudes des mécanismes réseaux associés à la restauration préventive dans le réseau cœur à fibre optiques

---

Thèse de Doctorat

Mention : STIC

Présentée par **Jelena Pesic**

Département : OPTIQUE

Laboratoire : Orange Labs

Directeur de thèse : Laurent Dupont

Soutenue le 6 avril 2012

Jury :

M. Slavko Pokorni, Professeur, Information Technology School, Belgrade (Rapporteur)
M. Bernard Cousin, Professeur, IRISA, Rennes (Rapporteur)
M. Marc Sevaux, Professeur, UBS, Lorient (Examinateur)
M. Yves Jaouen, Professeur, Télécom Paris Tech, Paris (Examinateur)
Mme Esther Le Rouzic, Ingénieur, Orange Labs, Lannion (Examinatrice, encadrante)
M. Laurent Dupont, Professeur, Département d'Optique, Télécom Bretagne, Brest
M. Michel Morvan, Ingénieur d'études, Département d'Optique, Télécom Bretagne, Brest
M. Philippe Gravey, Directeur d'études, Département d'Optique, Télécom Bretagne, Brest

ACKNOWLEDGEMENTS

The way you get good ideas is by working with the talented people who are also fun to be with. Orange labs is a wonderful place to work, so many great colleagues that gave me all the support I needed while working on this manuscript. I would like to thank to members of the entire SOAN team guided by Dr. Maryse Guena Moignard.

My special thanks go to Dr. Esther Le Rouzic. I am deeply indebted to her for her support over the years, for her boundless patience, for her constantly being there for me, not only as a colleague but also as a friend and last for helping me revise and piece together this manuscript. Her comments on general organization of the manuscript, have greatly improved the work, both in content and form. It is an honor to have called her my supervisor these past three years. Merci Esther.

I would like to thank Professor Laurent Dupont for believing in me from the start, for following and supporting me throughout these years. Suggestions received from him and Michel Morvan are precious for my research.

I am grateful to Professor Bernard Cousin and to Professor Slavko Pokorni for accepting the role of reporters. Also I would like to thank Professor Yves Jaouen, Professor Marc Sevaux and Michel Morvan for serving on my thesis examination committee.

I would also like to show my gratitude to Dr. Fabrice Clérot who directed me in machine learning studies. His kind support and guidance have been of great value in this study.

I warmly thank to Professor Annie Gravey and to Philippe Gravey for their presence in my life and for their endless support.

I would also like to show my gratitude to other students: Julie, Abud, Nassima, Sofienne, Ahmed, Edoardo (mamma mia), Paul (Bol), Damien and of course Dior for all the great moments spent together. Also, I would like to thank Julien Meuric for his expert advices at many stages along the course of this project.

Special thanks go to Mathieu Berger for supports and being there for me during these three years.

And finally, I would like to thank my father and brother for giving me precious advices, strength and courage to finish this manuscript and to keep my head up smiling no matter what happens.

Table of Contents

List of Tables

List of Figures

List of Symbols

ANN	Artificial Neural Networks
APS	Automatic Protection Switching
ATM	Asynchronous Transfer Mode
B&S	Broadcast and Select
BFD	Bidirectional Forwarding Detection
BN	Bayesian Network
BP	Back Propagation
CD	Chromatic Dispersion
CWDM	Conventional/Coarse Wavelength Division Multiplexing
DEMUX	De-multiplexer
DGD	Differential Group Delay
DWDM	Dense Wavelength Division Multiplexing
EDFA	Erbium Doped Fiber Amplifier
FBG	Fiber Bragg Grating
FCC	Federal Communications Commission
FIT	Failure In Time
FN	False Negative
FP	False Positive
FT	Fourier Transformation
HDPE	High-Density Polyethylene
IGP	Interior Gateway Protocol
IP	Internet Protocol
ITU	International Telecommunications Union
LOS	Loss Of Signal
ML	Machine Learning
MPLS	Multiprotocol Label Switching
MPLS FRR	Multi-Protocol Label Switching Fast Re-Route
MTBF	Mean Time Between Failures
MTTF	Mean Time To Failure
MTTR	Mean Time To Repair
MUX	Multiplexer

OADM	Optical Add/Drop Multiplexers
OCh	Optical Channel layer
OFDM	Orthogonal Frequency-Division Multiplexing
OMS	Optical Multiplex Section layer
OSI	Open Systems Interconnection
OTN	Optical Transport Network
OTS	Optical Transmission Section layer
OXC	Optical Cross-Connects
PMD	Polarization Mode Dispersion
PMDC	Polarization Mode Dispersion Compensation
PVC	Polyvinyl Chloride
QoS	Quality of Service
RBF	Radial Basis Function networks
ROADM	Reconfigurable Optical Add-Drop Multiplexer
S&C	Select and Combine
SDH	Synchronous Digital Hierarchy
SLA	Service Level Agreement
SONET	Synchronous Optical Network
SOP	State of Polarization
SRLG	Shared Risk Link Group
SVM	Support Vector Machines
TCP	Transmission Control Protocol
TDM	Time Division Multiplexing
TN	True Negative
TP	True Positive
WDM	Wavelength Division Multiplexing
WSS	Wavelength Selective Switch

1 Chapter
INTRODUCTION

Fiber optics has become the core of today's telecommunications and data networking infrastructures. Thanks to its advantageous properties like low attenuation, huge bandwidth and immunity against electromagnetic interference fiber cables are replacing existing copper cables. They have been widely deployed to realize high-speed links that may carry either a single wavelength channel or multiple wavelength channels by means of wavelength division multiplexing (WDM). The rapid evolution of technology, coupled with the insatiable demand for bandwidth resulted with the existence of two generations of fiber optic networks.

The first generation of fiber optic networks called point-to-point networks used optical fiber for simple transmission at high bit rates over longer distances. In these networks at every intermediate node an optical signal is converted to an electrical signal, buffered, processed and transmitted again as the optical signal. Despite the large transmission capacity, costly optical-electrical-optical conversions represent one of the largest expenditures in terms of power consumption, footprint, port count and processing overhead.

The second generation of fiber optics networks is now being deployed. It exploits routing and switching of signals in the optical domain. Data are transmitted between two nodes using a lightpath without requiring any electro-optical conversion and buffering at the intermediate nodes. A Lightpath is an optical connection that is carried end to end from a source node to a destination node over a wavelength on each intermediate link. If the network has wavelength conversion capabilities, lightpath can be converted from one wavelength to another wavelength as well along their route. This allows the same wavelength to be reused spatially in different parts of the network. The key network elements that enable optical networking are optical add/drop multiplexers (OADMs), and optical cross-connects (OXC).

Having such a complex network carrying great amount of the traffic, control functions are necessary to set up, modify, and tear down optical circuits such as lightpaths. This is done by (re)configuring tunable transmitters, receivers, wavelength converters, and reconfigurable OADMs and OXCs along the path. As the survivability is considered as one of the most important features of optical networks, control functions are also used to monitor optical networks and guarantee their proper operation by isolating and diagnosing network failures and by triggering recovery mechanisms.

Existing recovery mechanisms make optical networks fault-tolerant. Fault tolerance refers to the ability of the network to reconfigure and reestablish communication upon a failure. Usual recovery mechanisms that deal with network failures can be divided into protection and restoration. The protection mechanism activates in advance backup resource that will be used in case of failure, while the restoration mechanism takes over backup resource upon a failure; that is why protection mechanisms can recover quickly but are more demanding in terms of resource. Restoration mechanisms are less demanding when it comes to resource and therefore may be less costly than protection mechanisms in term of initial investments, but they generate longer service disruption.

Recovery may be provided at optical layer or the higher layer of the OSI (Open Systems Interconnection) network model. For example it can be done at the physical WDM layer using a dedicated control plane, in an electrical circuit layer like SDH (Synchronous Digital Hierarchy), SONET (Synchronous Optical Network) or OTN (Optical Transport Network), or it can be done at the IP (Internet Protocol) layer. Also it can be done locally, link based method that employs local detouring or globally, path based method that employs end to end detouring. Similarly, the difference can be made based on how the backup resources are shared. As we can see there are different types of recovery, but common to all of them is that they are triggered after the failure is detected. That makes them reactive.

The goal of the work conducted during this thesis was to find a solution for technical implementation of the proactive fault detection and fast recovery in the core optical network. This dissertation outlines the different solutions and their evaluation from the point of view of the network telecommunications operator.

The motivation for this work comes from the study concerning the most frequent reasons for the network failures. Depending on the environment fiber is exposed to various risk factors. For example, terrestrial cables are frequently exposed to mechanical engines (wayward backhoes) that can cut fiber by accident or rodents that eat up cable coatings. Aerial cables are often exposed to mechanical engines for tree cutting or alike. Besides these external causes, failures may also occur due to human mistakes and other equipment failures, but the most frequent ones are caused by dig-ups, representing almost 60 percent of the all the failures in France Telecom cable infrastructure. Finding a method that would be able to proactively detect potential fiber cut in the backbone optical network caused by construction work i.e. digs-ups was the main objective of this work.

First chapter of this thesis is devoted to reviewing the existing recovery methods in the optical networks. In order to understand this thesis it is necessary to establish the vocabulary and basic elements of telecommunications and in particular fiber-optic communications. For that reason we will start with the description of the building

blocks of the optical network and the used technologies followed by the source of motivation for this study, so–called reasons for network failures and their recurrences.

Chapter II addresses the existing methods of prediction. This part covers the area of machine learning. Once the reader has been introduced to the typical methods for prediction, an enhanced system design is proposed.

Chapter III consolidates all the previous review work to an estimation of the most promising technique for proactive fault detection. An experimental test bed using fiber as a sensor was set up and used to quantify exactly the performance of the selected solution. This requires building an advanced representation of data that was used as input data for machine learning software. The relative importance of some effects is discussed. Once a deeper understanding of the potential of this technique has been achieved with an experimental test bed, theoretical investigations through the development of analytical models are conducted to validate and generalize them.

Chapter IV describes the advantages and drawbacks of this kind of detection. Simulations were made that prove the knowledge obtained using the test-bed. Later on, a case study concerning the phase of recovery in the transport network is presented.

Finally, the last chapter is devoted to conclusions and the presentation of perspectives that result from this study.

This work involves and undergoes through three different areas of research: the area of optical networks, the area of using fiber as a sensor and machine learning area. Concerning the area of optical networks, we suppose that the reader has the prior knowledge needed. The chapters concerning the other two fields are structured and written in a way that should be easily understandable for any potential reader providing minimum knowledge needed.

2 Chapter
CONTEXT AND DEFINITIONS

2.1 Introduction

At the heart of an optical communication system is the optical fiber that acts as the transmission channel carrying a light beam loaded with information. The definition of light has been changing over the years and light can be defined as a name for a range of electromagnetic radiation that can be detected by the human eye.

The first interpretation of that electromagnetic radiation is that it has the nature as wave. Light wave, like any other wave, has amplitude, which is the brightness of the light, wavelength, which is the color of the light, and an angle at which it is vibrating, called polarization. This is the classical interpretation, crystallized in Maxwell's Equations, which held is way until Planck, Einstein and others came along with quantum theory.

Second interpretation, in terms of the modern quantum theory, electromagnetic radiation consists of particles called photons, which are packets ("quanta") of energy which move at the speed of light. In this particle view of light, the brightness of the light is the number of photons, the color of the light is the energy contained in each photon, and four numbers (X, Y, Z and T) are the polarization.

As a result light can be understood as an electromagnetic radiation and can have both wave-like and particle-like properties. In this thesis, we will primarily take the wave viewpoint as it is a more useful description of the everyday properties of light, but keep in mind that both viewpoints are valid, and sometimes we will use the quantum viewpoint too.

All electromagnetic waves propagate with the same speed in the vacuum, and this speed is denoted by c and is equal to 299,792.457 km/s. This value is usually approximated by 300,000 km/s. According to the theory of relativity, the highest velocity that any wave or object can have is the velocity of light in free space. Light waves travel at a slightly slower speed when propagating through a medium such as glass or water. The light beam gets guided through the optical fiber due to phenomenon of *total internal reflection*.

2.2 Architecture of optical network

The aim of this section is to present the architecture of optical network, with the emphasis on the outside plant portion of the fiber network. Among other parts, the outside plant portion includes fiber network that may be buried, pole-supported in an aerial configuration or placed on the seabed.

2.2.1 Fibers, cables, ducts …

Nowadays, optical fibers are slowly replacing the copper wires used as a transmission medium because of their properties, like high bandwidth and immunity to electromagnetic interference. Like copper wires, optical fibers are not usable for outside installation purpose if they are not protected properly. They have to be converted to cable form for use in the field. A fiber optic cable consists of one or more optical fibers protected by either a *loose tube* or by coating with the *buffer that fits tightly on the fiber*. All fiber optic cables include various plastic coatings to protect the fiber. Loose tube is one of the most widely used methods to protect optical fibers from environmental stresses and climatic changes.

In loose tube construction, the fiber is placed within the plastic tube of larger inner diameter than the fiber diameter. In this construction the fiber is placed loosely within the plastic tube, and the tube is usually filled with silicone gel to prevent moisture from seeping into the optical fiber. During manufacture it is ensured that the optical fiber to buffer tube length ratio is controlled such that no optical fiber is compressed against the tube wall when the tube expands or contracts with changes in temperature. This way the loose tube design protects the fiber from exterior mechanical forces acting on the cable while establishing a strain-free environment. This characteristic enhances the operating temperature range of the loose tube design.

The modular design of loose-tube cables typically holds up to 12 fibers per buffer tube with a maximum per cable fiber count of more than 200 fibers. That kind of design permits easy drop-off of groups of fibers at intermediate points, without interfering with other protected buffer tubes being routed to other locations. Loose-tube cables typically are used for outside-plant installation in aerial, duct and direct-buried.

If fiber cable is used in aerial installation, optical fiber cable must be able to withstand direct exposure to ultraviolet (UV) sunlight. Loose tube construction cable incorporates carbon black into its jacket material to provide maximum UV protection. On the contrary, tight buffered cables do not contain carbon black in their outer jacket and thus should not be used in aerial installations.

If fiber cable is buried, depending on the type of installation duct or directly buried, cable needs to be armored or not. Direct buried cables include an outer armor

layer for mechanical protection and to prevent damage from rodents. Armor is in that case surrounded by a polyethylene jacket. When using duct installation, unarmored cables can be used. The duct material is normally PVC (Polyvinyl chloride) or HDPE (high-density polyethylene).

Tight buffering is achieved during the cable manufacture using a direct extrusion of plastic over the basic fiber coating. This way the buffering material is in direct contact with the fiber which makes it easier to handle and connect. This is one of the reasons why they are primarily used inside buildings. This design is also suited for "jumper cables" which connect outside plant cables to terminal equipment, and also for linking various devices in access network. Standard tight buffered cables do not have filling compounds or water blocking protection, making them susceptible to damage caused by water penetration and migration. If water penetrates the cable jacket and buffer material, the individual tight buffered fibers will be subject to increased attenuation.

Cables used in fresh or salt water are especially complex designed to protect fibers from damage by fishing trawlers and boat anchors. They need to have elaborately designed structures and armors.

As previously mentioned optical cables are deployed (installed) in various environments; suspended through air (aerial), on the seabed (submarine cable) and most frequently, buried into the ground (terrestrial). Optical cables are designed to protect the optical fibers from damage due to the rigors of installation and from the demands of the surrounding environment however, no single optical cable design is universally superior in all applications. In general, optical fiber cables installed in outdoor environment are exposed to more severe mechanical and environmental conditions than are experienced in the protected, climate-controlled, indoor environment. Outdoor installations (usually lashed aerially, dulled through duct, or directly buried in the ground), are subjected to combinations of cable-gnawing rodents, ultraviolet radiation, standing water, temperature extremes and other outdoor-specific hazards like construction activities. Later on, we will present the greatest threats (enemies) of optical cables and at the same time the most common reasons for optical network failures.

2.2.2 Planning and installation of optical fiber systems-with emphasis on buried plant

When designing an optical network special attention should be paid to the plans for the location and installation of below-ground fiber optic cables. It should also take into the consideration future work operations that could be performed in that area of interest. Right-of-way is one of the most important cost factors in outside plant design for fiber optic cable systems. Cables are generally placed on the public rights-of-way

such as along highways, and the duct systems are under or adjacent to suburban streets or roads. But sometimes obtaining a right-of-way can be more complex and more difficult, for example if an optical cable should pass over agricultural land. Cables are often along railroad tracks, power transmission lines or using natural gas and petroleum pipelines. Planning phase is followed by a field survey to find out whether the planned route can in fact be installed. For example, if cable ducts or other entities already exists that can be used, or if other institutions pose a problem.

2.2.2.1 Depth of plant

Buried optical cables should meet the depth requirements indicated in Table 1 (source AFNOR NF P98-332). Equally, if a fiber cable is buried jointly with electrical cable there are additional requirements given by AFNOR NF P98-332. Once buried, it is recommended that optical cables are marked with above-ground markers and also with underground tape in order to identify the general location of the facility route.

2.2.2.2 Marking the facility route

The standard of placing the markers recommends that they are placed within line of sight of each other so the direction and location of the route is clearly indicated. Separation between markers should be 300 m (1000 ft) or less and they are identified by facility name, owner, etc.

Underground tape, as the name says is buried and is at least 300 mm above the cable. These warning tapes should have sufficient tensile strength and elongation properties so that when encountered in excavating, they are not easily broken and will stretch significantly before break. Further, we will see that although cables are visibly marked, sometimes they are not spared by the sudden cutting. There are procedures that are intended to ensure safe working operations and to minimize any possibility of damaging existing subsurface facilities. Procedures should cover among other things also the subject of advanced notification to facility owners before excavation starts and the question of the size of the tolerance zone. Despite all the necessary taken precautions, the greatest enemy of all buried cables stays construction activity with digs-ups.

2.2.3 Planning and installation of optical fiber systems-with emphasis on aerial cable

An aerial installation has its advantages and also disadvantages. For the installation aerial cable can use existing pole lines. Sometimes some of the existing poles are old and should be changed, but it’s probably faster to change few of them

than to make new network of poles. Using the existing poles, it is also easier to maintain the cables because they run along public roads. There are fewer problems with right-of-way in a case when they need to be repaired or changed. As the cables are suspended through air, cable is independent of soil conditions but on the other hand there is a possibility of excessive cable strain in special conditions such as wind or ice. It may seem that aerial cables are spared from cuttings due to construction activities but on the contrary, some of the biggest enemies are the trucks with their high trailers that can reach the cables and cut them by accident.

Table 1. Depth of plant, source AFNOR NF P98-332 [4]

Règles générales spécifiques à chaque réseau

Nature des réseaux	Textes de référence	Fouilles — Couverture minimum des câbles ou canalisations [2]			Distances en parallèle entre génératrices extérieures hors équipements et accessoires [1]	Distances en parallèle entre génératrices extérieures par rapport aux équipements et accessoires	Distances en croisement entre génératrices extérieures	Dispositifs avertisseurs [3]	
		Sous trottoir avec revêtement ou accotement	Sous trottoir sans revêtement ou accotement	Sous chaussée				Couleurs [15]	Distances minimales au-dessus des câbles ou canalisations
Télécom et vidéo en pleine terre transport, distribution, branchements et accessoires de jonction	— Arrêté interministériel du 02.04.91 — Arrêté interministériel du 17.05.01 applicable au 12.11.02 et annule le précédent — CCTP 1593 France Télécom	0,50 m admis au CCTP 1593	0,60 m	0,80 m	0,20 m (horizontal) 0,50 m si câble électrique BT ou HTA	(chambres, grilles de ventilation, ouvrages particuliers) 0,20 m (horizontal)	0,20 m	vert	0,30 m

2.2.4 Planning and installation of optical fiber systems-with emphasis on submarine cable

Long reach undersea fiber optic systems present a real challenge for a system designer. A submarine cable system should resist the sea bottom environment condition at the installation depth, and particularly hydrostatic pressure, temperature, abrasion, corrosion, and marine life. This implies that optical cables should be adequately protected (i.e., by armoring or burying) against aggression, for example due to trawlers or anchors. Due to the difficulty in accessing the submerged plant and the long and expensive link maintenance submarine cable system should have a long lifetime and a high reliability. In the case of a problem a specialized ship is required and the access may take many days. Furthermore, there are not much more than 40 fiber cable ships serving the entire world [1].

2.3 Overview of optical networks

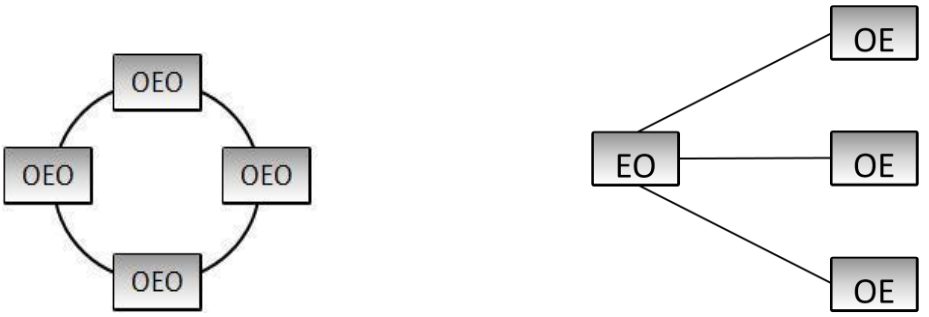
2.3.1 Point-to-point links

Optical fibers provide an unprecedented bandwidth potential that is far in excess of any other known transmission medium [2]. Apart from the fact that it has higher bandwidth than copper cable and is less susceptible to various kinds of electromagnetic interferences, optical fiber provides additional advantages such as low attenuation loss. Thanks to its potentials, fiber has been widely deployed to build high-speed optical networks using fiber links to interconnect geographically distributed network nodes. Optical fiber was primarily used to build and study point-to-point transmission systems (Figure 1). An optical point-to-point link provides an optical single hop connection between two nodes without any intermediate node in between. These optical point-to-point links may be viewed as the beginning of optical networks as they can be used to interconnect two different sites for data transmission and reception.

Figure 1. Optical point to point connection

At the transmitting side, the electrical data is converted into an optical signal (EO conversion) and sent on the optical fiber. At the receiving side, the arriving optical signal is converted back into the electrical domain (OE conversion) for electronic processing and storage. Soon with the growing demand for bandwidth, point-to-point links were used to interconnect more than two network nodes. Solution was

introduced using various network topologies, like ring and tree networks, with multiple optical single-hop point-to-point links (Figure 2).



a) Ring topology b) Tree topology

Figure 2. Optical a) ring and b) tree configurations

2.3.2 Network topologies

The optical ring networks can be realized by interconnecting each pair of adjacent ring nodes, where each node performs OE conversion for incoming signals and EO conversion for outgoing signals. The combined OE and EO conversion is usually referred to as OEO conversion. Ring topologies are mostly deployed in metro networks where they are used to collect/distribute the traffic over a given area and pass it on/from to the core networks.

In tree topology optical signal is forwarded to all output ports. Optical single hop tree networks make use of EO conversion at the transmitting side and OE conversion at the receiving side, similar to optical point-to-point links. Tree topologies are used for access networks connecting end users to the network operator.

Core networks (long haul networks), in contrast to metro and access networks interconnect major cities, peering points, gateways to internet and data centers. Topology used in core networks is mesh network, where each node not only catch and disseminate its own data, but also serve as a relay for other nodes (Figure 3).

Access networks in general do not use any recovery method. Using protection and restoration method would mean setting new fiber infrastructure in parallel to the existing one and that would be expensive solution for an ordinary client. Metropolitan networks are insured to have recovery method thanks to the ring topology but also using protection and/or restoration methods. As they are carrying higher amounts of traffic than access network, demands concerning the availability of the networks are also higher. If we take into consideration the amount of traffic that is being transported by core networks, recovery methods need to provide the highest level of availability.

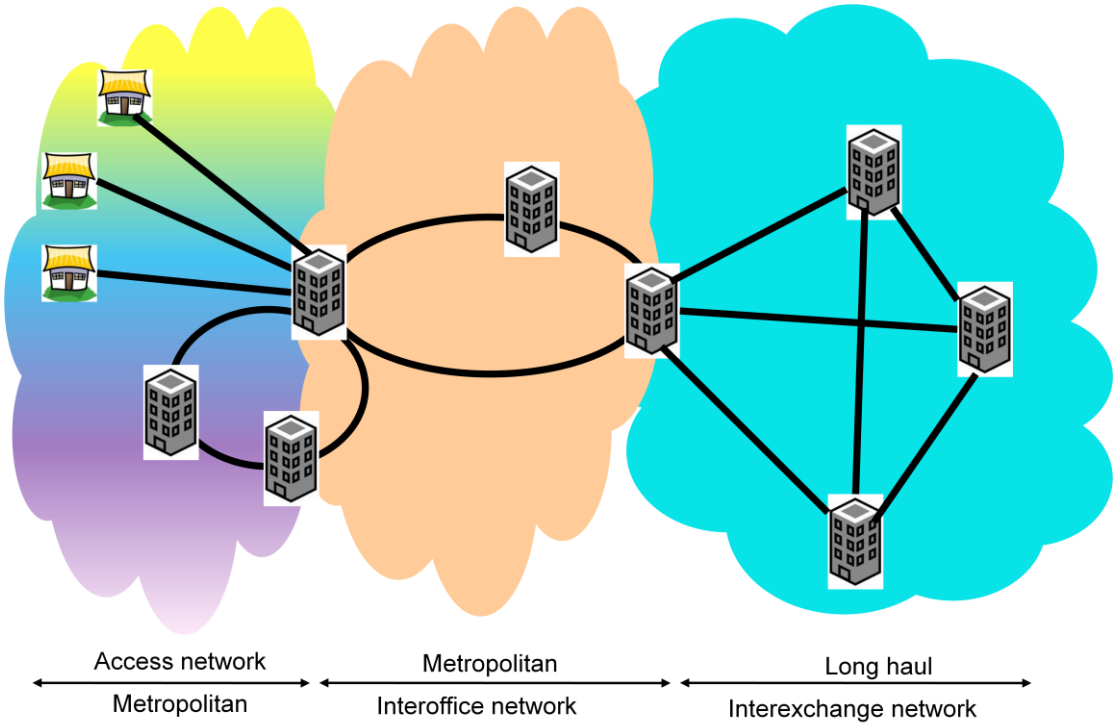


Figure 3. Access, metropolitan and core network

The objective of this work is the proactive link recovery method in the core networks when the highest availability is needed. As the access network does not deploy recovery method and there are no backup resources in the case of link failure (just one link going to the client), proactive link recovery can not improve the availability of access networks.

2.3.3 Standardization

With the appearance of the first point-to-point links, network operator was faced with equipment that works differently depending on the manufacturer. First standardization process for optical point-to-point links has begun during 1985 and it's called Synchronous Optical Network (SONET) standard in the United States and Canada and Synchronous Digital Hierarchy (SDH) in the rest of the world. SONET and SDH are nearly identical, though there are significant enough differences that equipment vendors must explicitly indicate whether they support SONET, SDH, or both on a port card. The goals of the SONET/SDH standard were to specify optical point-to-point transmission signal interfaces that allow interconnection of fiber optics transmission systems of different carriers and manufacturers and among others to provide new network features. SONET/SDH is deployed by a large number of major network operators. Typically, SONET/SDH is based on a digital TDM (time division multiplexing) signal hierarchy where a periodically recurring time frame of 125 µs

can carry payload traffic of various rates. In ring configurations SONET/SDH is used to form optical ring networks with OEO conversion at each node.

Great attention was given to the systematic optical and electrical conversions in optical networks. A new effective concept arised, the concept of optical bypassing, that enabled designers to let in transit traffic remain in the optical domain without undergoing optical-electrical-optical conversion at intermediate network nodes. As a result, intermediate nodes can be optically bypassed and costly optical-electrical-optical conversions can be avoided, which typically represent one of the largest expenditures in optical fiber networks in terms of power consumption, footprint, port count, and processing overhead [3]. More important, optical bypassing gave rise to the so-called "transparent" networks in which optical signals stay in the optical domain all the way from source node to destination node. This topic will be further explored in one of the following sections.

2.3.4 Amplification

Like in the electrical communication in optical communication signals fade over the distance. The distances are much greater on optical networks but the problem still exists. This is because of the transmission characteristic of the fiber that is called fiber attenuation or loss. The optical power attenuation constant (in dB/km) of a fiber is typically plotted as a function of the wavelength (Figure 4).

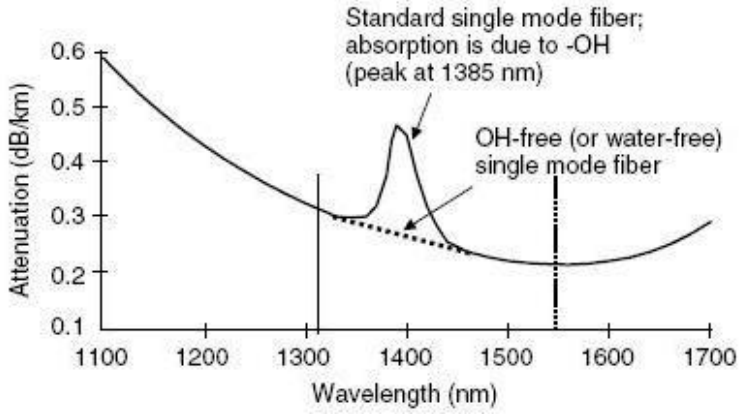


Figure 4. Single-mode fiber attenuation as a function of wavelength; source [4]

Conventional single-mode fibers have two low attenuation ranges, one about 1.3 μm and another about 1.55 μm, as shown on the Figure 4. Between these two ranges, and about 1.4 μm, there is a high attenuation range due to the OH radical with a peak at 1385 nm. This high attenuation range is also known as the “fifth window”. Fiber cables that are almost free of OH radicals have been successfully manufactured and on the Figure 4 its characteristics is represented with the dotted line (OH-free single mode fiber). That means that if the OH radical could be eliminated from the fiber

material, then the high attenuation unused region, about 1.4 μm, could be utilized. Conventional single-mode fibers transmit wavelengths in the 1300 and 1550 nm range and absorb wavelengths in the range 1340 to 1440 nm range.

As mentioned, fiber attenuation is measured in dB per kilometer and International Telecommunication Union ITU-T G.652 recommends losses below 0.5 dB/km in the region 1310 nm, and below 0.4 dB/km in the region 1500 nm. Some typical values are 0.4 dB/km at about 1310 nm, and 0.2 dB/km at about 1550 nm.

To address the problem of fiber loss, three types of devices are used, amplifiers, repeaters and regenerators. Optical amplifiers are "transparent" devices that increase the intensity of a signal detected, noise and all. They enlarge and strengthen signals without distorting the original signal but unfortunately they are also nondiscriminatory which mean that they will amplify noise and distortion as well as the desired signal (Figure 5) and each of them also add noise due to amplified spontaneous emission. Optical amplifiers typically do the first level of regeneration (1R). Regenerators generally use electronics and are more sophisticated. They detect the optical signal, convert it into an electronic signal, clean it up and retransmit it as an optical signal again (3R). Repeaters fall somewhere between "transparent" amplifiers and regenerators. They are also electro-optical devices, but typically provide only amplification and reshaping and not full regeneration of a signal (2R). Since the introduction of optical amplifiers repeaters are rarely used.

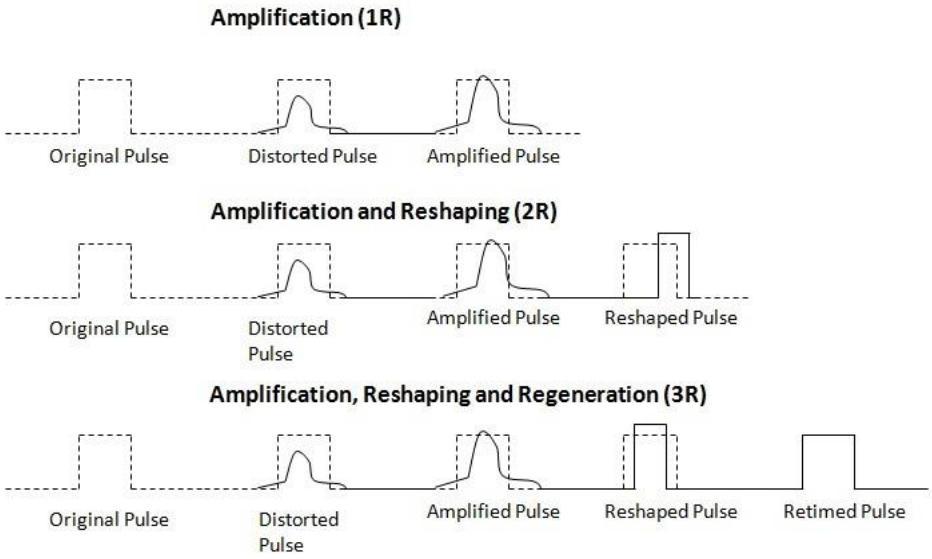


Figure 5. Amplification, Reshaping and Regeneration

There are three places in the network where amplifiers can be located: after transmission (postamplification or booster), during transmission (in-line amplification), and prior to reception (preamplification). Postamplifiers are placed directly after a transmitter to increase the strength of a signal before transmission. In-

line amplifiers are set every 80 to 100 km along an optical fiber link, to make up for signal attenuation while preamplifiers are placed just before a receiver. They magnify the signal to a power level within the receiver's sensitivity range. (Figure 6).

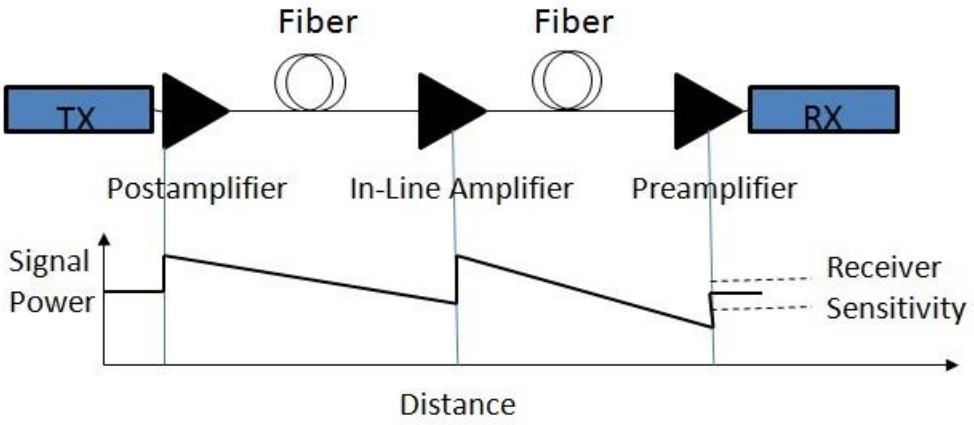


Figure 6. Amplifiers

2.3.5 Multiplexing

There is a continuous demand for bandwidth since the construction of the Internet. As it is relatively expensive for operators to lay new fibers and furthermore to maintain them; the solution was to explore the existing fiber bandwidth. Three main multiplexing approaches have been deployed to increase the transmission capacity on the fiber:

1. Time division multiplexing (TDM)
2. Wavelength division multiplexing (WDM)
3. Orthogonal frequency-division multiplexing (OFDM)

In this paper we will put emphasis on the WDM and TDM approach, as they are the approach widely used in core transmission systems and we will show some advantages and drawbacks of the TDM approach. We just mention the existence of the OFDM, since this method is out of our scope.

2.3.5.1 Time division multiplexing (TDM)

Time division multiplexing is achieved through multiplexing many lower speed data streams into a higher speed stream at a higher bit rate by means of non-overlapping time slots.

We have mentioned earlier that SONET/SDH is an example for optical networks that deploy TDM. The main drawback of TDM is the so called "electro-optical"

bottleneck. In the context of high-speed optical networks, the optical TDM signal carries the aggregate traffic of multiple different clients and each TDM network node must be able to operate at the aggregate line rate. The aggregate line rate is limited by the fastest available electronic transmitting, receiving, and processing technology. The aggregate line speed was also limited by fiber dispersion but with the arrival of the new multilevel modulation format and coherent receiver that limit has been pushed.

2.3.5.2 Wavelength division multiplexing (WDM)

In optical WDM networks each transmitter sends on a separate wavelength. At the transmitting side of the terminal site, a wavelength multiplexer collects all wavelengths and feeds them into a common outgoing fiber. And at the receiving side of the terminal site, a wavelength demultiplexer separates the wavelengths and forwards each wavelength to a different receiver. Hence, WDM system consists of terminal sites, amplifier sites, placed along the link and of course spans of optical fiber (Figure 7).

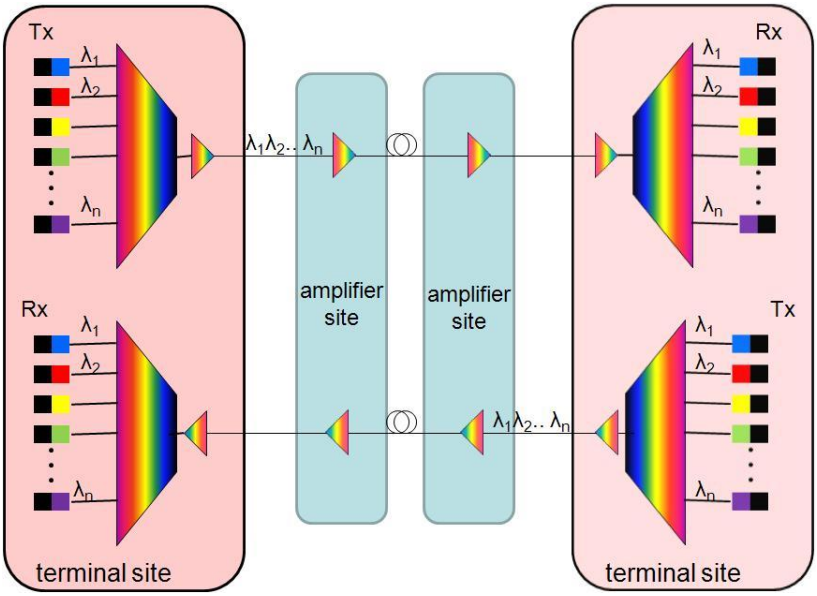


Figure 7. Principle of WDM

The major role of the terminal sites is to host transponders. The transponder is the element that converts a signal from the client side which can be electrical or optical into the signal line WDM which is optical. That way we obtain "colored" signal from color-less (also called grey or Black & White signal for signal carried on non WDM). In the Figure 7, we represent black part of the signal (client side) that may correspond to SDH/SONET, or Ethernet and WDM line side with different colors corresponding to different wavelengths.

The wavelengths generated by the transponder conform to standards set by the International Telecommunications Union (ITU): typically in the 1.55 μm wavelength window for the transmission side, while the incoming signal may be a 1.3 μm signal (Figure 8).

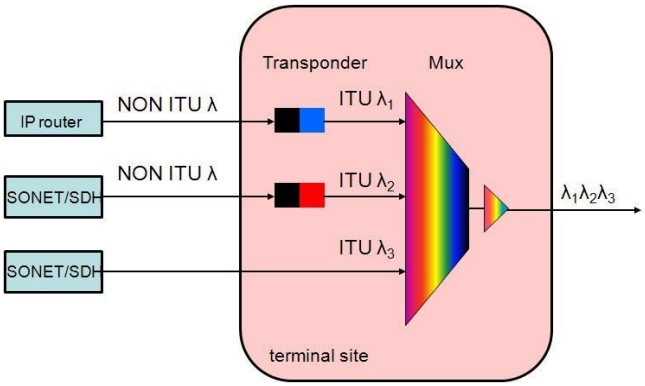


Figure 8. Optical line terminal

The transponder is not only converting signal to the appropriate wavelength but it also adapts incoming signals to the required specifications (optical such as power, modulation type, and also framing and coding. In the Figure 8 (for the reasons of simplicity), is presented just the transmission side of the terminal site.

In some situations, like shown on the bottom of Figure 8, transponders are directly integrated in the client equipment site (for example router interface) by having the adaptation function performed directly inside the client's equipment that is using optical network. Today, WDM interface specification on the line side is proprietary to each WDM vendor, and there are no standards.

When it comes to equipment, service providers prefer to deploy equipment for multiple vendors that operate together in a single network. Some of the reasons for that is to reduce the dependence on any single vendor and to drive down the costs. However in the case of WDM, achieving interoperability at the optical level is particularly difficult. That would mean standardization of set of parameters like optical wavelength, optical power, signal to noise ratio, bit rate, etc. Practical solution toward the interoperability is to use transponders to interconnect disparate all-optical sub-networks.

WDM systems are divided by the different wavelength patterns they are using into conventional/coarse (CWDM) and dense (DWDM). Dense wavelength division multiplexing (DWDM) enables high density of wavelengths in the same fiber and uses the same transmission window C-band (conventional band from 1530 nm to 1565 nm) as the conventional (CWDM) but with denser channel spacing. The CWDM scheme utilizes wavelength channels spaced 20 nm apart. Due to large channel

spacing, the wavelength of a transmitter needs not to be very precise. Such a system was developed for metropolitan applications in which cost is a very important factor.

2.3.6 All-optical networks

Optical WDM networks do not necessarily have to be transparent (all-optical). In this thesis we refer to optical WDM networks as the networks that deploy optical WDM links where each fiber link carries multiple wavelength channels. To build optical networks that are transparent, the optical signal must be able to remain in the optical domain until it arrives at the destination. This can be achieved by avoiding OEO conversions at intermediate nodes. Such nodes are also called OOO nodes to emphasize the fact that they do not perform OEO conversion. This way, data stay in the optical domain and is optically switched all the way from the source to the destination node.

As opposite to transparent networks, optical WDM networks can be opaque. In opaque networks, due to the fact that OEO conversion takes place at intermediate nodes, the most of the management information can be obtained from the electrical domain at every step of the signal propagation. This information is very useful when it comes to managing and controlling the network.

The two most common optical networking devices are Optical Add/Drop Multiplexer (OADM) and Optical Cross-connect (OXC). In this work we will introduce OADM and OXC separately for illustration purposes.

2.3.7 Optical Add/Drop Multiplexer (OADM)

The main functionality of OADM is to access, drop, add, or pass-through wavelengths channels in a WDM enabled optical network. Figure 9 shows the functional structure of an OADM. There are four input and output fibers in the figure, each of which supports N wavelengths. An incoming optical signal may be pre-amplified by means of an optical amplifier. After optical pre-amplification (usually done with so-called Erbium doped fiber amplifier) the WDM wavelength signal is partitioned into its N separate wavelengths by using 1xN wavelength de-multiplexer (Demux for short). The demuxed signal can propagate directly through the local node (optically bypass it) without changing wavelength, like shown on the top of the Figure 9. Or it can be dropped and detected by means of OE conversion, thus releasing wavelengths for further insertion of local traffic. Likewise, a wavelength can be added through an add port and directed to a wavelength port by configuring corresponding filters. Dropped wavelengths and added wavelengths can operate at the same optical frequency but carry different traffic. Then, all N wavelengths are combined onto a common outgoing fiber by using an Nx1 wavelength multiplexer (Mux). The

composite optical WDM signal may be amplified by using another optical amplifier at the output fiber (e.g. EDFA). Add/drop ports represent the WDM network entry and exit points. To handle certain client signal formats, the corresponding interface cards are employed at the add/drop ports, which are also known as the client interfaces.

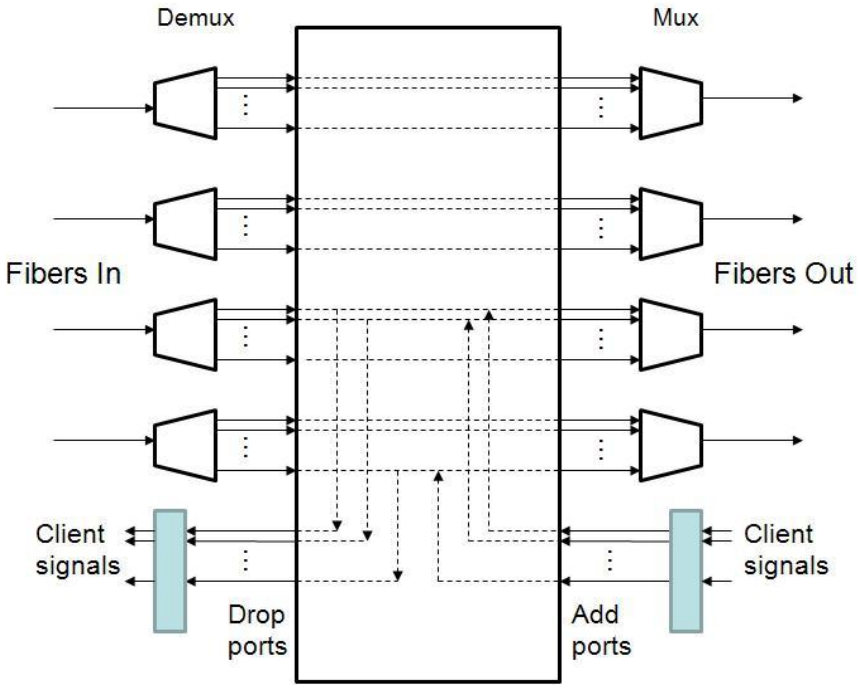


Figure 9. Functional diagram of an Optical Add-Drop Multiplexer (OADM)

2.3.8 Optical Cross-connect (OXC)

Compared to an OADM an OXC has the possibility to rearrange wavelengths from fiber to fiber within a WDM network. Figure 10 shows a possible structure of an OXC. In the figure, there are four input and output fibers, each of which has N number of wavelengths. We choose four input and output fibers in representation of OADM and OXC for easier illustrations of their similar and different functionalities. Like in OADM, incoming optical signal may be pre-amplified by means of an optical amplifier. After the pre-amplification, signals reach ports through demux. Depending on the switch setting, wavelengths from one fiber can be connected to the same wavelength but on different outgoing fibers. Also it is possible that a signal carried by a wavelength from one fiber can be converted to another wavelength before being directed to a fiber. This possibility is especially interesting to solve wavelength contention when more than one signal compete for the same wavelength channel on one outgoing fiber.

In addition to above mentioned wavelength switching, OXC can also support waveband switching and fiber switching. Waveband switching connects a subset of

wavelengths from an incoming fiber to an outgoing fiber while fiber switching switches an entire fiber including all the wavelength channels to an outgoing fiber.

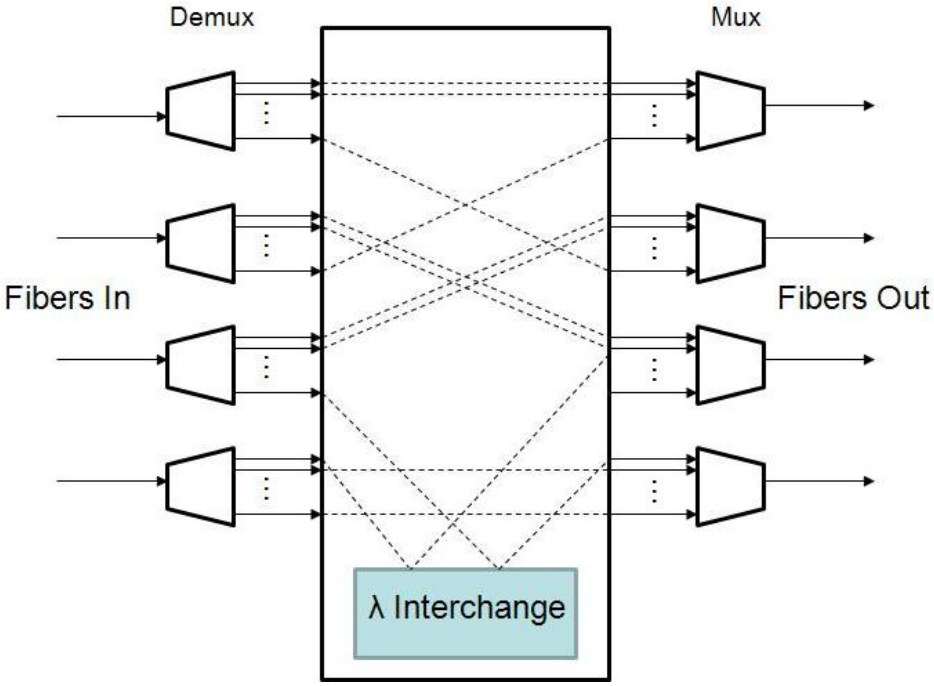


Figure 10. Functional diagram of an Optical Cross-Connect (OXC)

OADMs are useful network elements to handle simple network topologies, such as linear topologies or ring topologies while OXCs are key components of meshed networks with large number of wavelengths. Though the term optical is used, an OXC could internally use either a pure optical or an electrical switch fabric. (Note that one can also find the term multi-degree ROADM or photonic cross-connect in the literature to designate OXC).

An "all optical" network that deploys above-mentioned, OXCs and OADMs is commonly referred to as an optical transport network (OTN).

2.3.9 Wavelength management

The optical path between the source and destination in "all-optical" networks remains entirely optical from end to end. Paths with that property are termed lightpaths. A lightpath may keep its assigned wavelength unchanged and in that case it is said that the setup of lightpaths has to satisfy the *wavelength continuity constraint*. Or, alternatively it may have its wavelength altered along the path using the wavelength conversion present in OXC. If each lightpath has to stay at its assigned

wavelength, it becomes a constraint that makes it generally more difficult to accommodate lightpaths, leading to increased blocking probability.

Wavelength converters can be realized in two ways. The first way is using OEO conversion of the incoming optical signal and retransmission on the target wavelength. The second way is carried out in the all optical domain. The latter method is still under research: there are not yet available products, although there has been many prototypes proposed in the past.

Reconfigurability is an important property of the network that enables the rerouting and load balancing of traffic in response to the network failures and traffic load changes, respectively. Enabling the reconfiguration of the optical network is thus an interesting feature. This can be done by using reconfigurable OADM and OXC, tunable emitters and tunable wavelength converters should the case arise. Reconfigurable optical add-drop multiplexer (ROADM) can be built using for instance broadcast and select (B&S) or select and combine (S&C) architectures and for example based on WSS (Wavelength Selective Switch) technologies.

The functional operation of the ROADM is described below. In broadcast and select (B&S) ROADMs the incoming optical signal is broadcast through a passive optical coupler, that divides the incoming optical signal into drop and several pass-through directions (as many as output fibers directions). On each passthrough path, a reconfigurable wavelength blocker selects the individual wavelengths that can pass on the given direction and block the one that must be stopped (for example dropped), or switched to other direction. Selected wavelengths incoming from the ingress fibers are the combined to the local added wavelengths carrying added traffic and combined on the egress fiber.

A WSS has the possibility to combine the blocker and combiner function in a single device. The current WSS based architectures do not support strictly non blocking functionality today.

Although reconfigurable all-optical networks can be used to realize powerful telecommunication network infrastructures, possibility of reconfiguration also give rise to some new problems. For example, if the network elements are reconfigurable, what would be the optimal configuration at the given moment and also considering traffic load changes, network failures, etc.

2.3.10 Architectural choices for transport networks

The optical layer is the main transmission layer for backbone networks. And it is playing an increasing role in these networks. One of the reasons is the economics based on the savings in EOE thanks to optical by pass enabled by high transmission performances and ROADM. With the continuous worldwide deployment in optical

fiber and the maturity of transmission systems and ROADM, the optical layer is no longer just point-to-point pipes providing physical link services, but a network with new levels of flexibility requirements (resilience, on demand capacity, etc.).

These requirements are also dependent on the transported services. There is a set of technologies to be used above the optical layer to deliver services. The examples of client layers residing above optical network layer include SONET/SDH (for transport), ATM (Asynchronous Transfer Mode) (for traffic engineering), IP (for carrying applications)/MPLS (Multiprotocol Label Switching), and Ethernet (for data packet adaptation over the physical link). The use of the different technologies depends on the purpose and the cost trade-off. Figure 11 shows three possible approaches for IP over WDM.

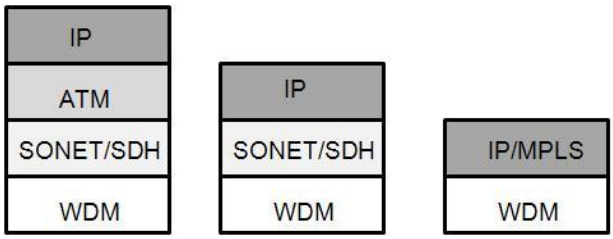


Figure 11. Three approaches for IP over WDM

The legacy transport network in place in networks run by established carriers is based on SONET and SDH. SONET/SDH provides end-to-end, managed, circuit-switched connections. It also provides efficient mechanisms for multiplexing lower-speed connections into higher-speed connections while ATM provides the possibility to carry different types of traffic onto the same pipe with different QoS (Quality of Service) requirements. Multilayer architectures, presented like the first solution in the Figure 11, typically suffer from the lowest common denominator effect where any one layer can limit the scalability of the other layers and the entire network. Further motivation was going into direction of designing two layer networks: IP over WDM.

The main motivation behind IP over WDM comes from the fact that most of the data traffic across networks is IP and nearly all the end-user data application use IP [5]. Even the conventional voice traffic can be packetized with voice-over-IP techniques. Also the use of WDM technology can significantly increase the use of the fiber bandwidth and address the continuous growth of the Internet traffic.

2.4 Transport network failures and their impact

This part of chapter is devoted to the most frequent causes of network failures. This small survey of the basic problems that the network is facing in the field will show the most frequent reasons for its outage and also how with the time, even with

all the invested human best-efforts to change and to protect it, construction activities and excavations stay the network enemy number one.

Networks failures are in the scope of our interest because they provoke, sometimes very small in order of milliseconds up to several hours/days outages of the network services. From the point of view of the telecom operator these services present a fairly significant annual income. This income can be reduced by the effects of the outage duration that might be very expensive depending on the proposed services. In order to give a better picture of the relevance of the duration of the outage we will present the average hourly impact of the outage of the different type of services.

2.4.1 Causes of failure

In this work, we use the term outage/downtime whenever there is a network service interruption. These outages can be planned in advance (so called planned outages) providing the exact and the complete information including the date, time and duration of the outage or like most of the time unpredicted (unplanned).

Planned outages are known in advance and are often scheduled during the maintenance window that gives the possibility to a telecom operator/network owner for performing certain tasks, including the following:

- upgrading/patching of the system with the newest technology,
- maintaining of the equipment,
- changing used parts/cables of the equipment,
- repairing hardware/software,
- fixing errors, etc.

Downtime of the planned outages has to be carefully scheduled, and that way can be maximally reduced, unlike the downtime of the unplanned outages that cannot be predicted in advance and that way leaving the impossibility for its reduction.

Unplanned outages, on the other hand can be also divided to the ones provoked by the nature, for example the earthquakes, tsunami, flooding, etc. meaning that their prediction would not be able to decrease the potential damage on the reduction of the downtime of the network and the ones which are the result of the human activities, animals, etc.

Planned outages and unplanned outages provoked by the nature are not in the scope of our interest and that’s why we are not going to go into the details explaining them. However, the recovery process for the planned outages will give us some of the

ideas and directions how to react in the case of unplanned outages. It will be more clearly explained in further chapters.

2.4.2 Unplanned outages

Unplanned outages in general concern equipment hardware failures, software failures, power supply failures and also failures produced by some internal or external source. This area is very wide and we could dedicate the whole chapter exploring the all possible reasons for the unplanned outages but we will concentrate on the most frequent reasons for the link failures. These link failures are having as a consequence outage of the network (which implies also the outage of the network services).

We mentioned above how it is important that fiber optic cables are buried suitably deep, put in the conduits and physically protected. These are necessary conditions, necessary but not sufficient conditions to guarantee 100 % protection from external impacts. Despite best-efforts at physical protection, it is statistically certain that a fairly high rate of cable cuts is inevitable.

Authors in [6] estimate that any given mile (1.61 km) of cable will operate about 228 years before it is damaged (4.39 cuts/year/1000 sheath-miles). This number sounds reassuring but on 100 000 installed route miles it implies more than one cut per day on average. Also when including the potential human activities which occur during the working week number of failures tend to cluster, producing some single days over the course of a year in which perhaps two or three cuts may occur. In 2002 the FCC (Federal Communications Commission) published findings that metro networks annually experience 13 cuts for every 1000 miles of fiber, and long haul networks experience 3 cuts for every 1000 miles of fiber [7]. These frequencies of cable cut events are hundreds time higher than corresponding reports of node failures, which helps to explain why we are focusing on the recovery from link failures arising from cable cuts. Equally, during 1992, fiber cable failures were the single largest cause of the network outages affecting more than 50 000 customers for more than 30 minutes and accounted for roughly as many outages as tandem and local switch equipment failures combined [8].

2.4.2.1 Dig-ups

Some previous research shows that almost 60 % of all cuts were caused by cable dig-ups. We define a dig-up as the damage to a fiber optic cable during an activity to penetrate the ground. Excavators usually involved in significant numbers of cable dig-ups include: water, electric and gas company contractors, and highway department contractors. In the case of the construction work or digging activities, the contractor/excavator is obliged to notify the facility owner before digging in order to

locate and establish the presence of a cable infrastructure which could be potentially damaged. Despite the notification, a large number of reports show that cables were difficult to locate because their locations were not accurately identified. One of the reasons for that kind of problem could be that the above ground infrastructure is changing fast with time and cable infrastructure maps are not updated.

Beside the problem of the so called inaccurate location when locating the real position of the cable infrastructure, another problem that occurs is called incorrect notification. In these cases, the contractor/excavator provides prior notification but does not accurately describe the location of the digging work to be performed. Therefore, the actual cable which is near the proposed excavation will never be located.

Another root cause for the fiber cuts is due to shallow cable burial depth quotes [8]. In these cases, the route was properly located and marked and excavation was conducted with hand tools but the cable was buried to a smaller depth than indicated. The first section presented examples of the industry standards recommended for the depth of the buried cables. We will just comment here on the recommendation for the use of permanent above ground markers and/or underground warning tape to identify the general location of a sub-surface cable. These permanent above ground marking is considered effective in reminding excavators to provide proper notification prior to digging. Even though some older researches show that there is virtually no difference in the reported dig-ups per sheath mile between marked and unmarked routes.

Beside dig-ups there is a wide variety of external events reported to have caused fiber and other cables to fail.

Figure 12 lists the immediate causes of fiber optic cables cuts reported to the France Telecom during the year 2009.

This statistic was done for the aerial and underground cable on the territory of France without taking into consideration the submarine cables. For the submarine cables we mention later what are the biggest menaces in general and how to prevent them from happening.

Historically, dig-ups have consistently been responsible for 55 % to 60 % of failures reported to France Telecom. This finding is consistent with results of Bellcore's Field Tracking Study which indicates that over 93 % of cable failures reported between 1990 and 1992 resulted from a broken fiber or cable of which 60 % have the mutual cause: dig-ups.

Cause	# of reports	% of total
Dig-ups	236	58.4
Vehicle	31	7.7
Process error	11	2.7
Power line	8	2
Rodent	22	5.4
Sabotage	48	11.9
Flood	32	7.9
Fallen trees	16	4

Figure 12. Failure causes

2.4.2.2 Vehicle damage

Vehicle damage is the type of the cable damage that results from vehicle collisions with utility poles which support aerial cable. There are few reports concerning high vehicles that caught a sagging aerial cable and few of them that involve a vehicle colliding with a highway overpass which housed fiber optic cable. One of the precautions that could be made if driving a high vehicle or vehicle with the high trailer is to measure before each journey the high, in both laden and empty situations.

2.4.2.3 Process error

We define process error damage as the failures caused by the telecommunication company personnel performing maintenance or installation work. In general, it's the human mistake (human factor), coming from the personal working for the company. For example, when an in-service fiber optic cable was accidently severed during removal of an obsolete cable or during the repair of a nearby damaged cable.

2.4.2.4 Power lines

Damage caused by power lines occurs when an electric power cable makes contact with an aerial fiber optic cable or its metallic messenger strand. The resulting heat dissipation melts the fiber cable. Fortunately, these reports were rare in France Telecom infrastructure.

2.4.2.5 Rodents

Rodents, like mice, rats, gophers and beavers seem to be fond of the taste and texture of the cable jackets and gnaw on them in both aerial and underground installations. Damage caused by rodents affects not only the aerial and underground installations but also intra-building fiber cables. Frequently, these damages result in only a partial failure of a cable. Some previous research [8] shows that only one of the six rodent induced failures reported severed every fiber in the cable. On the other hand by partial gnawing at cable sheaths, rodents also compromise a number of cables which then ultimately fail at a later time. Measures against rodents include climbing shields on poles and cable sheath materials designed to repel rodents from chewing.

2.4.2.6 Vandalism

Failures caused by sabotage are deliberate human activities whose sole purpose is to damage cables. This group includes also the acts of vandalism when facility huts or enclosures are broken into. Statistics made for 2009 year for France Telecom cable infrastructure show a quite high number of such cases (Figure 12). A problem observed in some developing countries is that aerial fiber optic cables are often mistaken for copper cables and pulled down by those who steal copper cable for salvage or resale value.

2.4.2.7 Floods

Floods cause damage when large quantities of water sever a fiber optic cable. For the places where there is the highest risk of flooding it is envisaged to use cables that are made with protection against moisture and water. For example, in the cable construction where the fiber is placed loosely within the plastic tube and the tube is filled with silicone gel, moisture is prevented from steeping into the optical fiber. On the contrary - the cable construction with tight buffering does not have water blocking protection, making them susceptible to damages caused by water penetration and migration. This kind of fiber cuts falls into the category of unplanned failures provoked by the nature.

2.4.2.8 Fallen trees

Fallen trees are not so rare in reports as the cause of the aerial fiber cuts. These failures occur when an aerial cable is severed by a falling tree limb, usually during the logging (cutting) trees. Sometimes falling tree limbs and sagging branches occasionally lead to failures caused by power line contact, like mentioned above.

2.4.2.9 Other causes

There is also another category which we will call ‘other causes’, where we place all the other cable cuts that was impossible to determine the cause for its destruction with certainty. For example, the excavator company guilty for the fiber cut that runs away from the crime scene without leaving any trace.

The greatest hazard for undersea cables is from ship anchors and fishnets dragging on the continental shelf portions. Extremely heavily armored steel outer layers have been developed for the use on the exposed sections as well as methods for the undersea trenching into the sea floor until undersea cable leaves the continental shelf. Beyond the continental shelf cables are far less heavily armored and they lay on the sea floor directly. In contrast to the continental sections of the undersea cables, the main physical hazard for deep sea cables appears to be the shark bite. Several transoceanic cables have been damaged by sharks which seems to be attracted to the magnetic fields surrounding the cable from power-feeding currents.

Now we are familiar with the most frequent causes that in general bring down the optical network provoking the outages. Next part of the work presents the effects of outage duration.

2.4.3 Effects of the outage duration

There are a variety of user impacts from optic cable failures. As mentioned in the introduction, one of the most important impacts for the telecom operator is the revenue loss and business disruption. For example, direct voice-calling revenue loss from failure of major trunk groups is quoted at $ 100,000/minute or more [9]. Also revenue losses can arise from default on service level agreement (SLA) for private lines or virtual network services. More recently many businesses became completely dependent on web-based transaction systems. For example, direct revenue loss and impact on the reputation of so called “dot-com” businesses if there is any outage of more than a few minutes. In Figure 13 are presented the average hourly impacts for different type of services, for example: Airline reservations, home shopping, pay per view services, etc. Source from which we obtained this data is Contingency Planning Research.

Business/Industry	Average hourly impact
Airline reservations	$89,500
ATM service fees	$14,500
Brokerage operations	$6,450,000
Catalog sales	$90,000
Cellular service activation	$41,000
Credit card authorization	$2,600,000
Home shopping	$113,750
Online network fees	$25,250
Package shipping services	$28,250
Pay per view services	$150,250

Figure 13. Cost of an Outage (Source: Contingency Planning Research, Inc)

2.4.4 Outage time impacts

Beside the effects on the revenue loss, outage time can have impacts on the harmful complications from a number of network dynamic effects that have to be considered. A study done by Sosnosky [9] provides summary of effects, based on a detailed technical analysis of various services and signal types.

In this study outages are classified by its duration and it is presented how with the given different outage time, main effects/characteristics change. For example, an interruption of 50 ms or less in a transmission signal causes a "hit" that is perceived by higher layers as a transmission error. The 50 ms figure originates from the specifications for dedicated 1+1 Automatic Protection Switching (APS) systems. So in the case of the outage less than 50 ms Transmission Control Protocol (TCP) recovers after one errored frame and the most of the TCP sessions see no impact at all.

If the outage time increases (moves up from 50 ms) then the chance that a given TCP session losses a packet increases. The effect is a "click" on voice, a steak on a fax machine and possibly several lost frames in video. It may also cause a packet retransmission within data services.

Outage duration between 150-200 ms results with disconnections of any calls in progress.

Outage duration between 2-10 s results with disconnection of all private lines, potential data sessions, X.25 and all switched circuit services. With that outage duration TCP session time–out starts, while web pages are no more available and hello protocol between routers begins to be affected.

This overview is given so that the potential reader could sense how such a small time values (order milliseconds) can make a great impact in the world of services. Once familiar with the reasons for network failures, how expensive consequences they could cause (not only to telecom operator but also to ordinary users/clients in

everyday life) and how much impact could have on the network services, reader will discover the existing recovery methods that are made to deal with these failures.

2.5 Network survivability

In the last few years with the emergence of new broadband services over the Internet like video data transfer, peer to peer and also boosted by optical access deployment, there has been a huge increase of the bandwidth in WDM systems deployed in optical core networks. With optical links capacity up to 1.6 Tbit/s [10], survivability becomes an important issue in the design of the WDM optical networks. Indeed a large amount of traffic and services can be impacted in a case of failure. A single outage can disrupt millions of users and result in millions of dollars of lost revenue to users and operators of the network [11].

That's why when designing a network, operators also develop a survivability concept. The survivability strategies must be able to cope with current and future network size. This point is important because the projected growths in optical networks are tremendous.

A great variety of survivability approaches are used in today's networks, and the terms working path and backup path are fundamental to understanding them. Working path (resource) is used for carrying traffic in normal circumstances while backup paths (resource) provide an alternate path for the traffic in case of a failure. In general, working and backup path are usually diversely routed so that both paths are not lost in case of a single failure.

2.5.1 Protection and restoration - basic concepts

The two main approaches that address the failures are protection and restoration [12]. By applying these approaches and designing in the most cost-effective way the network with enough redundant capacity, an optical network can be deployed with appropriate survivability to fulfill the requirements of all applications. In this context one of the most important questions is how the recovery methods will operate in response to a network failure and how long the service(s) will be down due to that failure.

The protection mechanism activates in advance backup resources that will be used in case a failure, while the restoration mechanism takes over backup resource upon a failure; that is why protection mechanisms can recover quickly but are more demanding in terms of resource. Restoration mechanisms are less demanding when it comes to resource and therefore may be less costly than protection mechanisms in term of initial investments, but they generate longer service disruption. Protection and restoration mechanisms are triggered after the failure is detected [13].

The approaches are designed to succeed under likely physical failure scenarios. In most cases, the recovery methods are engineered to protect against a single failure event or maintenance action. Typically it is assumed that the most likely failures are single failures rather than double failures. Multiple failures may also be considered but the probability of having multiple failures can be very small if the network has a proper design. For example a fiber cut can lead to multiple link failures at the client layer if fibers carry multiple wavelengths. Also links that fail together due to dig-ups are referred to as shared risk link groups (SRLGs). But with the proper design of the network, in this case if the backup path is physically separated from the working path, the recovery of the network is possible.

Depending on different authors, terms protection and restoration may be interpreted differently. Some people apply the term protection when the traffic is restored in the tens to hundreds of milliseconds, and use the term restoration when the traffic is restored on a slower time scale. Some of them do not distinguish between protection and restoration [11]. In this work we will use the term protection when the backup resources are planned and reserved at the moment of the set up of the working path and when the trigger for the traffic switching on backup routes is when a failure occurs, while we use the term restoration to define the schemes that consists to locate and set up a backup route on the fly upon a failure (Figure 14).

If the backup resource is planned and reserved it does not automatically imply that it is pre-provisioned and replicated. Protection may be dedicated or shared. In dedicated protection, to each working connection is assigned its own dedicated bandwidth in the network that will be used in a case of a failure. If the traffic is transmitted simultaneously on two separate fibers (usually over disjoint routes) from the source to destination (traffic is replicated on the planned and provisioned backup path) then it is usually called 1+1 protection.

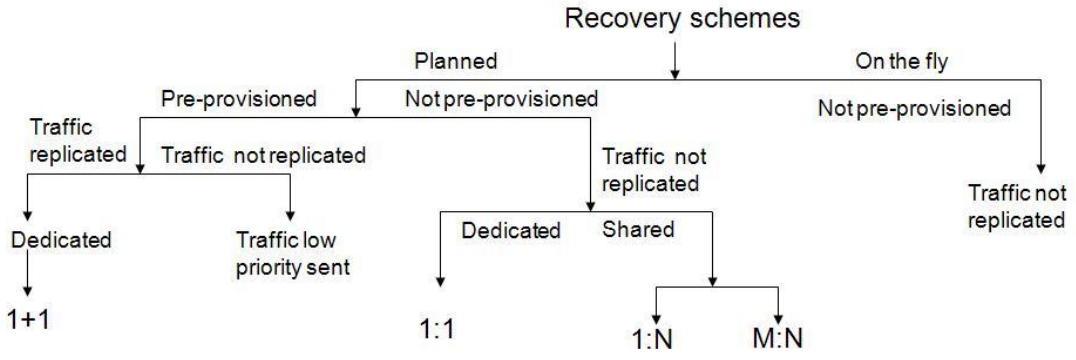


Figure 14. Recovery schemes (protection and restoration)

Using the fact that not all working connections in the network fail simultaneously, with a careful design, protection can be realized in a way that multiple working

connections can share the backup bandwidth. In that case we have a shared protection. This method reduces the amount of capacity needed in the network for protection. It is also possible to use the protection bandwidth to carry low-priority traffic under normal conditions. And in the event of the failure, this low-priority traffic is discarded and bandwidth given back to high priority traffic (pre-emption). The drawback of this method is that in the event of multiple failures, only traffic on one of the failed fibers is switched over to the protection fiber.

In 1:1 protection, there are still two fibers from the source to the destination. However, traffic is transmitted over only one fiber at a time. If the fiber gets cut, the source and destination both switch over to the other protection fiber. In a more general 1:N protection scheme, N working fibers share a single protection fiber.

In the case of protection and restoration, if a failure occurs traffic is switched from the working path to the backup path. Depending on the time when the traffic is switched back to a working path we can distinguish revertive and nonrevertive schemes. In nonrevertive schemes, the traffic remains on the backup path until it is manually switched back onto the original working path while in revertive scheme once the working path is repaired, the traffic is automatically switched back from the protect path onto the working path.

2.5.2 Multilayer survivability

Survivability can be addressed within many layers in the network. Before, it was widely believed that IP provides the only convergence layer in the global and ubiquitous Internet [5]. Equally, survivability can be performed at the physical layer, or layer 1, which includes the SONET/SDH, Optical Transport Network (OTN). It can be performed at the link layer, or layer 2 which includes MPLS, Ethernet, and/or at the network layer, or layer 3 like early mentioned.

These multiple layers work independently by default, which can be a drawback when handling network failures. Recovery methods can be easily duplicated in different layers, which results in allocating recovery bandwidth at each of the layers and might even raise the instability of the network. This approach is sometimes referred to as parallel or uncoordinated approach, as in [14]. The main advantage is that this approach is simple from an implementation and operational point of view because it requires no communication or coordination between layers.

Multilayer survivability starts from the viewpoint that a multi-technology network consists of a stack of single layer networks. In general, recovery schemes residing in lower layers often enable more effective recovery from burdensome failures like cable cuts, while failures of higher layers equipment (e.g., an ATM switch) requires additional resilience in the higher layer [15]. Most of the failures in contemporary networks are caused by digs-ups of cables during the construction works, forming

approximately 60 % of events in networks using optical cables [9] and they still happen despite a variety of preventive technologies. It is estimated that there is one failure per year per each 450 km of cables and its repair takes approximately 12 hours [16]. In this work we concentrate on failures that have a high frequency i.e. fiber-cuts and on the layer that can detect the failure the fastest way-the optical layer.

To simplify the presentation we use the example of two-layer network, where the IP (higher) layer is placed directly above the optical (lower) layer. We consider two network configuration options. In the first one (Figure 15) the IP routers are interconnected by two diversely routed WDM links. In this case although there are two independent fibers that carry the same traffic, the IP layer completely handles the protection against fiber cuts as well as equipment failures (for example router port failure).

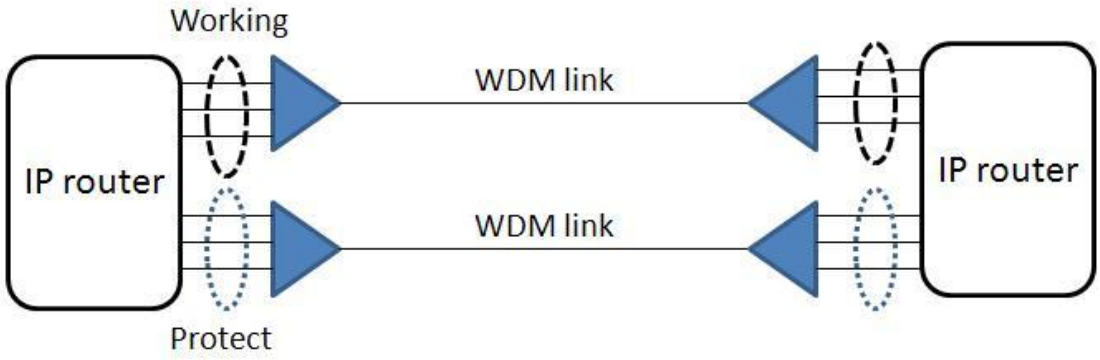


Figure 15. Protection handled by routers

The second one (Figure 16) implements protection in the optical layer. Two diversely routed fiber pairs in a single WDM system are connected with a simple bridge and switch arrangement. In this case, fiber cuts are handled by the optical layer. In this configuration the router just needs one port for protection instead of three ports in first configuration. Fiber cuts handled by the optical layer, can take care of restoring simultaneously all the channels, whereas when protection is handled by routers each individual IP link has to be restored.

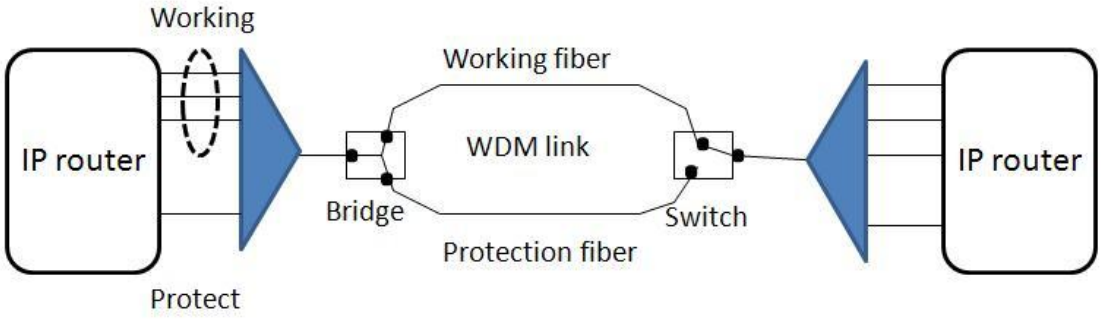


Figure 16. Protection handled by optical layer

2.5.3 Optical layer protection

To understand better the comparison between the different optical layer protection schemas, we introduce here the sublayers that constitute the optical layer.

2.5.3.1 Layers within the optical layer

As referred to the ITU G.872 OTN standard, the optical layer is an entity performing several functions such as multiplexing wavelengths, routing and switching wavelengths, and monitoring network performance at various levels in the network. In [17] ITU defined three optical layers: the Optical Channel layer (OCh), the Optical Multiplex Section (OMS) layer, and the Optical Transmission Section (OTS) layer (Figure 17).

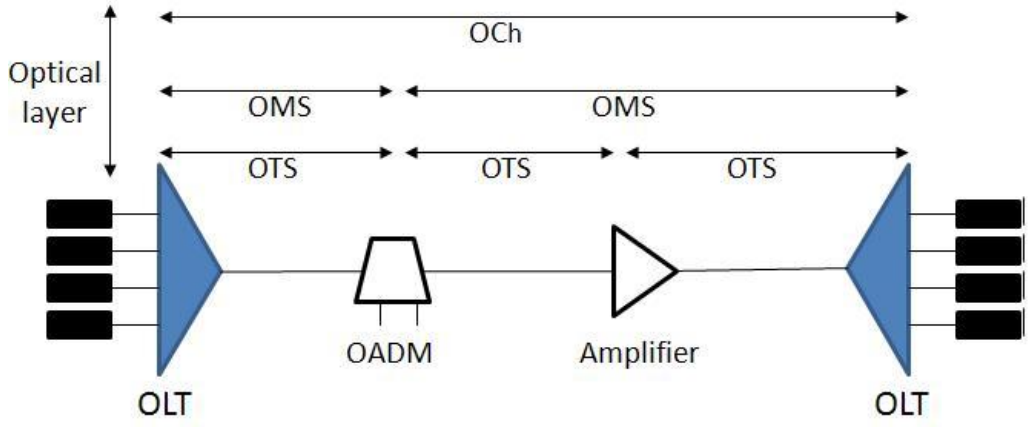


Figure 17. Optical layer

The Optical Channel layer (OCh) takes care of the end-to-end routing of the lightpaths. Here the term lightpath is used to denote an optical connection i.e. an optical channel trail between two nodes that carries an entire wavelength's worth of traffic. A lightpath may traverse many links in the network and it may get regenerated along the way but without any electronic multiplexing/demultiplexing.

The Optical Multiplex Section (OMS) is a link between OLTs or OADMs carrying multiple wavelengths. Each OMS consists of several link segments. These segments being the portion of the link between two optical amplifier stages are called optical transmission section (OTS).

Here we consider two protection schemes, 1+1 OMS and 1+1 OCh shown respectively in Figure 18 and Figure 19. For the sake of simplicity, figures only present one direction of the traffic. The OMS scheme requires two WDM terminals with one splitter and one switch (Figure 18). The composite WDM signal is bridged onto two diverse paths using an optical 50/50 splitter. The split incurs an additional 3

dB loss. At the other end, an optical switch is used to select the best among the two signals, based primarily on detecting the presence or the absence of light. An OMS layer scheme restores the entire group of lightpaths on a link and cannot restore individual lightpaths separately.

When using 1:1 protection, the WDM signal is sent over only one fiber at a time. If the working fiber fails, the WDM signal is switched onto the protection fiber. The only difference from the Figure 18 is that instead of an optical 50/50 splitter on the transmitter side there is an optical switch unit. With these approaches, the achievable protection time is lower than 10 ms [18]. On the other hand, the OCh scheme requires four WDM terminals and a splitter and switch per wavelength (Figure 19). Here two lightpaths on disjoint routes are set up for each client connection. The client signal is split at the input and the destination (optical switch unit) selects the better of the two lightpaths. Thus, an OCh layer scheme has the possibility to restore one lightpath at a time. This approach works in point-to-point, ring and mesh configurations, but the cost grows linearly with the number of channels that are to be protected. The major advantage of optical channel protection is that optical channels are not only protected against fiber cuts, but also against multiplexer/de-multiplexer failures.

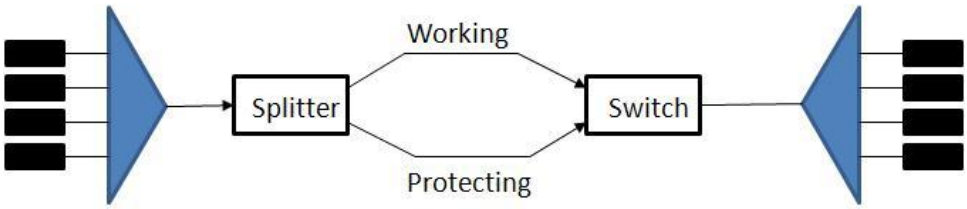


Figure 18. 1+1 OMS protection scheme

The maximum recovery time from the failure occurrence to the complete recovery of the optical link is less than 50 ms [18].

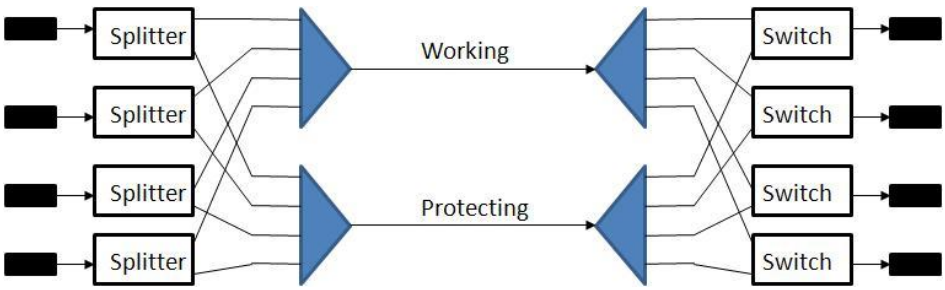


Figure 19. 1+1 OCh protection scheme

There is also significant difference in cost between OCh layer and OMS layer schemes. As the OMS layer operates on all the wavelengths, it requires less equipment than an OCh layer scheme that has to demultiplex all the wavelengths.

We could see that when using optical layer protection, recovery time needed for a complete recovery is of the order of milliseconds. For protection type 1+1, where the traffic is duplicated and sent on two distinct fibers using splitter on the transmitting and switch on the receiving side, recovery time is the smallest, around 10 ms. On the other hand for protection type 1+1 where we have also the protection in a case of failure of the multiplexers/de-multiplexers, recovery time is a slightly bigger, around 50 ms.

2.6 System availability and reliability

Recovery schemes (protection and restoration) play an important role in determining reliability and availability of the network [19]. We will use reliability and availability evaluation of the network in order to quantify the differences between recovery techniques. First, we define the terms of the availability and reliability.

2.6.1 Availability

Availability of system has been studied for many years. It is referred in many fields, such as power supply, city water supply, and nuclear power station. We define availability as a percentage of total time (e.g., in a year) that the system is up and operational. More formally, authors in [20] define availability as "the ability of an item-under combined aspects of its reliability, maintainability, and maintenance support-to perform its required function at a stated instant of time or over a stated period of time and as the ratio of uptime to uptime plus downtime." In literature we can often find a definition of the availability as the probability that a system (component, channel, path, connection, etc.) is found in the normal operating state at a random time in the future [21], [22].

Availability considers the system's failures and repairs and is usually expressed as a percentage. It reflects a statistical equilibrium between failure processes and repair processes in maintained repairable systems that are returned to the operating state following any failure.

Availability can be obtained by the formula:

$$Availability = \frac{MTBF}{MTBF + MTTR} \tag{1}$$

Where:

MTBF is mean time between failures, measured in hours;

MTTR is the mean time to repair, measured also in hours.

In the Figure 20, we can see the appearance of a term MTTF.

MTTF is the mean time to failure, expected time to failure of a system.

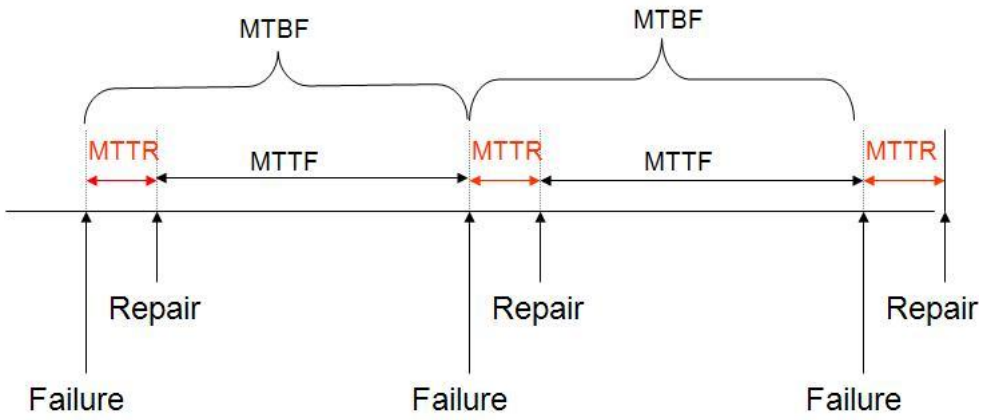


Figure 20. MTBF, MTTR and MTTF

While MTBF is one of the most used metrics in reliability engineering, it is also one that causes a great deal of confusion. As an attentive reader can see, we have decided to use the definition of the availability with the uptime of the system equal to MTBF and not MTTF. One of the reasons for that is that the time to repair the system (of our interest) is relatively fast and the value MTTR becomes negligible comparing to the values of MTTF or MTBF. Therefore, MTTF~MTBF and instead of the classic formula:

$$Availability = \frac{MTTF}{MTBF} = \frac{MTTF}{MTTR + MTTF} \tag{2}$$

We will use the equation (1).

Some systems cannot be repaired after a failure. These systems are called non-repairable. As they can fail only once, both MTTF and MTBF refer to the same metric. Because the time to failure is equivalent to the time before failure, some sources define MBTF as the mean time **before** failure (instead of **between** failure), which actually means the MTTF. That means that using MBTF to represent the mean time before failure is one of the major sources for confusion [23].

Table 2 shows the downtime that will be allowed for a particular percentage of availability, presuming that the system is required to operate continuously.

Table 2. Availability

Availability %	Downtime per year	Downtime per month	Downtime per week
90 % (“one nine”)	36.5 days	72 hours	16.8 hours
95 %	18.25 days	36 hours	8.4 hours
97 %	10.95 days	21.6 hours	5.04 hours
98 %	7.3 days	14.4 hours	3.36 hours
99 % (“two nines”)	3.65 days	7.20 hours	1.68 hours
99.5 %	1.83 days	3.60 hours	50.4 minutes
99.8 %	17.52 hours	86.23 minutes	20.16 minutes
99.9 % (“three nines”)	8.76 hours	43.2 minutes	10.1 minutes
99.95 %	4.38 hours	21.56 minutes	5.04 minutes
99.99 % (“four nines”)	52.56 minutes	4.32 minutes	1.01 minutes
99.999 % (“five nines”)	5.26 minutes	25.9 seconds	6.05 seconds
99.9999 % (“six nines”)	31.45 seconds	2.59 seconds	0.605 seconds

In this work we also use the term unavailability. If we let A be availability and U represent unavailability, given one value we can always calculate the other as follows:

$$U = 1 - A \tag{3}$$

There are assumptions that are generally accepted for practical analysis when modeling a large number of system instances over a long operating time:

1) Status of all elements can be described as a two-state “working-failed” status. A system (component, path, connection, etc.) is either available (functional) or unavailable (experiencing failure),

2) Elements fail independently,

3) Time between failure and repair times are independent memoryless processes with a constant mean,

4) The repair rate is very much greater than the failure rate. Equivalently, the MTTR is much smaller than the MTTF.

In the assumption number two, we suppose that elements fail independently, which does not imply that we disregard known correlated-failure scenarios; such as if two cables share the same duct, with a single failure would have impact on loss of both cables. Independence is assumed between elements which are not linked under a functional understanding of a system [24].

2.6.2 Reliability

Reliability is another parameter which measure is FIT, which stands for "Failure In Time." The definition of FIT is the number of failures in 10^9 hours.

In the technical sense of the word, reliability is not the same as availability. Reliability is the probability that a system or component will operate without any service-affecting failure for a period of time t. It is of concern to know how soon the next repair might be incurred, but it does not consider the repeated cycles of failure, repair time, and return to service which determine the availability of an ongoing service.

2.6.3 Modeling availability – continuous time Markov chain

In this section we briefly describe a Markov state model that is used for system availability modeling. Availability modeling is useful for the systems that still do not exist; otherwise availability could be measured rather than modeled. Markov chain is one of the methods widely used in for modeling the availability, because of their possibility to capture the probabilistic behavior of the system with attention to the design details.

We describe a Markov chain as follows: we have a set of states, $S= \{s_1, s_2 \dots s_n\}$ and the process starts in one of these states and moves successively from one state to another. It is a random process characterized as memoryless: the next step depends only on the current state and not on the sequence of events that preceded it. Moving from one state to another is happening with the probability denoted by p_{ij} (from state s_i moves to the state s_j). This probability is called transition probability. In this work we will rather use the transmission rates as the description of the transfer from one state to another.

Failure rate λ – denoted by the Greek letter lambda, specifies the rate of the transition from functioning state, "up" state to failure state "down" state. If the failure rate is constant, it can be calculated as the inverse of MTBF. In general, failure rate is expressed in failures per hour-unit (1/hour or $hour^{-1}$).

$$\lambda = {}^{1}/_{MTBF}$$

(4)

Repair rate μ – specifies the rate of the transition from one failure state, "down" state to the functioning "up" state. Repair rate can be calculated as the inverse of MTTR.

$$\mu = {}^{1}/_{MTTR}$$

(5)

In this work we will express MTBF and MTTR in seconds, taking into account that the systems in our observations are able to recover in order of seconds, therefore failure and repair rate will be also expressed in units (1/second or s^{-1}).

The simplest repairing model for availability modeling using Markov chain-state model is presented in the Figure 21. Usually, the "up" state is denoted as 0 and the "down" state as 1 to facilitate their identification.

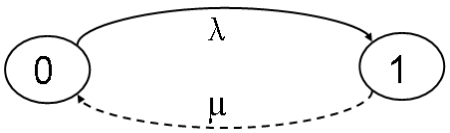


Figure 21. The simplest Markov state model for availability modeling

This means that the system can be either in the working state or in the failure state. Knowing the values of the system's failure and the repair rate it's relatively easy to calculate the availability of the presented model. Steady state availability can be computed as the equilibrium state probability of the working state (probability of being in the "up" state).

In order to include failure prediction, we have incorporated more transitions states corresponding to the cases of prediction correctness. Adding more states makes the computation more complicated. Keep in mind that building the state model with online prediction changes not only the number of existing states in which one system can be found, but also changes its parameters. For example, for the system with the possibility of proactive fault recovery is expected to have shorter meant time to repair (MTTR) value then the ordinary one. Therefore, as the MTTR is directly related to the parameter repair rate (inversely proportional), it increases it.

Models of proactive schemes have been developed along with preventive software maintenance (an overview can be found in [25]) but these models were mainly based static distributions and have not covered online prediction. In the case of software rejuvenation authors in [26] used Markov state models to demonstrate improved availability/reliability. However, to our knowledge none of the models published so far have explicitly modeled the process of link failure prediction including the false predictions and missed predictions as well as prediction-driven repair actions. Developed method, with all the necessary explanations will be presented in the next chapter.

2.6.4 Modeling reliability – continuous time Markov chain

As we have earlier defined the difference between availability and reliability, here we will just clarify the difference when it comes to modeling. Reliability is defined as the probability of failure occurrence up to time t given that the system is fully operational at t=0. In terms of Markov chain-state modeling this is equivalent to a non-repairable system and computation of the first passage time into the "down" state.

3 Chapter
MACHINE LEARNING FOR PROACTIVE RECOVERY

3.1 Introduction

In this work we focus on the prediction of link failures. As the networks are growing more and more complex, the term “failure prediction” varies among authors and also its meaning has been changed over the decades. In this chapter we present the basis of the failure prediction and discuss several methods that have been proposed in the literature.

With ever-growing complexity and dynamicity of the network, classical reliability theory and conventional methods do rarely consider the actual state of a system and failure processes. In contrast to classical reliability methods, online failure prediction is based on runtime monitoring and a variety of models and methods that use the current state of a system and, often, the past experience for learning as well.

3.2 Proactive method

As mentioned, the traditional fault tolerance mechanisms have encountered limits due to the growing complexity, dynamics and flexibility of new network architectures. Emphasis has thus been placed on the network with self- * properties where the asterisk can be replaced by any of “healing”, “optimization”, “configuration” or “recovery” [27].

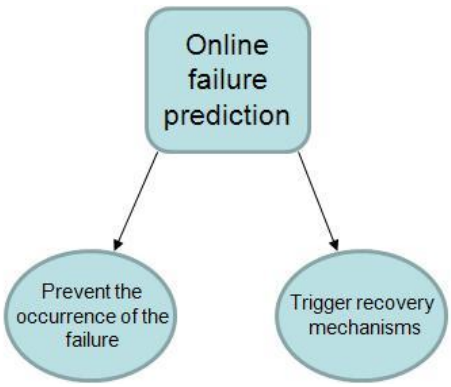


Figure 22. Online failure prediction

In such networks, goal becomes how to proactively handle the failures. If a system knows about a critical situation in advance, it can try to apply countermeasures in order to prevent the occurrence of a failure, and/or it can prepare/trigger recovery mechanisms for the upcoming failure in order to reduce the down-time (Figure 22).

3.2.1 Definition of basic terms

The aim of online failure prediction is to predict the occurrence of failures during runtime based on the observation of the current system state. The following section provides more precise definitions of the basic terms such as fault and failure, which will be used throughout this work.

- Faults are the adjudged or hypothesized cause of an error; the root cause of an error. Several classifications of faults have been proposed in the literature among which the distinction between transient, intermittent and permanent faults is best known [28]. This distinction is based on the frequency of the occurrences.

- We define failure as an event that occurs when the delivered service deviates from correct service. We can say that failures are manifestation of faults. For example, fault like accidental fiber cut can provoke a failure (lost of signal). Following [29] differentiation can be made on the permanent nature of the failure. In this way we can separate failures that can bring down an entire link (for example due to a fiber cut or an equipment breakdown) and failures that are not permanent and often only affect some of the channels in the WDM link (for example outages due to polarization mode dispersion effects). In [30], a second differentiation is proposed, based on the dynamics of the failure. A separation is made between failures that are unexpected sudden events (hard) and failures which are the result of the aging of the equipment (soft). In this work we consider both, hard and soft failures like in [29] and [30].

- We define also features as the distinguishing characteristics of classes of data that precede the failure. The features are what allow us to distinguish different types of failures. For example, the features in character recognition might be the number of straight or curved lines, the number of holes in the character, while in speech recognition; features might be the properties of the electrical signal generated by a microphone close to the speaker.

Online failure prediction is concerned with a short-term assessment that allows to decide, whether there will be a failure, e.g., few seconds to few minutes ahead or not. On the other hand, prediction of systems reliability is concerned with long-term predictions based on failure rates, repairing rates, architectural properties, etc.

Part of the online failure prediction is a root cause analysis. Root cause analysis, having observed some misbehavior in a running system tries to identify the fault that caused it, while failure prediction using that information tries to assess the risk that the misbehavior will result in future failure (Figure 23).

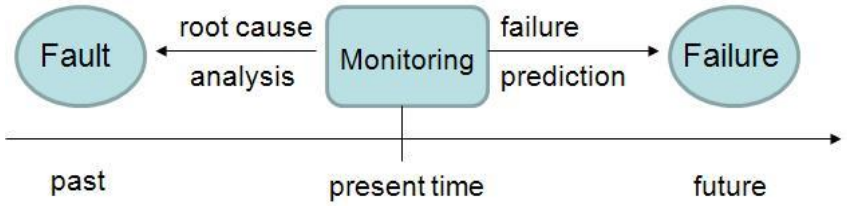


Figure 23. Fault, failure and failure prediction

For example, if it is observed that the connection is broken, root cause analysis tries to identify what is the reason for that unavailability and failure prediction tries to asses whether this situation bears the risk that the system cannot deliver its expected service which may also depend on the system characteristics (is there a backup connection or some other fault tolerance mechanisms available?) in the network.

3.2.2 Online prediction

The task of online prediction is visualized in the Figure 24. The potential occurrence of a failure is predicted at the present time denoted as t. Decision is made based on the current system state and based on the system monitoring within a data window of length $\Delta t_{m.}$ The prediction is valid for some interval $\Delta t_{p,}$ which is called the prediction period. Increasing Δt_p increases the probability that a failure is predicted correctly. For example, if we simply let $\Delta t_p \rightarrow \infty$, predicting that a failure will occur would always be 100 % correct.

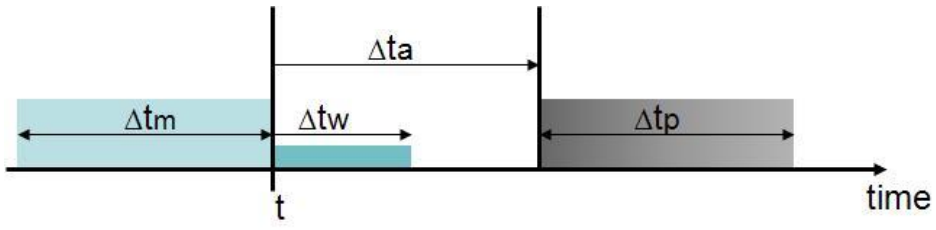


Figure 24. Online prediction

Failures are predicted with some time in advance $\Delta t_{a\ .}$ If we perform a prediction at time t, we would like to know whether at time t+ Δt_a a failure will occur or not. If for example a preventive recovery is triggered upon a failure prediction, Δt_w is the minimum time needed for a system to go back to a working state. This means that the

time in advance Δt_a has to be at least as long as the warning time Δt_w . If time in advance Δt_a is shorter than the warning time, there would not be enough time to perform any preparatory or preventive actions.

Reader must keep in mind that in the Figure 24, sizes of the time intervals Δt_m, Δt_a and Δt_p are not representative. Depending on the applied Machine Learning (ML) algorithm monitoring interval can vary. If we let the monitoring interval to become very wide, in order to increases the probability of the accurate prediction of the failure, we risk decreasing the advance interval Δt_a missing the prediction. More discussion about the tradeoff between the sizes of the intervals will be done in following chapter.

Now that we have described the basic terms of online prediction, we introduce the proactive fault management and its phases.

3.3 Proactive fault management - design cycle

Proactive fault management can consist basically of six steps:

1) The first step is **defining the problem**. The goals of a knowledge discovery must be identified and the goals must be verified as actionable. For example if it is possible to detect in advance a failure, is it possible to put the newly discovered knowledge to use? Does the network have the possibility to reroute the potentially threatened traffic? Simply having the information without the possibility to use it does not improve the situation.

2) The second step is **collecting the dataset**. In order to detect failure-prone situations it is necessary to monitor certain parameters. The simplest method is the method of "brute-force", which means measuring everything available in the hope, that the right (relevant) features can be isolated (for example voltage, temperature, etc.). However, a dataset collected by the "brute-force "method contains in most cases noise and missing feature values, and therefore requires pre-processing [31].

3) **Data Pre-processing** comprises techniques concerned with analyzing raw data mainly including data segmentation, data transformation, data cleaning, data reduction, and data discretization. Technique of data segmentation attempts to separate the data into useful units of information for the following use. These data units may be incomplete, noisy or inconsistent. In a case of incomplete data, missed values can be filled, and in a case of noisy parts they can be removed (data cleaning). Finally data pre-processing generates a dataset more pertinent than the original one, which can significantly improve the efficiency of further prediction.

Often data pre-processing can be more time consuming than prediction itself [32]. In practice, it has been generally found that data cleaning and preparation takes approximately 80 % of the total data engineering effort [33]. So it can be understood that data pre-processing is not a small task. In this work, we will also show not only how the process of data pre-processing has the important role to the outcome but also how the outcome changes with different types of pre-processing.

4) Next step is to make an **online failure prediction**. For that purpose various methods are proposed in literature. We choose to predict failure using machine learning (ML) algorithms. Inductive machine learning is the process of learning a set of rules from instances (examples in a training set), or more generally speaking, creating a classifier that can be used to generalize from new instances. Every instance in any dataset can be represented using the same set of features. These features may be either categorical or numerical. Values of a categorical features are discrete while values of a numeric features are either discrete or continuous [34]. In this work we call the conversion of a numeric feature to a categorical one, discretization, irrespective of whether that numeric feature is discrete or continuous.

   In the literature, two types of machine learning algorithms can be found, supervised learning and unsupervised learning. Learning is called supervised if the above-mentioned instances are given with the known labels (the corresponding correct outputs), in contrast to unsupervised learning, where instances are unlabeled. In this work we will be using supervised learning because in order to obtain the clear information about the risky event we need to label the instances. By applying unsupervised algorithms researchers hope to discover unknown but useful classes of items [35].

   The choice of which specific supervised learning algorithm should use be used is a critical step. Many different learning algorithms have been proposed and evaluated experimentally in different application domains. It is not important whether a certain learning algorithm is superior to others, but under which conditions a particular method can significantly outperforms others on a given application problem. Evaluation is more often based on prediction accuracy (the percentage of correct prediction divided by the total number of predictions). And if the error rate evaluation is unsatisfactory, we must return to a previous stage of supervised ML process. In that case, a variety of factors must be examined: maybe relevant features for the problem are not being used, the parameter tuning is needed, larger training set is needed, etc. Or the selected algorithm is inappropriate.

   The goal of this work has not been to provide a review of all existing learning techniques but rather to cover wide-ranging issues of supervised machine

learning such as data pre-processing and according to the needs to suggest one method that will give satisfying results: a proof of concept.

5) Based on the outcome of online failure prediction, a decision has to be made which of the actions, i.e., countermeasures, should be applied and when it should be executed. This step is called **action scheduling.** Decision is based on the function that takes into consideration confidence of the prediction (probability of the event) in the one hand and the effectiveness, the complexity and the cost of actions in the other hand in order to determine the optimal trade-off. For example, if we want to trigger a rather costly technique, the scheduler should be almost sure (high confidence of the prediction) about an upcoming failure, whereas for a less expensive action less confidence in the correctness of failure prediction is required.

6) After online failure prediction and execution of the actions it is necessary to constantly compare the results to an accuracy feedback in order to modify the ML process if needed. During the **post-processing phase** adjustments may be applied to data collection, to segmentation and/or to feature extraction. This phase is required to maintain the validity of the process.

The process of applying supervised ML to a real-world problem is described in the Figure 25. Blue line represents the part needed in order to modify the steps in process when the evaluation gives the unsatisfied results. As it can be seen from the figure, all the steps can be the subjects of modification, starting from the initial step of identification of the parameter.

As we noted before, if for some reason we can not obtain an acceptable results with online prediction maybe the cause lies in the wrong choice of the measured parameter. For example, instead of measuring the temperature, the measure of voltage would give better results.

Also, there can be a problem with the representation of the data (data pre-processing step). Maybe data segmentation and/or transformation were not well done. Once having finished the phase of data pre-processing, the phase of algorithm selection should follow.

The choice of the algorithm is based on the conditions given by the implementation of the online prediction. There is no universal ML algorithm that can correspond to all the problems. The world of ML algorithms is very large and sometimes it’s difficult to make a good choice. With the good knowledge of the strengths and limitations of each method it is possible to find the learning algorithm that will suit the most. For example, sometimes online prediction needs to be very fast with no tolerance to missing values, or to noise and sometimes online prediction has to be very accurate, not depending on the speed and sometimes both. That's why the choice of a suitable algorithm is a very important part of the overall process. In this

chapter we will also concentrate on the conditions imposed for the case of the prediction of link failures. Based on the list of requirements we will show the direction that we had to follow for the right choice of algorithm.

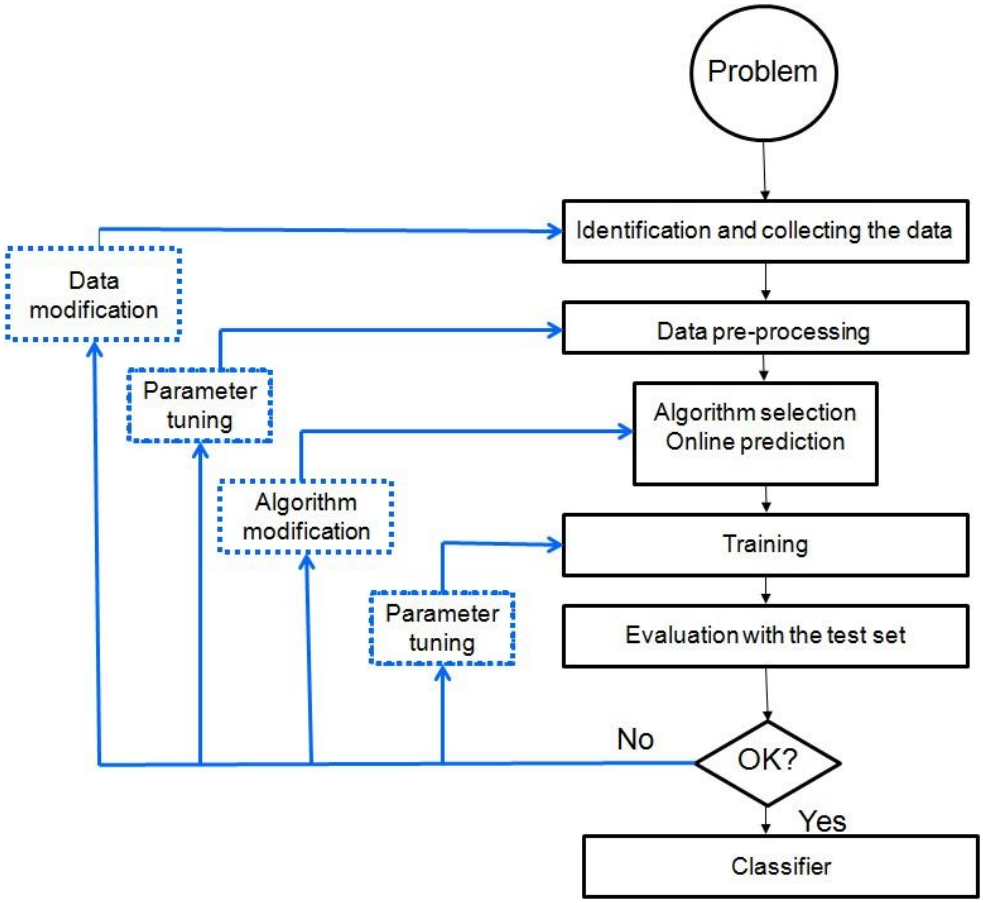


Figure 25. The process of supervised ML

We mentioned earlier that the ML algorithm has to be accurate -precise. Without being accurate online prediction can cause more problems and provoke bigger unavailability time of the observed system. The precision is just one of the metric that are used for the evaluation of the algorithm. This metric is an important mean to compare the adequacy of the algorithm to our problem. In the next section we provide an overview of the most frequently used metrics along with their definitions.

3.3.1 Evaluation metric

The goal of failure prediction is to predict failures accurately, which means to cover as many failures as possible while at the same time generating as few false alarms as possible. A perfect failure prediction would be able to achieve a one to one matching between predicted and true failures. In order to investigate the quality of

failure prediction algorithms and to compare their potential it is necessary to specify metrics. This section will introduce several established metrics for the goodness of fit of prediction. A more detailed discussion and analysis of evaluation metrics for online failure prediction can be found in [36].

To be able to define two frequently used metrics to express prediction quality, precision and recall, first we need to define four classes of prediction. These classes are given in the contingency table in Table 3.

Any failure prediction belongs to one out of four cases. Decision given by the prediction algorithm can be right or wrong. A failure prediction is a true positive (TP) if a failure occurs within the prediction period and a failure warning is raised. If the algorithm misses to predict a true failure, it is a false negative (FN). Analogously, if no true failure occurs, and no failure warning is raised, the prediction is a true negative (TN) and if no true failure occurs and a warning is given we are talking about false positive (FP) prediction.

Table 3. Contigency table

	Failure	**No Failure**
Prediction: Failure (warning)	Correct warning (TP)	False warning (FP)
Prediction: No Failure (no warning)	Missing warning (FN)	Correct no-warning (TN)

These metrics are also called “contingency table metrics” because they are based on the afore-mentioned contingency table.

Precision is defined as the ratio of the number of correctly identified failures to the number of all predicted failures.

Recall is defined as the ratio of the number of correctly predicted failures to the total number of failures that actually occurred.

$$precision = \frac{n_{TP}}{n_{TP} + n_{FP}} \tag{6}$$

$$recall = \frac{n_{TP}}{n_{TP} + n_{FN}} \tag{7}$$

Measures precision and recall, can take values in the interval [0, 1] and values close to 1 are the most desirable. And if both are equal to 1, optimal prediction is reached: a one-to-one mapping of true and predicted failures.

In general, precision and recall show an inverse proportionality. Improving the precision, i.e., reducing the number of false positives, often results in worse recall, i.e., increasing the number of false negatives, at the same time and vice versa.

Another widely used metric integrating the trade-off between precision and recall is the F-measure. F-measure is defined as [37]:

$$F - measure = \frac{2 * precision * recall}{precision + recall} \tag{8}$$

Attentive reader can notice that metrics precision and recall do not take the number of prediction of true negative (TN) into consideration. It might be concluded that true negatives are not of interest for the assessment of failure prediction techniques. This is not necessarily true; on the contrary, the number of the true negatives can help to assess the impact of failure prediction method on the system. For example if we observe two prediction methods that perform equally well in terms of TP, FP, and FN, hence both methods will achieve the same precision and recall. However, if one operates on measurements taken every millisecond and the other on the measurements that are taken every second, the difference between the two methods is reflected only in the number of TN and will only become visible in metrics that include TN.

Beside prediction and recall, another frequently used metrics is called accuracy.

Accuracy is defined as the ratio of the number of all correct predictions to the number of all predictions that have been performed, given with the equation (9).

$$accuracy = \frac{n_{TP} + n_{TN}}{n_{TP} + n_{FP} + n_{FN} + n_{TN}} \tag{9}$$

As we can notice from the definition, metric accuracy take the number of prediction of true negative (TN) into consideration.

As we need our method to be very fast, to detect the premises of the potential risky event almost immediately, measurements should be taken with the largest

possible sampling rate; this sampling rate is often limited due to the equipment constrains. Using the largest possible sampling rate, we risk of getting too much data that has to be processed by the ML algorithm. Chosen ML algorithm needs to have that possibility and speed of processing.

When choosing the ML algorithm that is the most appropriate to the problem, it should be mentioned that the quality of prediction also depends on the data monitoring window size $\Delta t_{m,}$ ahead time Δt_a, and warning time Δt_w. That's why the contingency table should be determined for one specific combination of $\Delta t_{m,}$ $\Delta t_{a,}$ and $\Delta t_{w.}$

3.3.2 Discussion on the Precision/Recall curve

Now that have defined metrics precision and recall it is possible to use the precision/recall curve for the visualization of the trade-off between them. Many failure predictors use the simple adjustable decision threshold, upon which a failure warning is raised or not. It's a simple solution that consists in finding a right threshold level. For example, if the threshold level is too low, a failure warning is raised very easily which increases the chance to catch a true failure-resulting in high recall. And if the threshold level is very high, precision is good while recall is low.

3.4 Online failure prediction methods in different telecom-areas (related work and approaches)

Online prediction that we could find in the literature connected to the telecom area can be split into several major categories by the type of the input data used. Authors in [38] divide approaches into 2 types: methods that evaluate the current system state and methods that do not evaluate the current system state (Figure 26). The later one is reliability based with the key input parameter distribution of time to failure. A lot of work exist providing methods to fit various reliability models to data with failure time occurrences. Nice overview can be found in [25]. However, these methods are tailored to long-term predictions and do not work appropriately for short-term predictions needed for online prediction. For this reason, they are not in the center of our scope.

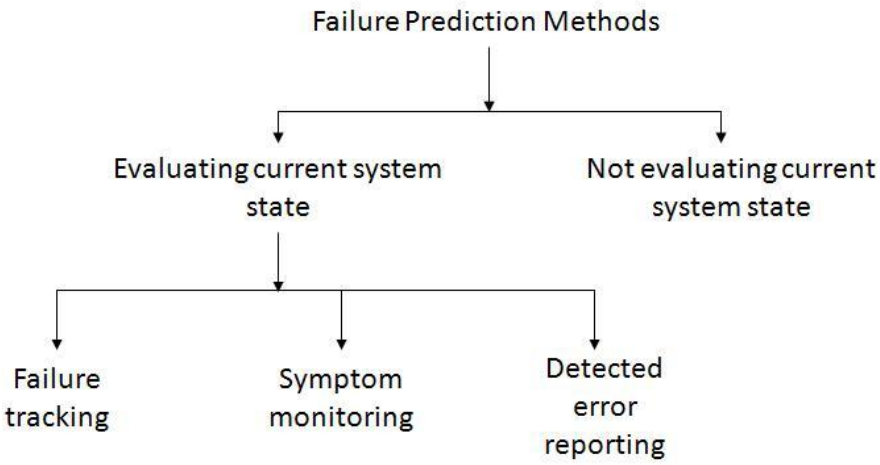


Figure 26. Online failure prediction approaches

Different methods that evaluate the current system state have been developed. They can be subdivided into methods that evaluate the occurrence of previous failures (failure tracking), methods that evaluate symptoms of faults (symptom monitoring), and methods that evaluate the manifestations of faults (detected error reporting).

3.4.1 Failure tracking

Prediction methods that belong to the failure prediction based on failure tracking try to estimate the probability distribution of the time to the next failure from the previous occurrence of failures. As we are focusing on the link failure prediction caused by the machines during the excavation, simple failure tracking would result in poor estimation since there is independence between the events of fiber cut. More details concerning the prediction method using failure tracking can be found in [39], and [40].

3.4.2 Symptom monitoring

The majority of existing prediction techniques are symptom based. Symptoms are defined as the side-effects of faults. For example, when trying to predict a software failure, side effects are the increase of the memory consumption, the increase of the number of running processes, etc. Methods based on the symptom monitoring evaluate periodically measured system parameters (such as amount of memory usage, number of processes, etc.) in order to detect deviation from normal system behavior. With this monitoring it is possible also to detect service degradation which would lead to a failure. In this group of prediction techniques four principle approaches have been identified: failure prediction based on the function approximation, classifiers, system model, and time series analysis (Figure 27).

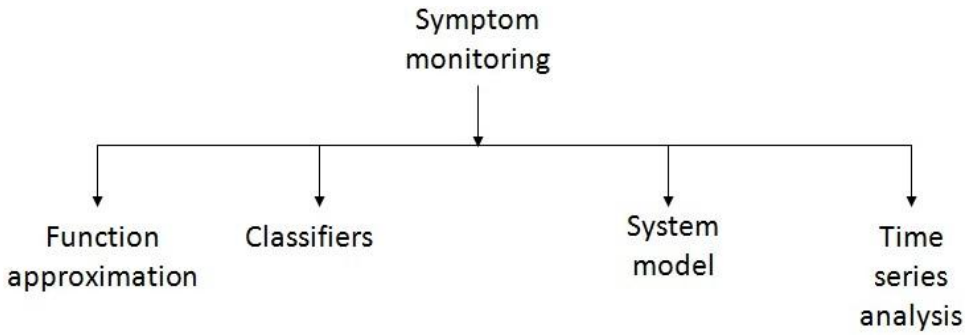


Figure 27. Online failure prediction approaches - symptom monitoring

Here we will describe basic principles of these four groups with the examples.

3.4.2.1 Symptom monitoring - using Function approximation

The term function approximation is used in a large variety of areas. When used in terms of online failure prediction it tries to mimic a target value, which is supposed to be the output of an unknown function of measured system variables as input data. The current value is measurable during runtime, but function approximation is used in order to extrapolate resource usage into the future and to predict the time of resource exhaustion. Function approximation can be done using regression (curve fitting) like in Figure 28, where parameters of a function are adapted such that the curve best fits the measurement data.

Authors in [41] used function approximation for prediction of performance of Apache Axis server. Furthermore, function approximation can be completed using the machine learning, more specifically using neural networks. For example, authors in [42] have proposed to use neural networks for failure prediction of mechanical parts while [43] described how standard neural networks can be used for failure prediction in large scale engineering plants.

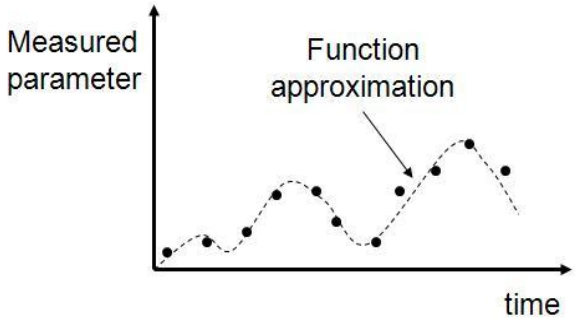


Figure 28. Function approximation

3.4.2.2 Symptom monitoring - using Classifiers

Instead of approximating a target function and trying to predict the future value of the parameters of the interest, it is possible to evaluate the current values of system directly. This algorithm uses method called classification.

Failure prediction using method of classification has the objective to give as the final outcome whether the current situation is failure prone or not. On the one hand, there is no need for the complicated prediction of the future state like in symptom monitoring using the function approximation. But on the other hand, failure prediction methods based on classifiers have to be trained from failure-prone as well as non failure prone samples. Once the classifier is trained, the goal of classification is to assign a class label to a given input data vector. In general, monitoring one parameter (one parameter builds one input data vector) is not sufficient to infer whether a failure is imminent or not. That's why the input vector is usually constructed from several monitored parameters within a time window.

Numerous approaches with a large number of techniques have been developed for the classification based on various functional representations such as decision trees, decision lists, Artificial Neural Networks (ANN), Support Vector Machines (SVM) and learning set of rules. Authors in [44] made a following division of the approaches (Figure 29):

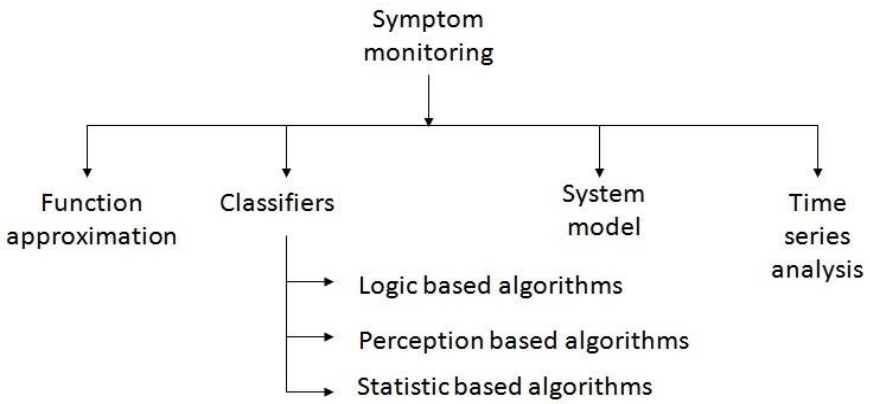


Figure 29. Classifiers

1. **Logic based algorithms**: they consist of two groups of logical (symbolic) learning methods: *decision trees* and *rule-based classifiers*. One of the most useful characteristics of the logic based algorithms is their comprehensibility.

   For example, it can be easily understood why a decision tree classifies an instance as belonging to a specific class. Decision tree is a classifier in the form of a tree structure where each node is either a leaf node or a decision node, like in the Figure 30. Decision node specifies some test to be carried out on a single attribute value, and the leaf node indicates the value of the target

attribute (class) for example. This type of classifier constitutes a hierarchy of tests and an unknown feature value during the process of classification is dealt with the passing the example down all branches of the node where the unknown feature value was detected, and each branch outputs a class distribution [44].

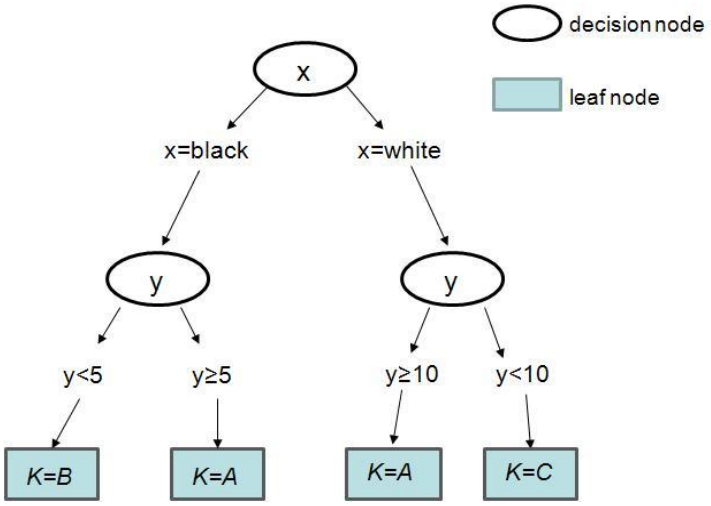


Figure 30. An example of a simple decision tree

Decision trees are usually univariate (since they use splits based on a single feature at each internal node); however, there are a few methods that construct multivariate trees [45].

We have decided not to use them in our research because the majority of decision tree algorithms can not perform well with the problems that require diagonal partionining. Partitioning means splitting the data into subsets based on attributes. The resulting regions after partitioning are all hyper rectangles because the division of the instance space is orthogonal to the axis of one variable and parallel to all other axis.

Decision trees can be translated into a set of rules (building a rule-based classifier) by creating a separate rule for each path from the root to a leaf in the tree [46]. Basic idea is to construct the smallest rule-set that is consistent with the training data. A large number of learned rules is usually a sign that the learning algorithm is attempting to “remember” the training set, instead of discovering the assumptions that govern it. This problem is called overfitting and its usually facing logic based algorithms. This situation, however, is very dangerous if we want to use our resulting decision tree for the purpose of prediction. Most likely a tree of this sort is over fit for the training data and will not perform well on new data.

2. **Perception based techniques**: they consist of *single layered perceptrons*, *multilayered perceptrons* (also called Artificial Neural Networks-ANN) and *Radial Basis Function networks* (RBF). Basic inspiration for creating the neural networks comes from the model of the functioning of the human brain. Human brain is composed of very large number of processing units, namely neurons, operating in parallel. Neurons have connections called synapses, also operating in parallel. Perceptron based techniques are using that as a role model, where the basic processing element is called perceptron. It has inputs that may come from the environment or may be the outputs of other perceptrons.

   Perceptron-like methods are binary, meaning that in the case of multiclass problem one must reduce the problem to a set of multiple binary classification problems. In addition to being binary, perceptrons can only classify linearly separable sets of instances. For example, if a straight line or plane can be drawn to separate the input instances into their correct categories, the perceptron will find the solution for the classification. On the contrary, if the instances are not linearly separable, learning will never reach the point where all the instances are classified properly.

   If we compare perception based techniques with the decision trees (logic based algorithm), we can notice that neural networks usually perform as well as decision trees, but seldom better. Also the training time for a neural network is usually much longer than training time for decision trees.

   Our first instinct was to use neural networks for online link failure prediction (that's why we will pay more attention to the ANN in this chapter) but as they are often characterized by high variance and unsteadiness we have decided to try the classification with the classifier based on the statistic based learning algorithm (Naive Bayes classifiers). However, in the next few paragraphs we will make a basic brief description of the ANNs.

   A multi-layer neural network consists of large number of neurons (layers) joined together in a pattern of connections, shown in the Figure 31. We can distinguish three classes of layers: input layer (which receive information to be processed), output layer (where the result of the processing can be found) and hidden layers (the layers in between). Properly determining the size of the hidden layer can present a problem. There have been studies concerning the minimum amount of neurons, given the fact that the underestimation of the number of the neurons can lead to poor approximation and generalization capabilities, while excessive number can result in overfitting (problem already mentioned with logic based algorithms).

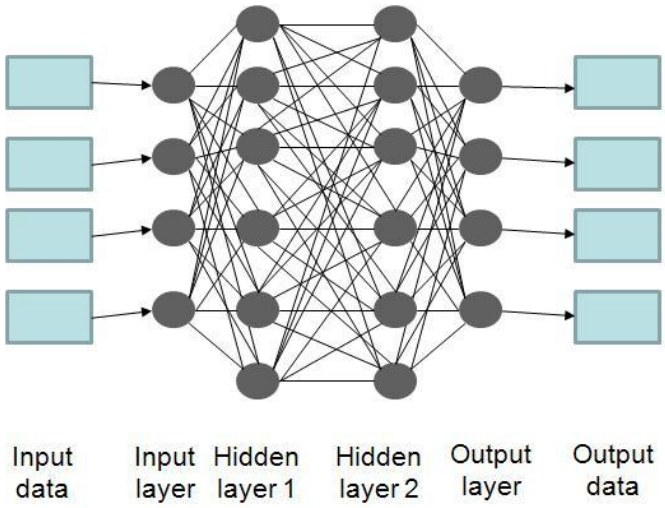


Figure 31. An example of an artificial neural network with one input layer, two hidden layers and one output layer

Network is trained to determine input-output mapping using the set of paired data. Initially, the weights of the connections between neurons are set to random values and during the training period, instances of the training set are repeatedly exposed to the net until the weights are fixed. Output of the net is compared to the desired output for the chosen instance and all the weights in the net are adjusted slightly in the direction that would bring the output values of the net closer to the values for the desired output. In general, it is necessary to perform a number of weight modifications before it reaches a good weights configuration. There are several algorithms that exist with which a neural network can be trained. One of the most well known and the most widely used algorithm for the estimations of the weight values is the Back Propagation (BP) algorithm. When the weights are fixed the network is ready to be used for the classification of a new set of data.

To sum up, although ANNs have been applied to many real-world problems, their biggest disadvantage is their lack of ability to reason about their output in a way that can be effectively communicated [44], in another words the lack of comprehensibility.

Radial Basis Function (RBF) networks are also ANNs, consisting of three-layer feedback network, in which each hidden unit implements a radial activation function. This type of perception based technique is out of our scope.

3. **Statistic based learning algorithms**: they consist of *Naive Bayes classifiers*, *instance-based learning* and *Support Vector Machine* (SVM). Bayesian classifiers are the most well known representative of all the classifiers. They are also one of the most effective classifiers, in the sense that their predictive

performance is competitive with the state of the art classifiers. A comprehensive book on Bayesian networks and Bayesian artificial intelligence with its applications can be found [47].

Conversely to earlier mentioned Artificial Neural Networks (ANN), Bayesian classifiers are characterized by having an explicit underlying probability model, which provides the probability that an instance belongs in certain class, rather than simply a classification.

One of the reasons why the Bayesian classifiers are usually less accurate than ANNs is the strong assumption of independence among features. This strong assumption of independence among features is the reason for the descriptive name "naive" Bayes classifiers. There were attempts to overcome this independence like in [48]. Semi-naive Bayesian classifier is another important attempt to avoid the independence assumption.

On the other hand the major advantage of the naive Bayes classifier is its short computational time for training compared to other prediction algorithms [44]. That was one of the reasons why we chose Khiops classifier based on the Naive Bayes classification for the classification of the events. Also, the most interesting feature of Bayesian Networks (BNs) compared to decision trees or neural networks is the possibility of taking into account prior information about a given problem in terms of structural relationships among its features. For example if some event is more frequent in the nature, there is more chance to reappear after the classification. In the next paragraph we explain the principle of the Bayes' rule.

Using Bayes' rule, we combine the prior and the evaluated probability and calculate the posterior probability distribution:

$$p(A/B) = \frac{p(A) \cdot p(B/A)}{p(B)} \tag{10}$$

Where:

- $p(A)$ is the prior probability; it represents what we know regarding the possible values that A may take *before* knowing the results of classification. This probability plays a big role in decision-making for proactive rerouting. It means that if some event is very frequent in the nature, it has more chances to reproduce. For example, if we have as the outcome from the classifier two events with equal probabilities, our final decision will be based on the frequency of those events in the reality;

- $p(B/A)$ is the evaluated probability, obtained using the classification method. It tells us how likely our event B is if the parameter of the distribution takes the value A;

- $p(B)$ in the denominator is the normalizer to make sure that the posterior probability $\mathrm{p(A/B)}$ integrates to 1;

- $p(A/B)$ is called the posterior probability because it tells how likely A is *after* the classification. This is the value that we are interested in, crucial for making a decision of rerouting.

When using Bayes' rule, one can notice the strong influence of the prior probabilities to the final result. So it should not be assumed that all events are equally probable (and we showed that this is especially not the case concerning cable cuts). The objective of the data collection regarding Naïve Bayes classification is then two-fold: on the one hand to build training data based on the different types of events and on the other hand to build the prior probabilities.

More details about the Bayes classifiers can be found in [49]. For the purpose of our research we use the classifier called Khiops. This classifier falls into the category of the Bayesian classifiers and more explications about the way of functioning are provided in [50], [51], and in [52].

Apart from the Bayesian classifiers we also mention the existence of the Fuzzy classifiers. Bayes classification in general requires that input variables take on discrete values; therefore the monitoring values are frequently assigned to finite number of bins. This can lead to bad assignments if monitoring values are close to a bin's border. Fuzzy classification addresses this problem by using probabilistic class membership.

Support Vector Machine (SVM) is another type of algorithm using the statistic based learning. SVMs have been developed by V. N. Vapnik [53] and this technique revolves around the notion of a margin. This margin is presented as a clear gap that separates two data classes. The goal of this method is to create the largest possible distance between the hyperplanes that separate these classes. Once the optimum separating hyperplane is found, data points that lie on its margin are called support vector points and the solution is presented as a linear combination of only these points. One can come to a conclusion that the question of complexity of an SVM it is not related to the number of features encountered in the training data. That's why SVMs are well suited to deal with online prediction (won't- fail/will-fail) where the number of features in the learning task is large with the respect to the number of training instances.

When choosing the most appropriate type of classifier between classifiers based on neural networks, naive Bayes rule and SVMs our preference was the classifier based on naive Bayes rule, because for among other reasons, in order to achieve its maximum prediction accuracy, naive Bayes classifiers need a relatively small dataset comparing to others that need a large sample size. In another words they train very quickly since they require only a single pass on the data either to count frequencies (for discrete values) or to compute the normal probability density function (for continuous variables). Univariate decision trees are also reputed to be quite fast, even several orders of magnitude faster than neural networks and SVMs but as we were dealing with the multivariate problem, univariate decision trees were not a good option.

So far we presented two methods of symptom monitoring for the purposes of online failure prediction, using function approximation method and using classifiers. Algorithms using the function approximation method, as the name says itself, try to approximate the certain function and to predict the future value, meaning that there is no mapping between input and output values. On the other side, algorithms using classification method need inevitably two sets of data; one for training the algorithm and another for testing. In the training algorithm, a set of data that corresponds to the failure prone event and failure free event has to be provided. In the next paragraph we present another method of symptom monitoring that uses system models.

3.4.2.3 Symptom monitoring - using System models

Failure prediction approaches belonging to this category utilize a model of failure free (normal system behavior). Online failure prediction approaches rely on modeling of failure free behavior only. Real time measurement is compared to the expected normal behavior (stored values) and if there is a significant deviation between these values a failure is predicted. There is no need to train the system with the failure prone situations. Depending on how the normal behavior is stored, model-based prediction approaches can be categorized into: instance models, clustered instance models, stochastic models and control theory models. As they are out of our research, we will not go into the details explaining them.

3.4.2.4 Symptom monitoring - using Time series analysis

Failure prediction approaches belonging to the time series analysis accounts for the fact that data points taken over time may have an internal structure (such as autocorrelation, trend or seasonal variation) that should be accounted for. Time series are defined as the ordered sequence of values of a variable at equally spaced time intervals. They are often used to monitoring industrial processes.

There are many different methods used to model and forecast time series. We can distinguish two groups, one concerning univariate time series and multivariate time series models but as it is beyond the realm and intentions of our research, we will not go into the details.

3.4.3 Detected error reporting

This group of prediction techniques implies that before the failure, system is capable of producing the error report that precedes that failure. Usually these kinds of reports are feasible in the computer systems where error is defined as the part of the total state of the system that may lead to its subsequent service failure. If we assume that we are observing a system capable of producing error reports, these reports would be input data to different failure approaches that deals with the event-driven input data. There comes the difference between prediction using detected error reporting and the prediction using symptom monitoring. Symptom based monitoring approaches operate on periodic system observations while detected error reporting approaches operate on the observation obtained with the error report whenever some error is detected in the system. Furthermore, symptoms are in most cases real-valued while error events are mostly discrete, categorical data such as event IDs, component IDs, etc.

We mention here two main groups of failure prediction approaches that analyze error reports. First group consists of rule-based approaches and the second one consists of pattern-based approaches. As in our work we don't have the possibility to have error reporting (whenever an error is detected) that these approaches use, we will however use the idea of pattern recognition while making a representation of the input data for classifier. This way we increase the accuracy of the prediction. Method will be explained later on.

Failure prediction methods that belong to the group of rule-based approaches derive a set of rules where each rule consists of error reports. For example, authors in [54] define a rule where if an error type A (link alarm) and B (link failure) occur within 20 seconds, then error C (high fault rate) will occur within 40 seconds (Figure 32). In general, the relationships between error reports are captured as rules and used for a prediction.

Pattern recognition techniques on the other hand operate on sequences of error events trying to identify patterns that indicate a failure-prone system state. Authors in [55] investigate the type of error reports while authors in [56] focus on the time when errors are detected. Method that integrates both parts of error reports, time and type together turns the sequence of error reports into a temporal sequence.

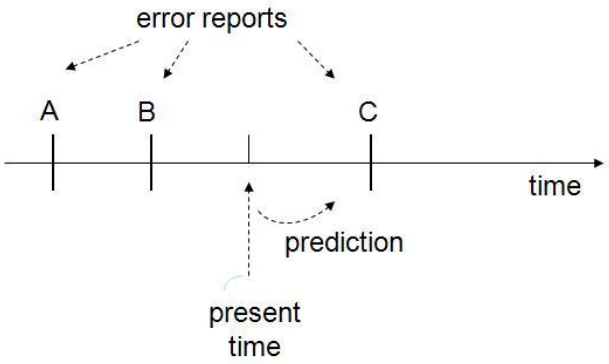


Figure 32. An example of a failure prediction based on the occurrence of error reports

Pattern recognition techniques gave us not only the idea but also the technique and inspiration for the presentation of the data. We didn't use any error reports like in failure prediction concerning software but nevertheless pattern recognition had the part in the link failure prediction.

3.4.4 Focus of this overview

We made a short overview of the existing failure prediction methods that have been proposed in the literature and some of them used to predict failures of computer system online (Figure 33).

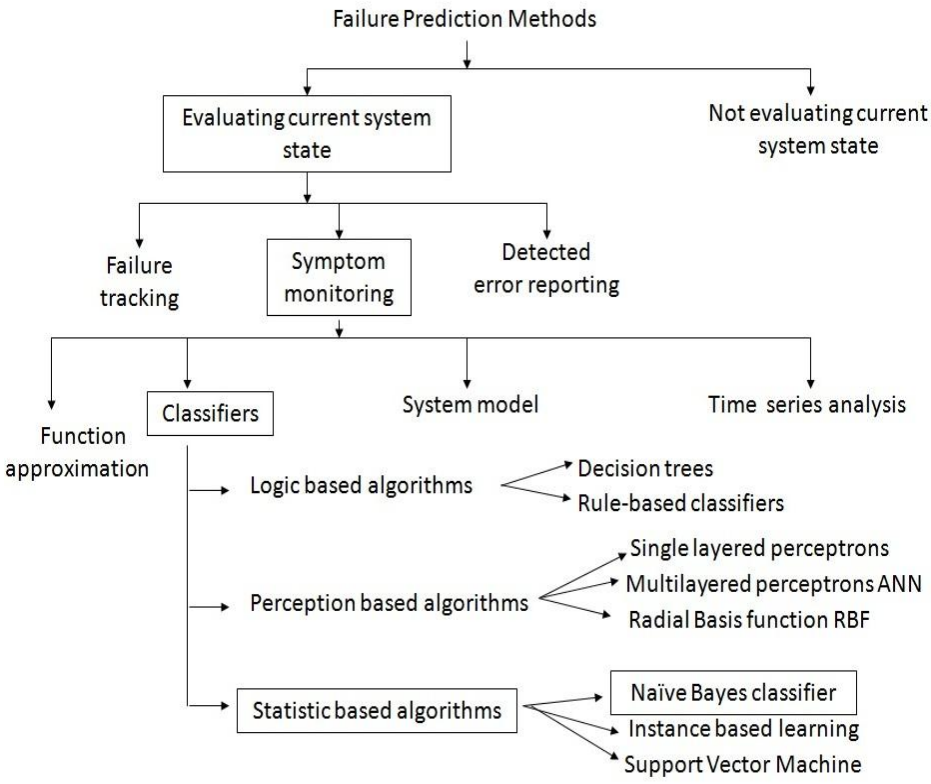


Figure 33. Overview of the prediction methods

The goal of this overview was not to make a complete catalog of all the existing methods presenting their strong and weak sides but to explain and to develop a theoretical understanding of the relationships among these algorithms, and of when it is appropriate to use each, justifying the choice that we made comparing them and evaluating them. It can be seen in the Figure 33, that the method that we used in our research is framed by a rectangle.

4 Chapter
RISKY EVENT DETECTION PROOF OF CONCEPT

4.1 Introduction

The most important application of optical fibers is in the field of communication, but at the same time optical fibers are finding more and more applications in the area of sensing. In this section we briefly describe several examples of optical fibers used as sensors for various types of parameters. Emphasis is places on the two categories of optical sensors: extrinsic and intrinsic ones.

Once familiar with the wide range of possibilities of using fiber as a sensor for various types of parameters, we concentrate on one parameter in particular, state of polarization (SOP) of the light-Stokes parameters. Basic explanations needed for understanding the Stokes parameters are also given in this chapter.

Finally, we present the possibility of detecting the changes in the fiber's environment directly by following the changes of the SOP. In order to evaluate the feasibility of recognition of events external to the fiber (like vibration, hit, etc.) we have set up an experimental test bed where we have provoked different situations. We also explain the problems that we encountered during the process of classification of these events and solutions that we used to overcome them. Results are presented at the end of this chapter.

4.2 Fiber as a sensor

Using fiber optic sensors, it is possible to measure almost any external parameter, such as pressure, temperature, electric current, magnetic field, rotation, acceleration, strain, and chemical and biological parameters with great precision and speed [57]. Compared to other types of sensors, optical fibers offer lower cost, smaller size, higher accuracy and greater flexibility. Another important attribute of fiber optic sensors is the possibility of measuring over a continuous region or measuring at a large number of discrete points in some region, which would be otherwise too expensive or complicated using conventional sensors.

Fiber optic sensors can be classified broadly into two categories: extrinsic and intrinsic.

In extrinsic sensors, fiber acts as a device to transmit and collect light from a sensing element that is external to the fiber. The sensing element simply responds to the external perturbation and the change in characteristics of the sensing element is transmitted by the return fiber for analyses. Fiber as an extrinsic sensor, plays a role of a transmitting the light beam to and from the sensing region. These types of sensors are easy to design and fabricate. Examples of extrinsic sensors are liquid-level sensors (based on the changes in the critical angle), movement detectors (based on the change in the transverse alignment between two fibers) and pressure sensors which find wide application in automobiles and aerospace [58].

In the other type of sensors, called intrinsic sensors, the light beam never leaves the fiber. The physical parameter to be sensed directly alters the properties of the optical fiber, which in turns leads to changes in a characteristic such as intensity, polarization, and phase of the light beam propagating in the fiber leading to sensing. Compared to above mentioned sensors, intrinsic sensors are much more complex, but much more sensitive. Examples of intrinsic sensors are fiber optic gyroscopes; sensor based on fiber Bragg gratings, etc.

In this work we will use the fiber as an intrinsic type of sensor. Sensing signals will be in the form of changes of the properties of the light beam called polarization of the light, which propagates through the fiber.

In the following section we will give some examples of simple extrinsic sensors with the explanations of how they operate and in what kind of industry they are used. Objective of that part is to give the reader the main vision about sensors and to introduce into the more complicate world of intrinsic sensors. More details about fibers as sensors with all necessary explanations and examples can be found in [59], [60], [61] and [62].

4.2.1 Extrinsic fiber optic sensors

One of the simplest sensors is the fiber optic liquid-level sensor [63]. Principle is based on the changes in the critical angle due to the liquid level moving up or down. In the Figure 34, we can see that the light that is propagating down an optical fiber is totally internally reflected from a small glass prism and coupled back to the return fiber. While the external medium is air, the angle of incidence inside the prism is greater than the critical angle, and hence light experiences total internal reflection.

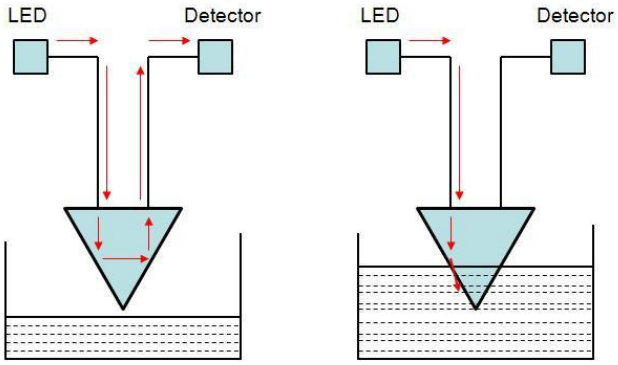


Figure 34. Fiber optic liquid-level sensor

When the prism comes in contact with a liquid, the critical angle at the prism-liquid interface decreases and the light gets transmitted into the liquid, resulting in a loss of signal. This kind of sensor can be used for sensing levels of various kinds of liquids, such as water, gasoline, acids, etc. just with the proper choice of prisms material. Since the sensor does not carry any electrical signal, it can be used to monitor the level of highly inflammable liquids, such as petroleum products.

Another interesting case is movements' detection. This simple sensor is based on the fact that the transmission through a fiber joint depends on alignment of the fiber cores. Light coupled into an optical fiber couples across a joint into another fiber that is detected by a photodetector. Any movement provokes deviation of the fiber pair from perfect alignment and any misalignment can be sensed immediately by the detector. The misalignment between fibers can be caused also by acoustic waves and pressure meaning that such devices can be used for measuring the pressure in the arteries, bladder, etc. This domain is out of the scope of our interest but we are mentioning it here to present how wide the application area of the optical fiber sensors is.

4.2.2 Intrinsic fiber optic sensors

As mentioned before in intrinsic sensors the light beam never leaves the fiber and the physical environment changes some characteristic of the propagating light beam. A typical example is the sensor for bending. When an optical fiber is bent, a portion of the propagating light beam along the bend is incident at angles less than the critical angle and thus it suffers from attenuation. This can be used for the pressure sensors that specially used to measure the load distribution.

Usually when fibers are deployed as sensors they are physically embedded in materials and that way create so called "smart structures" [64]. Reasons why the fibers are embedded into the materials are to allow measurement of parameters such as load, strain, temperature, and vibration, from which the health of the structure can

be assessed and tracked on a real-time basis. One of the examples of smart structures is the bridge, like in [65] where the strain measurements are performed on the concrete railway bridge in Sweden using series of fiber Bragg gratings (FBGs) sensors [66]. As the bridges represent a big infrastructure investment, the management using the smart system which detects internal conditions of the structure (that would be difficult to access otherwise) and that provides an automated, fast response plays an important role in safety issues. Like early mentioned, a key parameter of interest in structural applications is the measurement of strain. The dimensional deformation due to load (frequent passing of heavy trucks) and temperature can be related to various performance problems. More interesting examples of the smart bridges with fiber-optic sensors were treated in [67], [68].

Grating based sensors appear to be useful for applications where sensors should offer distributed sensing of strain or temperature. The basic principle used in FBGs based sensor system is to monitor the shift in wavelength of the returned 'Bragg' signal with the changes in the measured parameters (e.g., strain, temperature).

Here in the Figure 35 is presented the basic Bragg grating based sensor system. A spectrally broadband source of light is injected into the fiber and a narrowband spectral component at the Bragg wavelength is reflected by the grating.

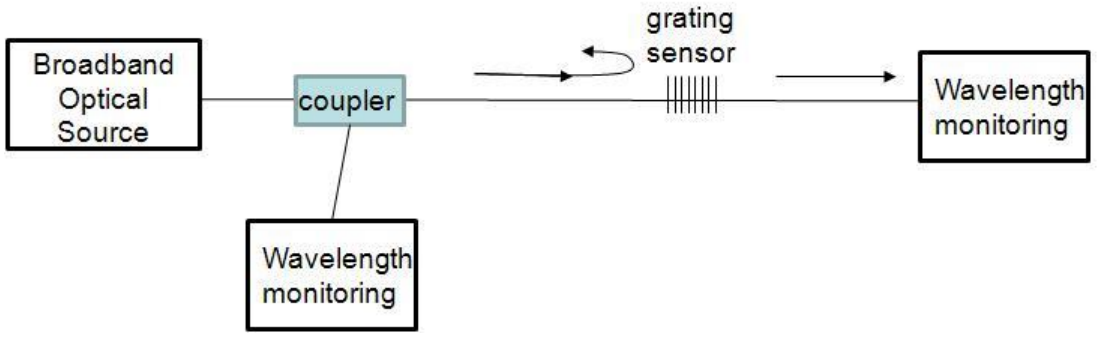


Figure 35. Basic Bragg grating based sensor system

This reflection is achieved by adding a periodic variation to the refractive index of the fiber core, which generates a wavelength specific dielectric mirror. As depicted in the Figure 35 this spectral component is missing in the transmitted light. That means that a perturbation in strain or temperature results in a shift of the Bragg wavelengths which can be detected in either the reflected or transmitted spectrum.

The strain response arises due to both the physical elongation of the sensor, and the change in fiber index due to photoelastic effects, whereas the thermal response arises due to the thermal expansion of the fiber material and the temperature dependence of the refractive index. For example to resolve a temperature change of ~

0.1 °C, or a strain change of 1 μstrain, wavelength resolution of ~ 1 pm is required (for Bragg signal with wavelength λ around ~ 1.3 μm) [66].

Besides being a part of the smart structures systems these sensors are finding more and more application in other areas of life. For example, they have been used also for detection of any kind of activity in the vicinity of the asset over long distances [69]. Same authors suggest using these sensors for continuously monitoring vulnerable borders, gas transmission pipelines and high speed rail network.

All previously given examples of deploying fiber as a sensor were explored in the environment such as air or ground. In the next section we present the sensing possibilities of the fiber deployed as submarine cable. We shall adopt the knowledge of its sensing possibilities and shall base our further research on its one potential that is proven to work in submarine environment as well as in the air or ground environment: measuring the state of polarization of the light traversing the fiber.

In November 2010, International Telecommunication Union (ITU-T) released the technology watch report entitled "Using submarine communications networks to monitor the climate" [70]. This report gives an overview of how old and new submarine cables could be used as a major resource and a real-time global network to monitor climate change and to provide tsunami warnings. Here a term submarine cable is used for copper wires and optical fibers.

As the temperature and salinity are basic elements of the ocean, their measurement on the sea floor (where submarine telecommunication cables lie) becomes the essential. In the report it is stated that temperature could be obtained by measuring the resistance of the copper wire or by measuring the optical round-trip travel time for a transoceanic cable using the fibers in the cable.

Also, submarine cables have been used to measure ocean currents around the world. In particular, over the last 25 years a cable has been used to take daily measurements of the volume of water transported by the Florida Current, creating one of the longest available time series of data on ocean water transport [70].

In previous paragraphs, we showed some of the interesting examples of using fiber as a sensor. Still, the most common use of the fiber stays in the communications systems. Besides measuring the external parameters in order to detect environmental irregularities, optical fibers can be used to monitor the appropriate parameters that are directly connected to the transmission of the light. In this work we concentrate on one particular parameter called state of polarization (SOP) of the light-Stokes parameters.

4.3 Stokes parameters

4.3.1 Why Stokes parameters?

Signals used in communication systems are susceptible to signal degradation caused by various physical factors such as chromatic dispersion (CD), polarization mode dispersion (PMD), amplifiers noise accumulation and non–linear effects. Most of these phenomena can be controlled by system design except the polarization mode dispersion (PMD) that is known to degrade performance and to contribute a major obstacle for the upgrade of already installed fiber using per channel bit rates of 10 Gbps or above especially for long haul optical transmission. In fact, fibers fabricated and installed before the year 1995 tend to exhibit PMD coefficients of 0.5 ps/km or even higher [71]. Polarization mode dispersion compensation (PMDC) has been proposed both in electrical or optical domains as an approach to increase the tolerance of high speed transmission systems against PMD [72]. Unfortunately, PMD is not a static effect and the biggest problem of PMD mitigation is the random temporal drift of PMD due to the environmental disturbances, such as temperature, wind speed, sun altitude, etc [73].

Recently new modulation formats based on phase modulation and coherent detection have been introduced for 40 Gbps and 100 Gbps transponders generation offering the possibility to compensate the PMD using the adapted dynamic digital filter directly implemented in the transponder boards. But until a few years ago, optical fiber systems were using the direct detection, where the decision on the receiver side was based on the intensity of the signal, without any information of the signal phase making it impossible for the use of such approach. So, it was important to find the fastest changes in both state of the polarization (SOP) and differential group delay (DGD) as they provide the speed requirement for PMD compensators. That was one of the reasons for the large number of studies of the SOP changes (changes of the polarization of the light) in different environments and under different conditions.

Previous experiments showed that the SOP drift is relatively slow in buried fibers [74], [75], on the order of hours or days, and relatively fast in aerial fibers [76], [77], on the order of microseconds in the winter.

In [78] authors measured the SOP variation on WDM systems, during a 6 month field trial and discovered a “human activity signature”. That means that the SOP variation can perfectly capture environmental variations around the fiber. Aerial fibers on the other hand show faster SOP variations because the fiber is exposed directly to a dynamic environment and undergoes greater strain and temperature fluctuations [79]. In [79] a clear correlation between daylight and fast SOP changes can be seen. In general, during the day the sun causes heating on the fiber and the wind causes strain, while nights are relatively calm.

Submarine cables also presented the different SOP drift times between the day and night. Authors in [73] noted that SOP data during the night starts at a higher magnitude and drops faster than during the day, which means that during the day, the vibration frequencies of the cable shift to the higher frequencies. One can assume that there is a correlation between deep ocean waves and fiber vibration. Rapid SOP variations have also been measured in [80] and have been correlated with the tide's effects.

Seeing the great possibility of capturing the vibrations around the cable, authors in [81] have decided to artificially induce mechanical vibrations that could be easily produced in installed systems carrying live traffic. For example, hitting rack edges with the cable or dropping the patch cable on a table top. This is explained by the fact that the patch cables of the working systems are frequently touched or moved when doing service or maintenance work with currently inactive systems sharing the same patch panel or cable duct. As a result, polarization changes follow a 3 dimensions random walk on a microsecond timescale.

Previous experiments confirmed that locally exerting stress on a fiber induces birefringence, which causes a change in the SOP of the transmitted light. And changing the SOP at one location affects the whole downstream part of the fiber.

Taught from the experience of others aforementioned, where it is shown how changes in the fiber's environment directly influence on the changes of the SOP, for the purpose of our research we have decided to follow up the: polarization of the light in order to detect in advance event that could potentially damage the fiber.

Once detected, events that present future threats for the link should be classified in order to react adequately in the vicinity of the danger and escape the very likely bad outcome. For the classification of the events we have decided to use Orange Labs tool for mining large data bases called Khiops which is also free to use and upload from http://khiops.com/.

Before giving more details about that software, including the instructions for our specific use we give some details about the polarization of the light, the SOP and Stokes parameters. Presuming that the potential reader may not have the basic knowledge of the polarization of the light in order to simplify the reading process, we will give the meaning of the basic terms.

4.3.2 Stokes parameters in general

The polarization state of a light source is represented by four numerical quantities S_0, S_1, S_2, and S_3 called the "Stokes parameters". Notation varies; one can find in the literature equivalent Stokes vectors given as (S_0, S_1, S_2, S_3) or (I, Q, U, V), where all of the four elements in the Stokes vector S_0, S_1, S_2, and S_3 are real numbers (Stokes

parameters). The first Stokes parameter S_0 is a measure of the total intensity of the light incident on the sensor. The second and third Stokes parameters S_1 and S_2 provide information about the linear polarization state of the incident light while the fourth stokes parameter S_3 provides information about the circular polarization state of the incident light and cannot be determined using only linear polarization filters [82].

If we choose a Cartesian coordinate system (x, y, z), so that the x and y are perpendicular to the direction of light propagation z, and if E_x and E_y are the electric field components in the x and y directions, where the brackets < > indicate averaging over a long time, hence, Stokes parameters are presented by:

$$S_0 = I_{(0°)} + I_{(90°)} = < |Ex|^2 > + < |Ey|^2 >$$

(11)

$$S_1 = I_{(0°)} - I_{(90°)} = < |Ex|^2 > - < |Ey|^2 >$$

(12)

$$S_2 = I_{(45°)} - I_{(135°)} = Re < ExEy >$$

(13)

$$S_3 = I_{RHC} - I_{LHC} = Im < ExEy >$$

(14)

In equations (11)-(14), $I_{(0°)}$ is the intensity of the 0° filtered light wave, $I_{(90°)}$ is the intensity of the 90° filtered light wave I_{RHC} and I_{LHC} are the intensities of right- and left-handed polarized light and so on. For example a sensor capable of characterizing polarized light based on (11)-(14) must employ four linear polarization filters offset by 45°. More information concerning the Stokes parameters and their measure can be found in the literature [83], [84], [85].

Stokes showed that the beam of light (and electromagnetic radiation, in general) can be described completely by four parameters [86]. However, the polarization state is completely determined by the three ratios S_1/S_0, S_2/S_0, S_3/S_0, which is called the normalized Stokes parameters. It is standard practice to normalize the parameter by dividing it by the intensity; in this case S_0 represents the total intensity of the light. They can have possible values between -1 and +1. We have decided to use normalized values in our work because this way we got to eliminate the noise effects [87].

4.4 Experiment

In order to evaluate the feasibility of recognition of events external to the fiber, we have set up an experimental test bed where we have provoked different situations. Our experiment consists in measuring the normalized Stokes parameters (S_1, S_2 and S_3) which provide a description of the polarization state of an electromagnetic wave at a given time. We capture the Stokes parameters changes over the time with a fast polarimeter Adaptif Photonics.

The set up consists of a non modulated laser which is transmitting light into a spool of 100 km Standard Single Mode Fiber. Various mechanical movements are applied on the fiber. Because of the limited possibility to emulate destructive events in the laboratory we have not experimented real field fiber cuts, but instead movements which are not fatal for the fiber but reasonably close to a potential fiber cut premises (hit, swaying and vibration). For illustration purpose, Figure 36 and Figure 37 show the changes of the polarization states due to a hit on the fiber and due to a swaying of the fiber as a function of time represented with Cartesian and Poincare coordinates, respectively.

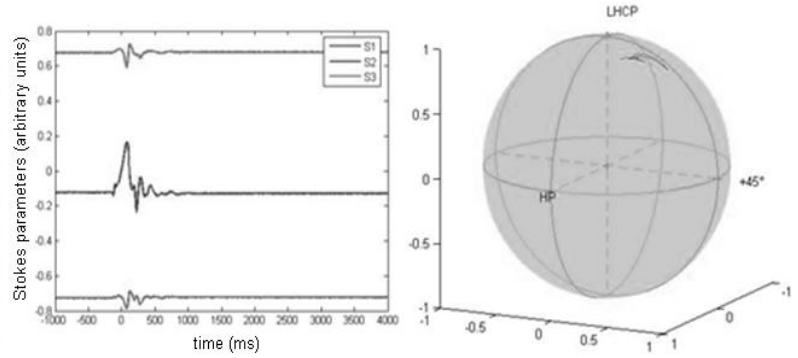


Figure 36. Cartesian and Poincare sphere representations of Stokes parameters time evolution in a case of a hit on the fiber.

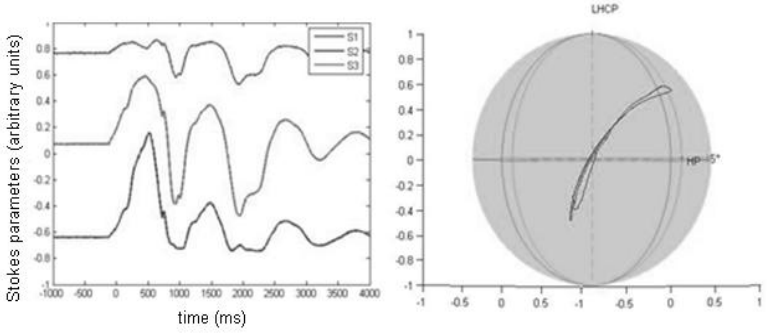


Figure 37. Cartesian and Poincare sphere representations of Stokes parameters time evolution in a case of a swaying of the fiber.

Stokes parameters show two different signatures for these two events. Experiments were repeated several times with comparable movements and always shown comparable patterns for the SOP variations.

The difference between both signatures is easily distinguishable by the human eye which gives a first clue that event recognition may effectively be implemented. We propose in this work to exploit artificial intelligence tools to recognize events while they are going on and then to determine which strategy should be applied to minimize the impact of the eventual risky events.

As explained in [88] the human brain is able to distinguish patterns and to make classifications without performing a lot of computation and measurement while computers are good at computation and relatively poor at association. The shortcomings of computers in associative activities can be compensated by using their high computational performance. Among the different existing techniques reviewed in the previous chapter, we chose to utilize a classifier called Khiops (as we need a simple identification of the events and not a prediction of the future state).

Khiops is France Telecom's scoring tool for mining large databases. It implements a discretization method based on the chi-square statistic. The tool also produces a scoring model for supervised learning tasks, based on a naïve Bayes approach [89]. The interested reader may find more information on classifiers in [90].

To work properly, Khiops needs a set of data for machine learning (training process) and a set of data for testing process. For the purpose of the training process several data sets were collected. Every data set constitutes and is represented as one class at the input of the Khiops. A class may belong to the group of the classes where "there is no potential risk of the changes in fiber's environment" or it may belong to the group of the classes where "there is approach of the risky event in the near future". The objective of the training process is to obtain the function (in the form of an equation) that most precisely describes the behavior of the transmission link in the case of the different mechanical attacks (in our case hit, swaying and vibration). That function maps sets of inputs attributes to certain classes- called supervised learning.

After obtaining the model function, for the purpose of testing process we are using again data sets represented as classes as input values for Khiops, but this time data sets are obtained from real time measurements and are arbitrarily assigned to the classes (predicted classes).

As the Khiops is based on naive Bayes approach it calculates the probability of each hypothesis for the data under test and makes decisions on this basis. Here we define hypothesis as the probability of a certain data set to belong to a certain class (including the predicted class).

Khiops gives results in the form of a confusion matrix presenting the instances of the predicted class with respect to the instances of the current class. Dividing these

two values we get probability of the event recognized and predicted by Khiops with the condition that this probability still does not take into account probability of events in reality. This probability plays a big role in decision-making for proactive rerouting. It means that if some event is very frequent in the nature, it has more chances to reproduce. For example, if we have as the outcome from the Khiops two events with equal probabilities, our final decision will be based on the frequency of those events in the reality.

Classification success is highly dependent on the form of the data representing the classes. In order to obtain a classification as accurate as possible of the events we have studied several representations of the measured data. The representations were used as set of input for the classifier. By measuring changes in polarization of the light (Stokes parameters) passing through the optical cable that is exposed to physical experiments we got data in a form of a function in time domain (Figure 36 and Figure 37). Next step, represented in the next section, was to determine the best possible representation of the measured data in order to obtain the highest classification success.

4.4.1 Problem of data representation

Classification of the events consists in the identification of the premises. Acquisition time is the time from the moment when premise of the risky event is detected to the moment of making a decision of rerouting, shown in the Figure 38. Duration of the acquisition time is a tradeoff between accuracy of the classification and service disruption time.

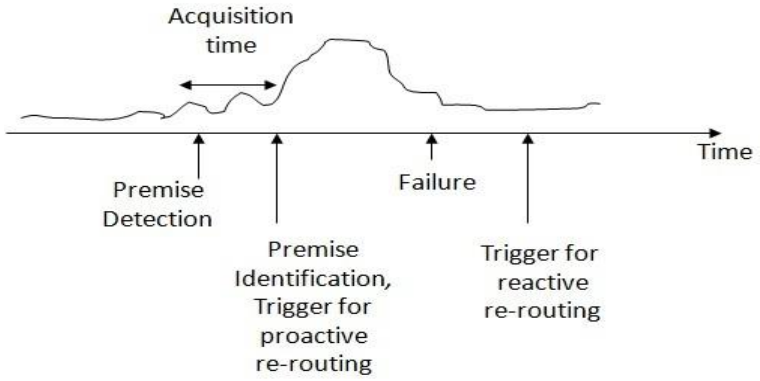


Figure 38. Definition of the acquisition time, premise detection and premise identification

If we allow longer acquisition time on the one hand, classifier Khiops will be able to perform classification of the events with more accuracy but on the other hand maybe that will not leave enough time to reroute all the traffic before the failure happens. If we decide to trigger the rerouting too early (acquisition time will be too small and not long enough to give a sufficient accurate classification), we may trigger

it uselessly. Reversely if we decide to wait too long for rerouting the traffic, we may lose the advantage of proactive failure detection.

We use Matlab to test several representations of the data. The method consists of a time window of data that is slid for previously determined step values. A Fourier transformation (FT) is performed on the data window to assess the frequency components of the SOP variations.

This representation can be configured with several parameters for a given measurement data set:

- Size of the window (*N)* points
- Number of points taken after Fourier transformation-FT (N_f)
- Step for sliding the window (*delta n*)

In the next section we show how the parameters have an impact on the success of events recognition expressed in percents (%). The more successful the recognition, the more accurate is the classification.

Sampling period for data acquisition is set to 8 ms corresponding to the time between two consecutive points in time domain. For experimental reasons, amount of collected data is not the same for all events. With the set of values we create the training data base for Khiops and then look at the success rate with respect to parameters change.

Our first instinct, at the beginning of the representation of the data, is to use just one Stokes parameter (we randomly chose parameter S_3) and to see if the obtained classification would result with success or not, and if it result with success, to determine how high is that success. First outcome of the Khiops shows that there is a potential for using this kind of recognitions of events but the success of recognition is not satisfactory.

Encouraged with the first outcome, next step is to explore the possibility of the utilization another two more parameters (S_1 and S_2) already given by the polarimeter. Khiops input values are established in a form of classes and each class consists of the combination of parameters S_1, S_2 and S_3. This way result of the classification is improved, comparing to the result when just one parameter (S_3) was used.

When creating a class that represents a certain event, we use the combination of the parameters S_1, S_2 and S_3 in the exact order as they appear here in the text (For example S_1, S_2, S_3 – class A). Having some doubts if the order of the appearing in the class would make any difference on the result of the classification, we created a class which would contain all the permutations (without repetitions) of these parameters. Since we dispose with 3 parameters, permutations would produce 3! elements in each

class. They are going to be processed as mentioned above with different sizes of the window, different number of points given after the FT, and with the different size of the step for sliding the window; all that just in order to determine the combination that would give the best results (in terms of accuracy).

Using the permutation of elements when forming a class does not introduce any improvement to the classifications. That brings us to the conclusion that Khiops is insensitive on the order of the appearance of elements within a class.

Attentive reader can notice that until here all the research is done with Cartesian representations of Stokes parameters. But, seeing the impossibility to obtain better results continuing using the Cartesian representation, we oriented our research toward the representation of Stokes parameters with Poincare sphere.

As shown in the Figure 36 and Figure 37, Stokes parameters are also presented on the Poincare sphere as the projection of normalized Stokes vector termination point onto the surface of a unity radius sphere. The Poincare sphere is a display format for monitoring signal-polarization changes, since all states of polarization are seen at the same time. This is accomplished by assigning each state of polarization its own specific point on the Poincare sphere. That way for example, points on the equator represent states of linear polarization, the poles represent right-hand and left hand circular polarization and other points on the sphere represent elliptical polarization.

Taking into consideration that each point on the Poincare sphere has a unique set of coordinates defined by the sphere's three-dimensional axes S_1, S_2 and S_3, data representation can be done using the inclination (polar angle) and azimuth (azimuthal angle) instead of typical Cartesian representation of parameters S_1, S_2 and S_3. Notice that the radius (radial distance) has a unit value.

The starting point of the polarization vector can be situated anywhere on the Poincare sphere. We have noticed that events that fall into the same category-class leave behind similar, comparable signature on the sphere, whether the start point is, for example, situated on the equator or on the pole or somewhere else on the surface of the sphere. In order to be sure that classifier Khiops will not make a decision based on where the signature is located (on which part of the sphere) but based on the difference between signatures, we have been using Matlab to distribute the same signature equidistantly all over the surface of the sphere (Figure 39). Process is repeated for all the signatures. That means that we are artificially producing signatures over the whole sphere so that during the training phase classifier Khiops has the real opportunity to learn (in our case to develop the above mentioned model function that the most precisely describes functioning the link of interest).

Other way for obtaining the same result (whenever a new signature/new event is made) is to instead of producing the copies of that signature/event all over the surface of the sphere, it should be transferred (also using Matlab) to the place where its first

point should start at the coordinate for example (0, 0, 1). This way is avoided the additional processing of the additional data.

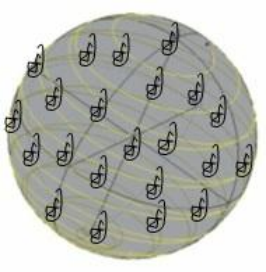


Figure 39. Distribution of the events

Note that after finding the so called perfect presentation on the Poincare sphere, still stays the important part of finding the most appropriate value for the three parameters listed above: size of the window, number of points taken after FT and the size of the step that is used for sliding the window. Results of the research are given in the next section.

4.5 Results

Figure 40 - Figure 42 show the success of recognition events in percents (%) as a function of the variation of the: size of the window (*N)*, number of the points taken after FT (N_f) and size of the step *(delta n)* respectively.

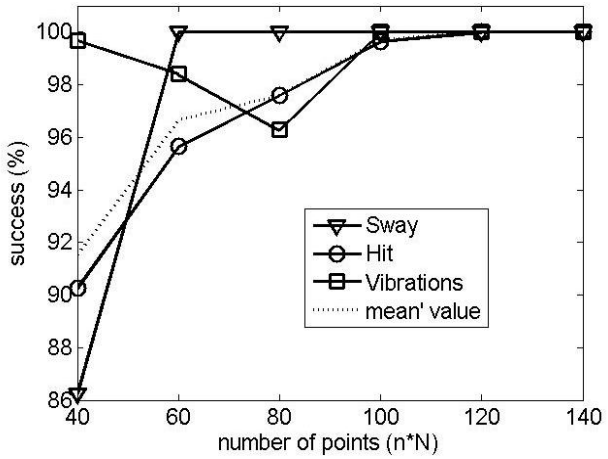


Figure 40. Variation of success of events recognition in percents (%) as a function of the variation of the size of the window (*N)*

As we can see in Figure 40 and Figure 41, when increasing the number of points (*N)* in the window and therefore increasing the acquisition time, Khiops is on average

more and more successful which means that it gives more and more precise decisions. Success is rising from around 92 % until 100 % in Figure 40.

In the Figure 40, vibration recognition success is 100 % for the smallest window. We explain that by the fact that vibration premise starts with a small peak which is obviously easily recognized by the classifier. When time window increases, the vibration pattern gets more complex and the classifier cannot so easily recognize its premises until the window gets large enough. So a small window would be suitable for this kind of event. However, as all types of events may occur (in our hypothesis), and the window size should also be set accordingly. Figure 40 also shows that 100 % recognition is achieved for almost 1 s (8 ms x 120 = 960 ms).

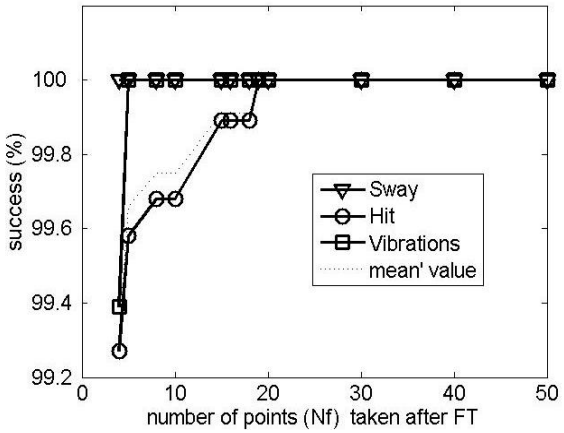


Figure 41. Variation of success of events recognition in percents (%) as a function of the variation of the number of points Nf taken after FT

Figure 41 represents recognition success as a function of the number of the points taken after Fourier transformation on a 960 ms window. Variation of the success is around 1 %. This small variation shows that this parameter has a low influence on the results. In the rest of the work we have thus fixed it to $N_f = 20$ points.

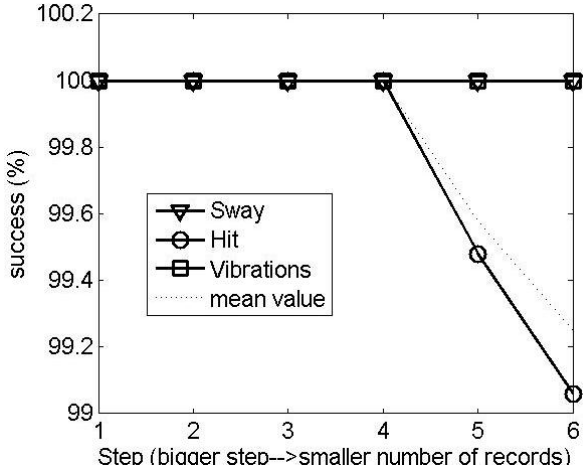


Figure 42. Variation of success of events recognition in percents (%) as a function of the variation of the size of the step delta_n

Figure 42 shows recognition success as a function of the size of the step between two consecutive windows. As we can see on the figure, a small step between two samples is enough to obtain a great success. But as we disposed a finite number of data, increasing the size of the step until a certain value results in decreasing the amount of sample windows, with the consequence that Khiops has not a sufficient amount of data to work. This explains the success decrease for steps greater than 4 for the hit samples, which has the less number of collected data overall.

5 Chapter
EVALUATION OF THE PROACTIVE REROUTING

5.1 Introduction

In this section we briefly describe a Markov state model to evaluate the availability of proactive protection/restoration on a single link. Because of their possibility to capture the probabilistic behavior of the system with attention to the design details, Markov models are being widely used for availability modeling. The system is composed of a single link and its backup path. We present all the states in which the system with proactive protection/restoration can be found and calculate its availability. Availability is defined as the probability of the system to be in the fully functioning state.

5.2 Analytical model

5.2.1 Defining the states of the system

The model has basically two types of states: functioning state (state S_0) and failures states: S_1, S_2 and S_3, shown in Figure 43. The notation used is given below:

S_0 state of the system when there is no detection of any risky event and there is no risky event.

→ outcome: nothing happening.

S_1 state of the system when there was a detection of risky event which never occurred in reality.

→ consequence: unnecessary rerouting (false alarm).

S_2 state of the system when there was a detection of risky event, proactive rerouting triggered on time.

→ result: less loss of the traffic.

S_3 state of the system when there was no detection of risky event although in

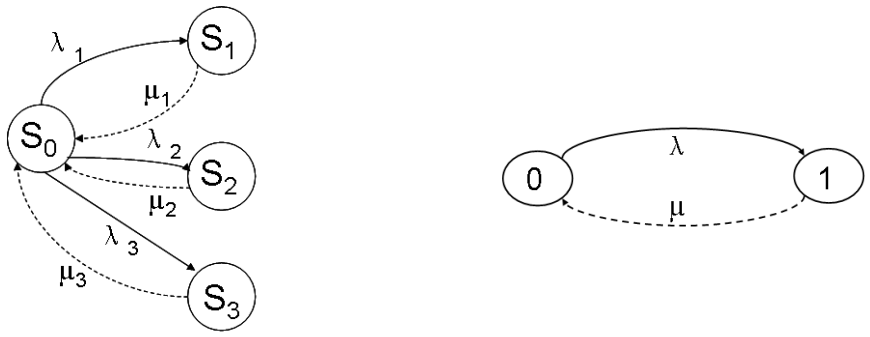
reality it occurred.

→ outcome: reactive rerouting was triggered.

P (S_i) is the probability of the system to be in the state S_i, with i=0, 1, 2, 3.

Failure rate: Failure rate λ specifies the rate of the transition from functioning state S_0 to failure states. Every failure state has its own failure rate: S_1 (λ_1), S_2 (λ_2), S_3 (λ_3).

Repair rate: Repair rate μ specifies the rate of the transition from one failure state to the functioning state. Every failure state has also its own repair rate: S_1 (μ_1), S_2 (μ_2), S_3 (μ_3). They are represented with dotted lines in the Figure 43a.



(a) (b)

Figure 43. Markov state model for the proactive (a) and reactive (b) system

We use frequency of the occurrences of the risky events in the nature (failure rate λ) and frequency of their reactive reparation (repair rate μ) as a reference to compare to frequencies of the occurrences and reparations of the events type E_1, E2 and E3 defined in Figure 44 (that lead to failure states S_1, S_2 and S_3 respectively).

	Proactive rerouting	No proactive rerouting
Fiber not cut	E1 λ_1, μ_1	E0 Nothing happens
Fiber gets cut	E2 λ_2, μ_2	E3 λ_3, μ_3

Figure 44. Definition of events type E0, E1, E2 and E3 related to the states S_0 to S_3 respectively

The following assumptions have been used in our proposed analytical model:

- All the states in which system can be found are: S_0, S_1, S_2 and S_3;
- The initial state of the system is the state S_0 (Figure 43a). That is the fully functioning state. From that state, system can go to any of the states: S_1, S_2 or S_3;
- Transitions between states have a Poisson distribution with λ_i and exponential service time with mean $1/\mu_i$;
- Our system for proactive rerouting is always active: classification of the events is performed non-stop and as soon as the premise of the risky event is identified, proactive rerouting is triggered;
- T_{tr} is defined as the time needed for total recovery. T_{sw} is defined as the time needed to switch to the alternate route with this definition, $T_{tr} = T_{sw} + \Sigma T$, in the reactive case where ΣT represents all other times involved in the recovery process (such as detection time, notification time and signaling time);
- Probabilities of occurrences of the events E0, E1, E2 and E3 in our model are mutually independent with exponential distribution.

Transitions T:

- $T(S_0 \rightarrow S_1)$ Transition from the state S_0 to the state S_1 occurs if during the process of the classification of the events, an error occurs and a risky event is detected (although the real danger of the fatal event never existed) and rerouting is triggered. In that case the needless extra rerouting is reducing the network capacity and introducing unnecessary traffic loss during the time $T_{tr} = T_{sw}$. This state S_1 is undesirable in the system but unavoidable in the real time functioning. Frequency of occurrence of the state S_1 is defined with the factor F with respect to the reference failure rate:

$$\lambda_1 = F \cdot \lambda \tag{15}$$

Repair rate is the reciprocal of the time in which the system will not work. In that case time needed to go back to previous configuration of the routing becomes T_{sw}.

$$\mu_1 = 1/T_{sw} \tag{16}$$

- $T(S_0 \rightarrow S_2)$ Transition from the state S_0 to the state S_2 occurs if during the process of the classification of the events, a risky event is detected long enough before it happens, which leaves enough time for proactive rerouting. When triggering proactive rerouting before the failure happens we are reducing the service disruption time and thus increasing the repair rate. This state of the system is highly desirable in the case of the further threats of risky events. Because we suppose that all real risky events results either in a proactive rerouting or in a reactive rerouting, failure rate of S_2 and S_3 both relate to the reference failure rate. This will be more discussed later in this dissertation. Frequency of the occurrence of the state S_2 is defined as:

$$\lambda_2 = R \cdot \lambda \text{, with R} \in [0, 1] \tag{17}$$

In the case of the state S_2 T_{tr} is in the interval between T_{sw} (for rerouting long before failure) and $T_{sw}+\Sigma T$ (for rerouting after the failure, reactive rerouting). Then:

$$\mu_2 = 1/\left(T_{sw} + \sum T'\right) \text{ with } \Sigma T' < \Sigma T \tag{18}$$

- $T(S_0 \rightarrow S_3)$ Transition from the state S_0 to the state S_3 occurs if during the process of the classification of the events, risky event was not detected, but in reality it occurred. In that case traditional reactive rerouting is triggered after the failure. Frequency of the occurring of the state S_3 is defined as:

$$\lambda_3 = (1 - R) \cdot \lambda \tag{19}$$

And since the rerouting is reactive, service disruption time is equal to $T_{tr} = T_{sw}+\Sigma T$, which means that repair rate is equal to μ.

$$\mu_3 = \mu \text{ with } \mu = 1/\left(T_{sw} + \sum T\right) \tag{20}$$

As mentioned before, factor R represents the ratio of risky events correctly identified before the failure occurs. If the proactive detection is good, the factor R will

be closer to the value 1. Because reparation time related to S_2 is smaller than the one of S_3, transition to state S_2 is more desirable. Therefore the objective of our work is to increase the value of the R. That is done by improving the representation of the data that we use as input values for Khiops or by enabling the machine to learn from its mistakes.

5.2.2 Deriving equations of the Markov state model

In the following we present the equations that describe the Markov state model from Figure 43a, taking into consideration the values of the variables λ_1, λ_2, λ_3 and μ_1, μ_2, μ_3.

$$dP_0(t)/dt = (-\lambda_1 - \lambda_2 - \lambda_3)\cdot P_0(t) + \mu_1 \cdot P_1(t) + \mu_2 \cdot P_2(t) + \mu_3 \cdot P_3(t) \tag{21}$$

$$dP_i(t)/dt = -\mu_i \cdot P_i(t) + \lambda_i \cdot P_0(t), \quad i = 1,2,3. \tag{22}$$

$$\text{and } \sum_{i=0..3} P_i(t) = 1 \tag{23}$$

We are interested of the system when it gets to the equilibrium state $(t \to \inf)$. Then we can say that:

$$dP_i(t)/dt = 0; \quad i = 0,1,2,3 \tag{24}$$

and (21) becomes:

$$P_i = \lambda_i / \mu_i \cdot P_0; \quad i = 1,2,3. \tag{25}$$

Equations (25) and (23) can be used to express the probability of the system to be in the state S_0:

$$P_0 = 1/(1 + \lambda_1/\mu_1 + \lambda_2/\mu_2 + \lambda_3/\mu_3) \tag{26}$$

Similar equations can be derived for the system with reactive rerouting of Figure 43b. Markov state model for the network with reactive rerouting has only two states: working state (state "0") and failure state (state"1"). The probability for the system to be in the working state (that is availability) can thus be expressed as:

$$P_0 = \mu/(\lambda + \mu) \tag{27}$$

Replacing the expressions of λ_1, λ_2, λ_3, μ_1, μ_2, and μ_3 of (15) to (20) in (26), we obtain the conditions on F, R, ΣT' and ΣT for which availability of the proactive solution improves the availability comparing to the reactive solution (with the condition that $\lambda>0$):

$$(26) > (27) \Leftrightarrow \sum T' < \frac{1}{R} \cdot \left(R \cdot \sum T - F \cdot T_{sw}\right) \tag{28}$$

We note that the condition (28) is independent from λ. Equation (28) also shows that for very small values of R, the proactive solution can not improve system availability, as (28) may only be satisfied for negative ΣT' values, which is impossible by definition. Identically, high values of F (false alarms) brings to the similar conclusion, that the right side of the equation becomes negative and then condition for $\Sigma T' \geq 0$ can not be met. Knowing these conditions, working on the representation of the data and enabling the machine to learn from its mistakes represents the way to bring the parameter R as closest as possible to the value one, and parameter F closes to the value zero and therefore reduce the downtime of service (unavailability time).

5.2.3 Summary

In this section, we presented a new method of proactive restoration in the optical link. Unlike reactive restoration that is triggered after the failure, proactive restoration is triggered before. We introduced one method of classification of the events based on the early premises detection of the risky events. This method is successfully validated with an experimental set up in the case of non destructive events with different types of representation of the SOP time variations. The possibility to distinguish between different events potentially risky is not limited only to Stokes parameters but can be extended to others parameters sensitive to variations in the fiber's environment. This opens an interesting subject for future work in the field of proactive detection.

An analytical model has also been developed for proactive protection/restoration. We demonstrated that under conditions defined with equation (28), the availability of

the system using the proactive rerouting is improved compare to the system where only the reactive one's is used.

5.3 Simulations

Simulations are made to validate the analytical model described in previous section. We were guided by the fact that simulating a part of the network and all possible states in which it can be found would give us the complete picture of the availability changes due to the introduced new option of proactive fault detection and rerouting.

All simulations are performed using the high-performance simulation tool OMNEST/OMNET. Interested reader can find more details about its features in [91].

Figure 45 presents a bidirectional link that connects node N_1 and node N_2. This link consists of four generators: g_0, g_1, g_2 and g_3. These generators are used for simulating four link states: S_0, S_1, S_2 and S_3 (that correspond to events: E0, E1, E2 and E3, respectively). This is done by creating and forwarding the corresponding type of the massage in both directions (toward the node N_1 and the node N_2).

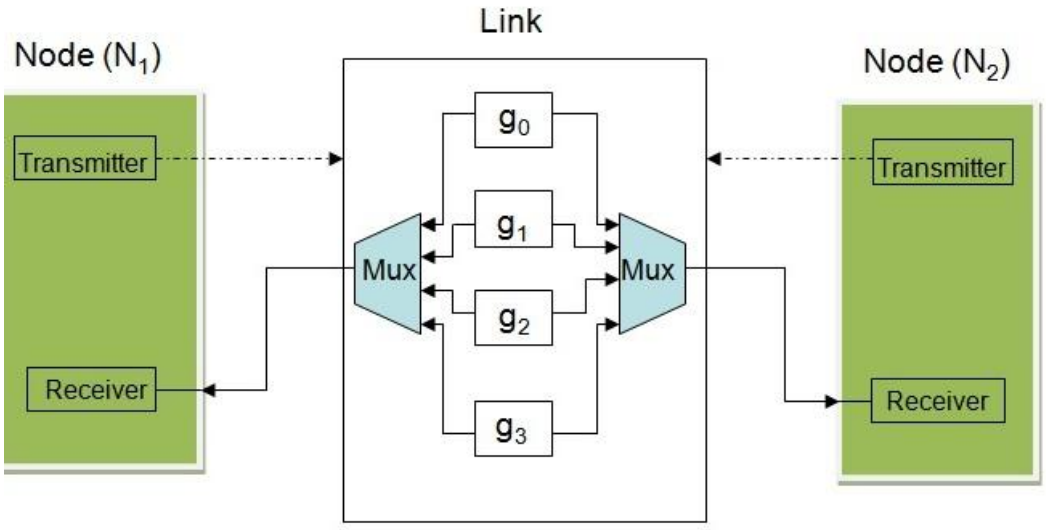


Figure 45. Simulation model of a bidirectional Link

These messages are being sent from generators first to multiplexers (Mux) and then forwarded to the nodes. Note that: passing through Mux do not change a thing from the message point of view. When a message is received by a node, depending from which generator it originates it increases the value of the timer T_{tot} (that presents the total unavailability time), for the appropriate value. These appropriate values are given with:

- Generator g_1 creates the message and schedules it using the exponential function with the parameter λ_1. Once received, the message increases the total unavailability time T_{tot}, for the value $t_1 = T_{sw}$;
- Generator g_2 creates the message and schedules it using the exponential function with the parameter λ_2. Once received, the message increases the total unavailability time T_{tot}, for the value $t_2 = T_{sw} + \sum T'$;
- Generator g_3 creates the message and schedules it using the exponential function with the parameter λ_3. Once received, the message increases the total unavailability time T_{tot}, for the value $t_3 = T_{sw} + \sum T$.

Hence the definition of the total unavailability time T_{tot}:

$$T_{tot} = t_1 + t_2 + t_3 \tag{29}$$

Also definition of the unavailability of the system:

$$U = {}^{T_{tot}}/_{SimTime} \tag{30}$$

Here, we define a term "system" as the bidirectional link including end nodes and a term SimTime as a total duration of the simulation.

Generator g_0 was not used because it represents state of the system S_0 when nothing is happening. Note that the values T_{sw}, T' and T are already explained/described in the previous section.

In the next section we show the simulation results. First, we present results obtained for reactive rerouting: comparing the result obtained using the analytical model/formula to the result obtained using the simulation tool. Secondly, we present results obtained for proactive rerouting, also comparing the result obtained using the analytical model/formula (but this time of the proactive model) to the result obtained using the simulation tool. And finally we compare these results.

5.3.1 Simulation of the reactive rerouting

In addition to above listed parameters: t_1, t_2, t_3 and T_{tot}, we shall adopt the following parameter values and later on we will justify their values.

$\lambda = 0.0000115740\ s^{-1}$;

R = 0.500; value without the unit.

F = 0.05; value without the unit.

$t_1 = 0$ s;

$t_2 = 4$ s;

$t_3 = 4$ s;

We consider that in the network there are 365 cable cuts per year, meaning that one cable cut occurs every 86 400 s. Thence the value of the parameter λ ($1/86\ 400\ s^{-1}$).

For the correct work of the simulator we had to assign the value of 0.05 to the parameter F, which in general defines the number of the generated false alarms in the system (in our case 5 %). In this simulation parameter F is directly responsible for creating messages by the generator g_1. These messages, despite of their existence, will never change the system's total unavailability time (T_{tot}), because the unavailability time that they produce is given by the parameter t_1=0 s. This way when simulating the reactive rerouting, false alarms are not taken into account.

With the value of 0.500, parameter R is directly responsible for creating 50 % of the messages within the generator g_2 and 50 % of the messages within the generator g_3. As values defining the unavailability time created by both types of messages are same ($t_2 = t_3 = 4$ s), it means that there is no influence of the proactive rerouting.

In the Figure 46 results concerning the reactive rerouting, obtained by simulations are presented with the blue line and results obtained by the analytical model are presented with the red line. It can be seen that results obtained by the simulation are with time approaching to results obtained by the analytical model.

In the Figure 46, we have plotted each point obtained with the simulation with its standard deviation. Standard deviation is a widely used measure of variability in statistics and it shows how much variation exists from the mean or expected value. High standard deviation indicated that the data points are spread all out over a large range of values and likewise, a low standard deviation indicates that the data points tend to be very close to the mean or expected value.

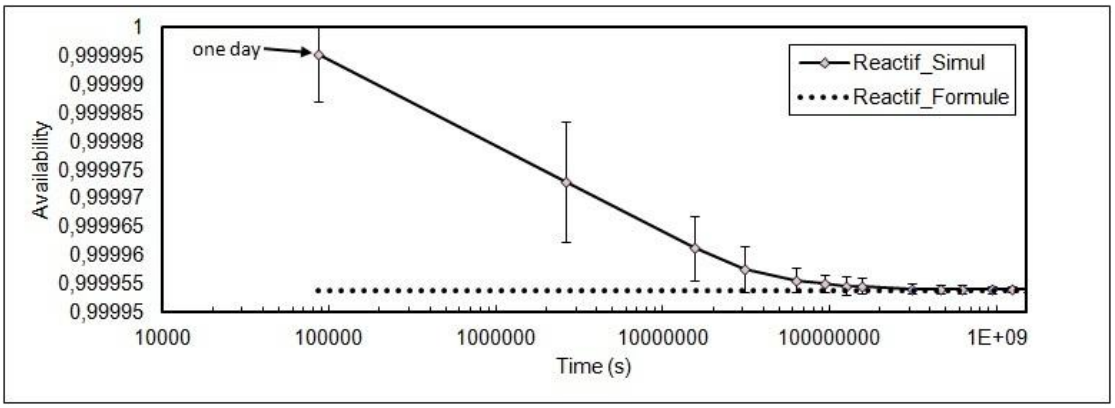


Figure 46. Reactive rerouting (simulation vs. analytical model)

Every point plotted in the Figure 46 is the mean value of 20 different values obtained by using 20 different seeds for the generation of random numbers of each generator. This ensures that generators are independent. For more detail about the used method can be found in [92].

5.3.2 Simulations of the proactive rerouting

When simulating proactive rerouting, parameters that define all three types of events, such as R, F, t_1, t_2 and t_3 are of essential importance. They determine whether and how much the proactive rerouting can improve the rerouting process. Therefore, firstly we present how the system's availability changes according to the changes of the parameter R (parameter that represents the recognition success). And after, we present the result obtained using the analytical model/formula compared to the result obtained using the simulation tool.

In order to determine the impact of the recognition success to the systems availability we let the parameter R takes values (0.5, 0.6, 0.7, 0.8, 0.9, 0.95, 0.97, and 0.99). Also, values used for other parameters are given below:

F= 0.05; value without the unit.

t_1 = 0.02 s;

t_2 = 2 s;

t_3 = 4 s;

These values assume the appearance of the false alarms in 5 % of all the cases (F= 0.05) resulting with the 20 ms of the unavailability (t_1 = 0.02 s) every time when they occur. This time is the time approximately needed for a switch to physically switch signal from one wavelength to another wavelength.

As we are using the proactive rerouting, we assume that our system is able to detect premises of the risky event 2 s before it really occurs and this way, for the system that needs 4 s for the total recovery after the failure (t_3 = 4 s), unavailability time of the system using the proactive rerouting would be only (t_2 = 2 s).

Figure 47 represents the change of the system's availability (that is using the proactive rerouting), depending on the change of the success of the recognition of events (R).

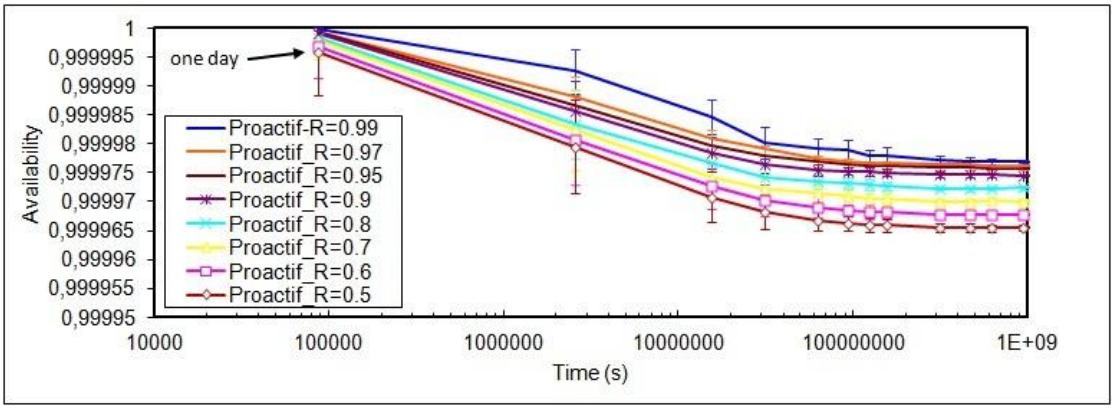


Figure 47. Proactive rerouting (simulations)

When we compare results obtained by the simulation (while parameter R= 0.5 and R= 0.6) with results given by the analytical model that we developed for the proactive rerouting (Figure 48), we can notice that, like in the case of reactive recovery, results obtained by the simulation are with time approaching to results obtained by the analytical model but in this case values of the system's availability are higher compared to the ones without proactive possibility.

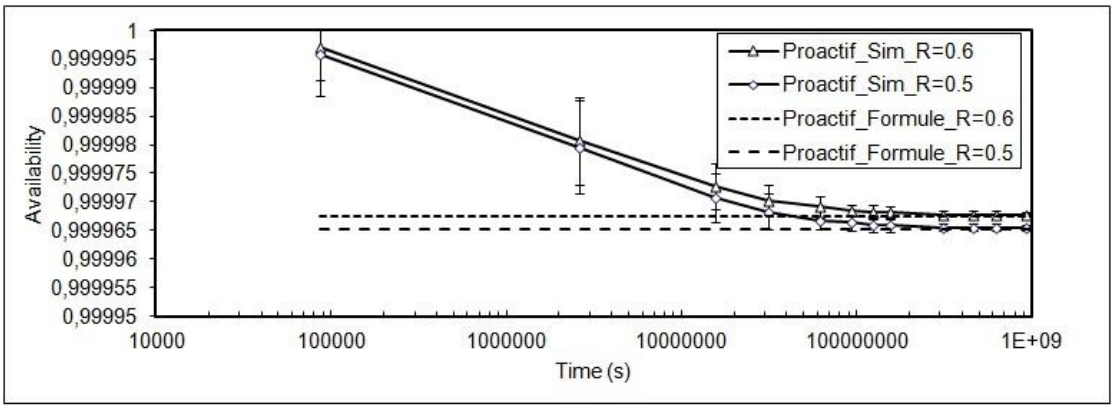


Figure 48. Reactive rerouting (simulation vs. analytical model)

5.4 Application to network recovery

In previous sections we described the usual recovery mechanisms that deal with network failures: protection and restoration. The protection mechanism activates in advance backup resource that will be used in case of failure, while the restoration mechanism takes over backup resource upon a failure; that is why protection mechanisms can recover quickly but are more demanding in terms of resource. Restoration mechanisms are less demanding when it comes to resource and therefore may be less costly than protection mechanisms in term of initial investments, but they generate longer service disruption.

In this chapter we present phases of which consist protection and restoration mechanisms. Also we consider multi-layer recovery in one case study and we compare the results obtained using the recovery done by different layers.

5.4.1 Multy-layer recovery

Both protection and restoration rely on 2 phases: *fault detection* and *recovery process*. Detection phase (Td) is the time needed for a certain layer of interest to detect a failure while recovery phase (Tr) is the time needed for a network to go back to fully functioning state counting from the moment of the detection of the failure (Figure 49).

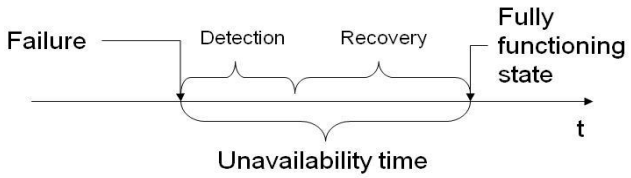


Figure 49. Reactive recovery scheme

Detection and recovery can be done at the physical WDM layer using a dedicated control plane, in an electrical circuit layer like SDH, SONET or OTN, or it can be done at the IP layer. These multiple layers work independently by default, which can be a drawback when handling network failures. Recovery methods can be easily duplicated in different layers, which results in allocating recovery bandwidth at each of the layers and might even raise the instability of the network. This approach is sometimes referred to as parallel or uncoordinated approach, as in [93]. The main advantage is that this approach is simple from an implementation and operational point of view because it requires no communication or coordination between layers.

A solution to improve the reliability of the network (and reduce the unavailability time) then consists in having some coordination between the recovery mechanisms in the different layers. A straightforward way is to ensure that the recovery in a lower layer happens quickly enough so that the higher layer does not even know that a

failure occurred. This solution may apply for the TDM network carrying IP traffic. As the typical IP layer can take up to several seconds to detect the failure, it is totally feasible for the TDM layer to have completed its restoration so that the IP layer does not detect the failure. The amount of data lost during the TDM recovery process is reduced compared to a pure IP reaction but still non negligible. To increase the stability of the multilayer interaction, another way is to add a priority mechanism where one layer attempts to restore the service first and the second layer only afterwards. This priority can be done implementing an additional hold-off timer in the higher layer, which would provide sufficient time for lower layer to do its restoration [93]. Nevertheless, a large hold-off time would increase the unavailability time. Another way could be done using a recovery token signal between layers [93]. In this case from the moment that one layer knows that it cannot restore traffic anymore it sends an explicit signal to the other layer to take over the restoration process.

In the following section we present the fault detection phase and the fault notification part of the recovery process for the particular case of IP and WDM layers. We have chosen to discuss first in details the application to the optical layer alone (WDM). Then, since nowadays the majority of traffic over a typical core WDM network is IP without intermediate switched layer (e.g. OTN), we have focused on IP networks carried over the WDM layer as a typical example for a multi-layer approach. However, the proposed approach remains applicable to any client network of the WDM layer (e.g. OTN).

5.4.2 Fault detection

An important feature of networks is the rapid detection of communication failures between adjacent nodes, in order to more quickly recover traffic. Depending on the type of mechanism used in the network, the time required to detect the failure can vary. It can be in the order of a few milliseconds when it can be detected at the physical layer, up to tens of seconds when a routing protocol Hello is employed [94]. Physical detection is the fastest way as it can be based on loss of light detection. When a routing protocol (such as IS-IS in IP and MPLS networks) is employed, detection highly depends on the two Hello timer settings: Hello-Interval timer is an emission rate of Hello messages and Dead-Interval define the number of lost Hello messages required to declare a link as "down" [94]. Commonly Dead-Interval is set to 3 times Hello-Intervals. Long timers increase the loss of traffic while short timer settings lead to network routing instability. Usual IGP timer values are usually set between 1 and 5 seconds in order to avoid instability problem. With these values of Hello-Interval timer, unavailability of the network due to the only failure detection process may be tens of seconds [94]. To reduce the unavailability time Bidirectional Forwarding Detection (BFD) was developed. BFD is a protocol that allows detecting faults in a bidirectional path between two forwarding engines in less than a second [95].

5.4.3 Fault notification

Once the traffic disruption is detected, the information must be known by the node in charge of triggering the recovery. In case of fiber failure, the node responsible of switching the traffic to the backup path may be the source node of a connection within a connection-oriented layer (e.g. WDM) or a higher layer node connected to the end of the failed link (e.g. a router). In most cases, the aforementioned node has no direct knowledge of the failure and cannot perform switching until it receives a failure notification message. Time needed for the source node to get notification about the failure depends on the communication delay between that source node and the failure detection point. All the data which is sent along the nominal path during that period of time will be lost.

Previous works have been focusing on the reduction of the durations of the latter phase but the time required for detection still remains the most impacting and challenging factor [96]. In this dissertation we propose to use proactive fault detection to reduce the detection time (as shown in Figure 50) and to use it in combination with the recovery phase done by different layers.

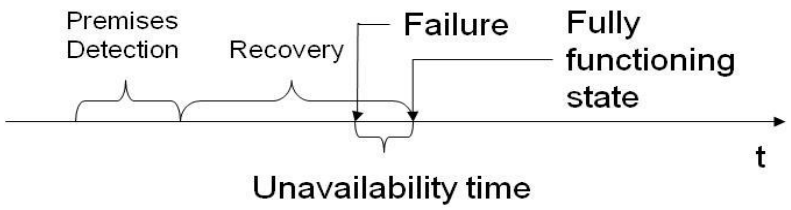


Figure 50. Proactive recovery scheme

In link-state protocol-based packet networks, proactive recovery could be realized by dynamically tuning the IGP link metrics in the way that flows will not use risky links anymore (the link graceful shutdown mechanism in the IGP would apply even better). This recovery can be accomplished with currently deployed protocols by modifying link metrics, without the need for standardization process. Information about the early fault detection on the physical/optical layer should be forwarded to the IP nodes in order to locally change the metric of the considered interface (increase the metric). Using the flooding capability of the IGP, information should be distributed to all nodes and therefore traffic deliberately driven away from risky paths. The advantage of this scheme is twofold: we benefit from the fact that early detection of the premises of the risky events is done on the physical layer long before it actually occurs and fast restoration is done on the IP layer using usual IGP rerouting.

5.5 Benefits from combining existing recovery schemes with the new proactive detection

In this section we present some possible combinations of recovery mechanisms. As every mechanism consists of two phases (detection and recovery phase) we analyze positive and negative sides of every phase and suggest how combined with the proactive fault detection we can reduce the unavailability time of the network. Some of the mechanisms have more negative sides than others but they deserve to be mentioned here.

5.5.1 Recovery using the IP layer

Nowadays, IP network survivability is achieved by conventional routing protocols that automatically reroute packets around a failure through routing table updates. As we mentioned before this method has a relatively long detection phase (based on the outage of the Hello messages) but fast restoration phase compared to the restoration phase which might be done on the WDM layer. As a result this is the scheme with the longest period of unavailability (as shown in Figure 51).

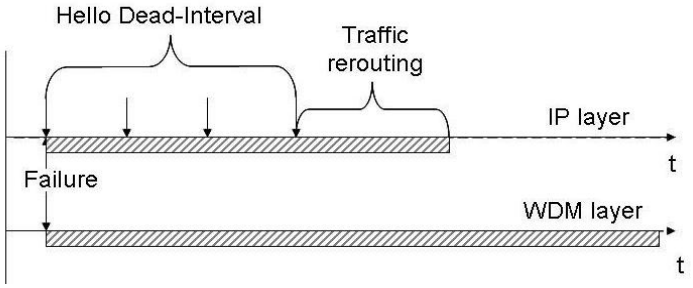


Figure 51. Recovery scheme using only IP layer

Some improvements in speed of the detection are made using BFD protocol and deploying the mechanism called MultiProtocol Label Switching Fast ReRoute (MPLS FRR) for the recovery phase.

5.5.2 Recovery using the WDM layer

Restoration on the WDM layer can be done thanks to ROADM (reconfigurable optical add-drop multiplexer) and automatic provisioning thanks to a control plane using the GMPLS protocol suite for example. This way we have fault detection almost immediately but restoration phase will be long using the WDM layer because of the switching speed and WDM line tuning, as shown in Figure 52.

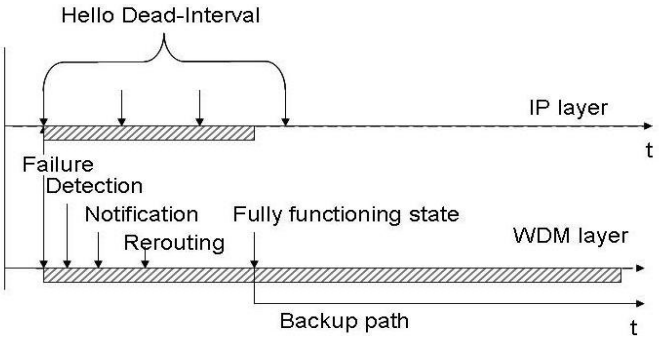


Figure 52. Recovery scheme using only WDM layer

If we take into account the possibility of recovery using multiple layers we can make a distinction between the following sub-cases.

5.5.3 Recovery using IP and WDM capabilities independently

In this case there is no correlation between layers and we risk triggering multiple recovery mechanisms, one at each of the layers involved, which is an inefficient way to recover and may introduce traffic flapping. This example exists only in theory. Because of its negative sides it has limited interest from an operational perspective. That brings us to the case where layers should communicate among them.

5.5.4 Recovery using IP and WDM capabilities dependently

5.5.4.1 Fault detection on the WDM layer and information forwarded to the IP layer

When receiving the information of fault detection (which can be achieved by immediately shutting down lasers on ports connecting WDM and IP nodes), the IP layer can trigger right away the recovery and reduce much more the unavailability time, as shown in Figure 53.

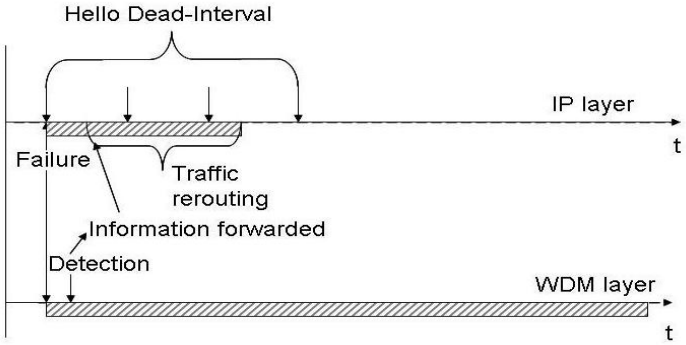


Figure 53. Recovery scheme using WDM layer for fault detection and IP layer for recovery

This simple method is not so simple to deploy in real networks because the router can not be sure that it will receive the information from the WDM layer. For example, both layers may be operated by two different service providers or the IP link may span several WDM segments which may not always propagate the fault information.

5.5.4.2 Proactive fault detection on the WDM layer and information forwarded to the IP layer

The method that we propose is to detect in advance the fault using the WDM layer (proactive fault detection) and to forward that information to the IP layer so that it can trigger immediately the IGP convergence. That way, most of the time during which the network is normally down (during the detection and recovery phases) is suppressed because the re-routing is done before the real fault occurs, that is while there is still undisturbed traffic in the network. This way we obtain the smallest unavailability time as possible, as shown in Figure 54. The benefits can even be twofold if we combine detection in advance and Fast Reroute (using MPLS or IP).

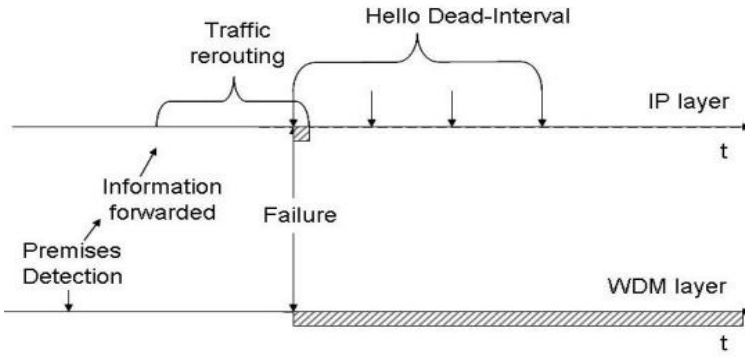


Figure 54. Recovery scheme using WDM layer for proactive fault detection and IP layer for recovery

Tight cooperation between the WDM layer and the IP layer can even improve these schemes. For example, using proactive detection on the WDM layer, information for the need to recover is forwarded to the higher layer, but if, for some reason, backup resource is no longer usable (in case of a double failure for example), it might be possible to notify the WDM layer to provision new resource. The time saved thanks to proactive detection may greatly reduce the unavailability time caused by this process.

5.5.5 False alarms

Proactive detection can also produce false alarms as well as missed alarms. False alarms correspond to the false identification of an event as a risky one, although it

does not cause a real fault, while missed alarms correspond to real risky events that cause faults and that were not predicted.

If the recovery was done on the WDM layer, false alarms would increase the unavailability time compared to the reactive detection, because they trigger recovery uselessly. Missed alarms would not modify the unavailability time because the failure would eventually be detected by reactive methods. On the other hand, recovery by IP layer improves this, because the false alarms would cause useless rerouting without strong impact on network availability (even though, depending on network dimensioning, it might create some congestion or reduce service bandwidth if no classes of service are used).

5.6 A quantitative comparison of recovery approaches

In the previous section, we have shown how the unavailability time changes depending on the type of the recovery scheme we are using. These time values for two phases (detection and recovery), for the different types of the recovery methods, WDM recovery (λ) and IP recovery (router) are presented in the Table 4.

For example, in the case of the fault detection on the physical WDM layer, detection phase is almost immediate (0 second) and, for the recovery phase, using the same layer takes around 200 seconds. Note that according to the size of the network and used equipment, time values may vary. We will use the values from the table for further analytical availability analysis in order to compare three different recovery schemes: the first done using the WDM layer, the second using the IP layer and the third recovery scheme using the proactive detection on WDM layer with IP rerouting. Proposed analysis was done using the Markov state models that are widely used for the availability analysis of systems.

Table 4. Unavailability time

T(s)	**Two Phases**		
	Detection phase		***Recovery phase***
λ	***0***		***200***
Router	***IGP: 3-5***	***LOS:*** 0	***IGP:*** 3-5

The following notations have been used in our proposed analytical model:

- μ_1 is the repair rate in the case of the WDM recovery (MTTR=200 s)
- μ_2 is the repair rate in the case of the IGP detection plus recovery (MTTR=6 s)

- μ_3 is the repair rate in the case of the proactive recovery (MTTR=1 s). We consider that decision for the rerouting was taken 2 seconds before an actual failure occurred. Note that recovery is done on IP layer (3 s), which leaves us with 1 second of unavailability time.

The first recovery scheme, WDM recovery without proactive detection has the smallest probability to be in the working state: 99.800 %. If we would like to see the benefits of the proactive detection coupled with WDM recovery, due to the longer recovery period of the mechanism, early fault detection should be in the order of a few hundreds of seconds before an actual failure occurs, which does not seem much reasonable. The second recovery scheme, based on usual IGP detection and rerouting has a probability of 99.993 %. And finally, proactive restoration with multi-layer coordination has the highest probability to be in the working state: 99.999 % (five nines): we can see that using the proactive detection can improve network availability but its interest depends on the reaction time of the involved recovery mechanism.

6 Chapter
CONCLUSION

The objective of this thesis was to study mechanisms associated to a preventive recovery of the optical core network. This dissertation outlines the different solutions and their evaluation from the point of view of the network telecommunications operator.

Existing recovery mechanisms make optical networks fault-tolerant. Fault tolerance refers to the ability of the network to reconfigure and reestablish communication upon a failure. Usual recovery mechanisms that deal with network failures can be divided into protection and restoration. The protection mechanism activates in advance backup resource that will be used in case of failure, while the restoration mechanism takes over backup resource upon a failure; that is why protection mechanisms can recover quickly but are more demanding in terms of resource. Restoration mechanisms are less demanding when it comes to resource and therefore may be less costly than protection mechanisms in term of initial investments, but they generate longer service disruption. This service disruption can present one of the most important impacts for the telecom operator in the form of the revenue loss and business disruptions.

In this context, we have studied methods that could provide preventive recovery of the optical core network and therefore reduce the potential service disruption and the revenue loss.

For that purpose, the first phase of our study was to indentify all the potential sources of the network failures, provoking service disruptions and their recurrences. Depending on the environment fiber is exposed to various risk factors. For example, terrestrial cables are frequently exposed to mechanical engines (wayward backhoes) that can cut fiber by accident or rodents that eat up cable coatings. Aerial cables are often exposed to mechanical engines for tree cutting or alike. Besides these external causes, failures may also occur due to human mistakes and other equipment failures, but the most frequent ones are caused by dig-ups, representing almost 60 percent of the all the failures in France Telecom cable infrastructure. Finding a method that would be able to proactively detect potential fiber cut in the backbone optical network caused by construction work i.e. digs-ups was the main objective of this work.

Once we have created the complete vision of the basic building blocks of the optical network, used technologies and the most frequent reason for network failures, we were able to search for a method that could provide proactive recovery.

The concept of proactive recovery can be decomposed to three parts (segments): a part of preventive risky event detection, a part of risky event recognition/classification and a part of a very act of recovery.

For the purpose of the preventive risky event detection we explored the area of using fiber as a sensor. We have demonstrated the possibility of detecting the changes in the fiber's environment directly by following the changes of the state of polarization (SOP) of the light-Stokes parameters. We have shown that these changes of the state of polarization are easily distinguishable by the human eye. We propose in the second part (part of risky event recognition/classification) to exploit artificial intelligence tools to recognize events while they are going on and then to determine which strategy should be applied to minimize the impact of the eventual risky events. Using the classifier called Khiops 100 % recognition of the events is achieved for almost 1 s (8 ms x 120 = 960 ms). This result has never been shown until now, and this thesis is the first document that shows the possibility to detect and recognize in advance an eventually risky event.

Once a deeper understanding of the potential of this technique has been achieved with an experimental test bed, theoretical investigations through the development of analytical models are conducted to validate and generalize them. This thesis has presented for the first time, to the best of our knowledge, Markov state models for the proactive recovery. We presented the equation that represents the tradeoff between the value of the desired systems availability and the value of the required accuracy of the system for detection.

Through numerical simulations, we studied the model of an optical fiber exposed to fiber cuts with the possibility of proactive detection of the risky event. Results confirmed the previously obtained results from the analytical model.

In this dissertation we have shown different schemes for fast network recovery. We compared these schemes based on unavailability time.

Nowadays, recovery is done on one layer but we showed that combining capabilities from multiple layers we can reduce the unavailability time. We thus proposed a new recovery method using the proactive fault detection on the WDM layer and rerouting using the IP layer. Our method compared to other recovery schemes results in the smallest unavailability time.

Regarding the deployment of the proactive detection that we proposed, it requires systematic Stokes parameters monitoring that may increase the cost; nevertheless new generation of transmission equipment rely on coherent detection and therefore the

required parameters may be given without extra cost thanks to the electronic digital signal processing embedded inside.

Presented proactive recovery presents a good solution when the extreme availability is needed. This extreme availability can be hard requirement for certain services, for business customers, for example or for new services based on the virtualization of the computing resources in the network.

Bibliography

[1] ITU-T Recommendation G.971, "General features of optical fibre submarine" 2004.

[2] P. E. Green, "Optical networking update", *IEEE Journal on Selected Areas in Communications*, Vol. 14, No. 5, pp. 764 - 779, June 1996.

[3] M. Maier, "Optical switching networks", Cambridge University Press, 2008.

[4] S. V Kartalopoulos, "Introduction to DWDM technology", IEEE Press, Lucent technologies, 2000.

[5] K. H. Liu, "IP over WDM", Wiley, 2002.

[6] W. D. Grover, "Fiber cable failure impacts, survivability principles and measures of survivability", Prentice Hall Professional, 2004.

[7] W. D. Grover, "Mesh-Based Survivable Networks: Options and Strategies for Optical, MPLS, SONET and ATM Networking", Prentice Hall PTR, Upper Saddle River, 2004.

[8] D. Crawford, "Fiber optic cable dig-ups-causes and cures" Network Reliability: A Report to the Nation–Compendium of Technical Papers, National Engineering Consortium, Chicago, June 1993.

[9] W. D. Grover, "Mesh-Based Survivable Networks: Options and Strategies for Optical, MPLS, SONET and ATM Networking", Prentice Hall PTR, Upper Saddle River, 2004.

[10] http://www.infinera.com/products/ILS2.html.

[11] R. Ramaswami, K. N. Sivarajan, G. H. Sasaki, "Optical networks", Elsevier, 2010.

[12] S. Ramamurthy, L. Sahasrabuddhe, and B. Mukherjee, "Survivable WDM Mesh Networks", *Jurnal of Lightwave Technology*, 2003.

[13] S. K. Lumetta and S. Stevan, "Restoration of All-Optical Mesh networks With Path-Based Flooding", *Jurnal of Lightwave Technology,* Vol. 21, No. 11, November 2003.

[14] D. Colle, S. De Maesschalck, et al."Data-centric optical networks and their survivability", *IEEE Journal on Selected Areas in Communications*, Vol. 20, pp.6-20, January 2002.

[15] P. Demeester, et al. "Resilience in multilayer networks", *IEEE Communications Magazine*, Vol. 37, No. 8, Aug 1999.

[16] S. D. Maesschalck, et al. “Pan-European Optical Transport Networks: An Availability-based Comparison”, *Photonic Network Communications* Vol. 5, No. 3, 2003.

[17] ITU-T Recommendation G.872, **“**Architecture for optical transport networks”, November 2001.

[18] P. Tomsu, C. Schmutzer, “Next generation optical networks”, Upper Saddle River, Prentice Hall, 2002.

[19] H. C. Cankaya, V. S. S. Nair, “Reliability and availability evaluation of self-healing SONET mesh networks”, IEEE Global Telecommunications Conference, GLOBECOM 1997.

[20] G. Kohn, “The IEEE Standard Dictionary of Electrical and Electronic Terms”, New York : 6th ed., 1996.

[21] R. Lin, S. Wang, L. Li, and L. Guo, “A New Network Availability Algorithm for WDM Optical Networks”, CIT 2005.

[22] M. Clouqueur, W. D. Grover “Availability analysis of span-restorable mesh networks”, *IEEE Journal on Selected Areas in Communications Special Issue on recent advances in fundamentals of network management*, 2002.

[23] http://pdffinder.net/MTTF-Versus-MTBF.html#

[24] D. Harms, M. Kraetzl, C. J. Colbourn, and J. S. Devitt, “*Network reliability”,* Boca Raton, FL : CRC Press, 223p, 1995.

[25] I. Gerbakh, “Reliability theory: with applications to preventive maintenance”, Berlin, Germany, Springer-Verlag, 2000.

[26] Y. Huang, C. Kintala, N. Kolettis and N. D. Fulton, “Software rejuvenation: Analysis, module and applications”, AT&T Bell Labs, Murray Hill, NJ 1995.

[27] O. Babaoglu et al. *“*Self-star Properties in Complex Information Systems”, Springer, 2005.

[28] R. S. Swarz, D.P Siewiorek, “Reliable computer systems”, Wellesley, 1998.

[29] C. R. Menyuk, J. Zweck, “Detection and Mitigation of Soft Failure due to Polarization-Mode Dispersion in Optical Networks”, OFC. 2006.

[30] C. Mas and P. Thiran, “An Efficient Algorithm for Locating Soft and Hard Failures in WDM Networks”, *IEEE Journal on Selected Areas in Communication*, Vol. 18, No. 10, October 2000.

[31] S. Zhang, C. Zhang, Q. Yang, *“*Data preparation for data mining”, Applied Artificial Intelligence, Vol. 17, 2003.

[32] Q. Yang, T. I. Li , K. Wang, *“*Web-log Cleaning for Constructing Sequential Classifiers”, Applied Artificial Intelligence, Vol. 15, 2003.

[33] S. Zhang, C. Zhang, Q. Yang, **"**Data preparation for data mining*"*, Applified Artificial Intelligence, 2003.

[34] R. Johnson, and G. Bhattacharyya, "Statistics: Principles and Methods", John Wiley& Sons Publisher, 1985.

[35] A. K. Jain, M. N. Murty and P. J. Flynn, "Data Clustering: A Review", *Jurnal ACM Computing Surveys*, Vol. 31, September 1999.

[36] F. Salfner, M. Malek, "Reliability Modeling of Proactive Fault Handling", Research Report number 209, Department of Computer Science, Humboldt University Berlin, 2006.

[37] C. J. Van Rijsbergen, "Information Retrieval", London, Butter-worth, second edition, 1979.

[38] F. Salfner, M. Malek, "Using Hidden Semi-Markov Models for effective online failure prediction", Proceedings on 26th IEEE Intl. Symposium on Reliable Distributed Systems , SRDS 2007.

[39] A. Csenki, "Bayes predictive analysis of a fundamental software reliability model", *IEEE Transactions on reliability*, 1990.

[40] J. D. Pfefferman, B. Cernuschi-Frias, "A nonparametric nonstationary procedure for failure prediction", *IEEE Transaction on reliability*, Vol. 51, December 2002.

[41] A. Andrzejak, L. Silva, "Deterministic models of software aging and optimal rejuvenation schedules", *10th IEEE/IFIP international Symposium on Integrated Network management*, 2007.

[42] T. Troudet, W. Merrill, N. Center and O. Cleveland, "A real time neural net estimator of fatigue life", *IEEE international Joint Conference on Neural networks*, 1990.

[43] S. W. Neville, "Approaches for early fault detection in large scale engineering plants", *PhD thesis, University of Victoria*, 1998.

[44] S. B. Kotsiantis, "Supervised Machine Learning: A Review of Classification Techniques", *Informatica*, 2007.

[45] Z. Zheng, "Constructing X-of-N Attributesd for decision tree learning", *Machine learning*, 2000.

[46] J. R. Quinlan, "C4.5: Programs for Machine Learning", *Machine Learning*, Morgan Kaufmann Publishers, 1993.

[47] K. B. Korb and A. E. Nicholson, "Bayesian artificial intelligence", Chapman & Hall/CRC, 2004.

[48] N. Friedman, D. Geiger, and M. Goldszmidt, "Bayesian Network Classifiers", *Machine Learning*, Kluwer Academic Publishers, 1997.

[49] N. Friedman, D. Geiger, and M. Goldszmidt, "Bayesian Network Classifiers", *Machine Learning*, Kluwer Academic Publishers, 1997.

[50] M. Boulle, “Khiops: A statisical discretization method”, *Machine learning*, Kluwer academic publishers, 2004.

[51] M. Boulle, “Optimum simultaneous discretization with data grid models in supervised classification: a Bayesian model selection approach”, *Advances in Data Analysis and Classification*, Springer, 2009.

[52] M. Boulle, “A parameter-free classification method for large scale learning”, *Journal of machine learning research*, Vol. 10, 2009.

[53] V. N. Vapnik, “The nature of statistical learning theory”, Springer, 1995.

[54] M. Klemettinen, H. Mannila, H. Toivonen, “Interactive exploration of interesting findings in the Telecommunication Network Alarm Sequence Analyzer TASA”, *Information and software technology*, 1999.

[55] R. Vilalta, and S. Ma, “Predicting rare events in temporal domains”, *IEEE International conference on Data mining*, ICDM2002.

[56] T. Y. Lin, D. P. Siewiorek, “Error Log Analysis: Statistical Modeling and Heuristic Trend Analysis”, *IEEE Transactions on Reliability*, Vol. 39, 1990.

[57] A. W. Domanski, “Application of optical fiber sensors in mechanical measurements”, *Instrumentation and Measurement Technology Conference, IMTC/97, 1997.*

[58] K. Thyagarajan and A. K. Ghatak, “Fiber optic essentials”, A John Wiley & sons, 2007.

[59] E. Udd, W. B. Spillman, “Fiber optic sensors - An introduction for engineers and scientist”, John Wiley & Sons, Inc, 2011.

[60] F. T. S. Yu and S. Yin, “Fiber optic sensors (Optical Science and Engineering)”, New York, Basel Marcel Dekker, Inc, 2002.

[61] S. Yin, P. B. Ruffin, F. T. S. Yu, “Fiber optic sensors”, Second edition, CRC Press, 2008.

[62] D. A. Krohn, “Fiber optic sensors”, ISA, 2000.

[63] K. Thyagarajan and A. K. Ghatak, “Fiber optic essentials”, New Jersey : John Wiley & Sons, Inc, 2007.

[64] E. Udd, “Fiber optic smart structures”, Wiley, 1995.

[65] A. Kerrouche et al, ”Strain measurement on a rail bridge loaded to gailure using fiber bragg grating-based distributed sensor system”, *IEEE Sensors jurnal*, Vol. 8, No. 12, 2008.

[66] A.D. Kersey, et al. “Fiber grating sensors”, *Journal of Lightwave Technology*, Vol. 15, No. 8, pp. 1442-1463, Aug 1997.

[67] S. E. Watkins, **“**Smart bridges with fiber-optic sensors”, *IEEE Instrumentation & Measurement magazine*, June 2003.

[68] S. E. Watkins, J. F. Unser, A. Nanni, K. Chandrashekhara, and A. Belarbi, "Instrumentation and manufacture of a smart composite bridge for short-span applications", Annual International Symposium on Smart Structures and Materials: Smart Systems for Bridges, Structures, and Highways, March 2001.

[69] http://www.optasense.com/media/Documents/Pipeline_Security_and_Monitoring.pdf

[70] Y. You, "Using submarine communications networks to minitor the climate", ITU-T Technology Watch Report, November 2010.

[71] P. M. Krummrich and K. Kotten, "Extremely fast (microsecond timescale) polarization changes in high speed long haul WDM transmission systems", Optical Fiber Communication Conference, OFC 2004.

[72] F. Heismann, D. A. Fishman, D. L. Wilson, "Automatic compensation of first-order polarization mode dispersion in a 10 Gb/s transmision system", ECOC, 1998.

[73] Z. Zhang, X. Bao, Q. Yu, and L. Chen, **"**Fast State of Polarization and PMD Drift in Submarine Fibers", *IEEE Photonics Technology Letters*, Vol. 18, No. 9, 2006.

[74] M. Karlsson, J. Brentel, and P. Andrekson, "Long-term measurement of PMD and polarization drift in installed fibers", *Journal of Lightwave Technology* 2000.

[75] C. Allen, P. Kondamuri, D. Richards, and D. Hague, "Measured temtemporal and spectral PMD characteristics and their implications for network level mitigation approaches", *Journal of Lightwave Technology,* Vol. 21, No. 1, 2003.

[76] D. Waddy, P. Lu, L. Chen, and X. Bao, "Fast state of polarization changes in aerial fiber under different climatic conditions", *IEEE Photonics Technology Letters*, Vol. 13, No. 9, 2001.

[77] J. Wuttke, P. Krummrich, and J. Rosch, "Polarization oscillations in aerial fiber caused by wind and power-line current", *IEEE Photonics Technology Letters,* Vol. 15, No. 6, 2003.

[78] S. Salaun, F. Neddam, J. Poirrier, B. Raguenes and M. Moignard, "Fast SOP Variation Measurement on WDM Systems", ECOC 2009.

[79] D. Waddy, P. Lu, L. Chen, and X. Bao, "Fast state of polarization changes in aerial fiber under different climatic conditions", *IEEE Photonics Technology Letters*, Vol. 13, No. 9, 2001.

[80] N. Brochier, J. L Barbey, "Field measurement of polarization fluctuation dynamics and related impact for 40 Gbit/s submarine systems", SubOptic2010.

[81] P. M. Krummrich and K. Kotten, "Extremely fast (microsecond timescale) polarization changes in high speed long haul WDM transmission systems", Optical Fiber Communication Conference, OFC 2004.

[82] G. A. Topasna and D. M. Topasna, "Stokes parameters in undergraduate laboratory exercises", Department of physics and astronomy, Virginia Military Institute, Lexington, VA.

[83] B. Kanseri, S. Rath, and H. C. Kandpal, "Direct determination of the generalized Stokes parameters from the usual Stokes parameters", *Optics Letters*, Vol. 34, No. 6, pp. 719-721 (2009).

[84] O. Korotkova, E. Wolf, "Generalized Stokes parameters of random electromagnetic beams", *Optics Letters*, Vol. 30, No. 2, pp. 198-200 (2005).

[85] H. G. Berry, G. Gabrielse, and A. E. Livingston, "Measurement of the Stokes parameters of light", *Applied Optics*, Vol. 16, No. 12, pp. 3200-3205 (1977).

[86] G. G. Stokes, Mathematical and Physical Papers, Cambridge Univ. Press, Cambridge, Vol. 3, p. 233.

[87] D. Clarke, B. G. Steward, H. E. Schwarz, and A. Brooks, "The statistical begaviour of normalized Stokes parameters", *Astronomy and astrophysics*, 1983.

[88]http://www.cs.montana.edu/~harkin/courses/cs530/topics/1-overview/chapter.pdf.

[89] M. Boulle, "Khiops: A Statistical Discretization Method of Continuous Attributes", *Machine Learning, page 53-59.* Kluwer Academic Publishers, 2004.

[90] P. H. Winston, *"*Artificial intelligence", Addison-Wesley Longmore Publishing, 1992.

[91] http://www.omnest.com/features.php

[92] http://dcsl-uhcl.net/public/download/OMNET++.pdf (page 160).

[93] D. Colle, S. De Maesschalck, et al**.** "Data-centric optical networks and their survivability", *IEEE Journal on Selected Areas in Communications*, Vol. 20, No.1, pp.6-20, January 2002.

[94] M. Shand, S. Bryant, "IP fast reroute framework", Internet RFC 5714.

[95] D. Katz, D. Ward, "Bidirectional forwarding detection", Internet RFC 5880, June 2010.

[96] B. Vidalenc, L. CiaVaglia, "Proactive fault management based on risk-augmented routing", IEEE Globecom, 2010.

Annex
List of publications

- J. Pesic, E. Le Rouzic "Fault prediction and proactive restoration in optical network links using events recognition" BONE 2010 (Building the future Optical Network in Europe) master and summer school, Budapest, Hungary, September 6-10, 2010.
  http://www.tmit.bme.hu/bone-school

- J. Pesic, E. Le Rouzic, N. Brochier and L. Dupont "Proactive restoration of optical links based on the classification of events" ONDM 2011, February 8-10, 2011. **Best student paper award.**
  http://www.ondm2011.unibo.it/papers.php

- J. Pesic, J. Meuric, E. Le Rouzic "Proactive Restoration of Optical Links using GMPLS" iPOP 2011 (International Conference on IP+ Optical Network), Kawasaki, Japan, June 2-3, 2011.
  http://www.pilab.jp/ipop2011/about/index.html

- J. Pesic, J. Meuric, E. Le Rouzic, L. Dupont, M. Morvan "Proactive Failure Detection for WDM Carrying IP" INFOCOM 2012, Orlando, Florida, USA, March 25-30, 2012.
  http://www.ieee-infocom.org/

- Patent: "Method and device for determining the risk of severing an optical fibre", France Telecom January 2012: EP2403164 A1
  https://register.epo.org/espacenet/application?lng=fr&number=EP11170531&tab=main