

**BACKUP RADIO PLACEMENT
FOR OPTICAL FAULT TOLERANCE
IN HYBRID WIRELESS-OPTICAL
BROADBAND ACCESS NETWORKS**

TRUONG HUYNH NHAN

**NATIONAL UNIVERSITY OF SINGAPORE
DEPARTMENT OF ELECTRICAL & COMPUTER ENGINEERING**

2010

**Backup Radio Placement for Optical Fault Tolerance in
Hybrid Wireless-Optical Broadband Access Networks**

Submitted by TRUONG HUYNH NHAN

Department of Electrical & Computer Engineering

**In partial fulfillment of the
requirements for the Degree of
Master of Engineering
National University of Singapore**

Summary

Hybrid Wireless-Optical Broadband Access Networks (WOBANs) are a new and promising architecture for next generation broadband access technology. WOBAN gives us more advantages than a mere connection between wire-line optical and wireless networks: cost effective, more flexible, more robust and with a much higher capacity. These advantages can be substantial only if WOBAN has an efficient and stable operation, i.e., its fault-tolerance requirements are satisfied.

For providing fault-tolerance capability in WOBAN, two general approaches using different ideas for solving the same problem coexist. On one side, there are conventional multi-path routing algorithms which make use of different paths connecting two nodes in the Wireless Mesh Network front-end of WOBAN. While these methods are widely for providing alternative routing paths without requiring extra resource planning, they have severe limitation in terms of low backup bandwidth and high packet delay. On the other side, there are methods that introduce new resources into WOBAN to provide extra bandwidth for backup traffic and reduce the packet delay. These include methods such as putting extra radio at every node or laying new fiber to connect different ONUs (Optical Network Units). But they are associated with problems such as gateway bottleneck, high restoration time and huge deployment cost.

In this thesis, a new approach to handle optical fault-tolerance in WOBAN is proposed. In case of a fiber or optical network component failure, a backup path through wireless network is used in order to provide failure restoration guarantee. The key idea is to deploy back-up radios at a subset of nodes among existing nodes in the Wireless Mesh Network front end of WOBAN and assign for them a

different frequency from primary traffic's channel. Each ONU is wirelessly connected to another ONU in a multi-hop way, hence fully protected. Determining a subset of nodes for backup radio placement so that the deployment cost is minimized is not trivial. This thesis addresses the problem to guarantee full protection against single link failures for optical part of WOBAN while minimizing the number of extra backup radios in order to save cost. We prove that this problem is NP-Complete (Non-Polynomial) and develop an integer linear programming to obtain the optimal solution. We also develop two heuristics to reduce computation complexity: Most-Traversed-Node-First (MTNF) and Closest-Gateway-First (CGF). To evaluate our heuristic algorithms, we run simulation on real and random networks. The simulation results show that our approach gives a more feasible and cost-effective way to provide optical fault-tolerance compared to other existing solutions.

Acknowledgements

I wish to thank my supervisor, Prof Mohan Gurusamy for his continuous guidance, support and encouragement during my research and study at NUS. Thank you for giving me the liberty to chalk out my own research path, all the while guiding me with your invaluable suggestions and insightful questions.

I would also like to thank Mr. Nguyen Hong Ha from Optical Networking Lab, whom I had many fruitful discussions. Some of the ideas applied in this thesis owe their origin to these discussions.

Finally, it's time to remember the blessing called family, and be grateful for their unconditional love and support.

Table of Contents

CHAPTER 1 – Introduction	13
1.1 Broadband Access Network Technologies	13
1.1.1 Passive Optical Network	13
1.1.2 Wireless Networks	15
1.2 Hybrid Wireless-Optical Broadband Access Network	16
1.2.1 Architecture	17
1.2.2 Advantages	18
1.3 Motivation for Research	19
1.4 Contribution of the thesis	20
1.5 Thesis outline	21
CHAPTER 2 – Background and Related Work	23
2.1 Fault-tolerance in traditional PON	23
2.2 Fault-tolerance in Wireless Mesh Networks	25
2.3 Literature review on fault-tolerance in WOBANs	26
2.3.1 Risk-and-Delay-Aware Routing Algorithm (RADAR)	27
2.3.2 Fault-Tolerance using Multi-Radio	28
2.3.3 Wireless Protection Switching for Video Service	30
2.3.4 Design of Survivable WOBAN	31
2.4 Summary	33
CHAPTER 3 – Optical Fault-Tolerance using Wireless Resources	34
3.1 Basic concept	34
3.2 Advantages	36
3.2.1 Restoration time	36
3.2.2 Guaranteed bandwidth	37
3.2.3 Delay performance	37
3.2.4 Cost-effective	38
3.2.5 Deployment and application	39
3.3 Enabling technologies	40
3.3.1 Multi-radio Multi-channel WOBAN	40
3.3.2 Off-the-shelf technology and equipment	41

3.4	Backup radio Placement problem.....	43
CHAPTER 4 – Problem Formulation and Complexity Analysis		44
4.1	Graph Modeling and Problem Definition.....	44
4.2	NP-completeness proof	45
4.2.1	Problem transformation	45
4.2.2	Polynomial-time verification.....	46
4.2.3	Reducibility.....	46
4.3	ILP model.....	49
CHAPTER 5 – Heuristic Algorithms and Performance Evaluation		52
5.1	Most-Traversed-Node-First (MTNF) heuristic.....	52
5.2	Closest-Gateway-First (CGF) heuristic	54
5.3	Performance Evaluation.....	55
5.3.1	Performance on a small network.....	56
5.3.2	Performance on San Francisco WOBAN	57
5.3.3	Performance on random networks.....	63
5.3.4	A special case	73
CHAPTER 6- Conclusions		75
LIST OF PUBLICATIONS.....		77
REFERENCES		78

List of Figures

Figure 1 - Passive Optical Network Architecture	14
Figure 2 – A WOBAN architecture	18
Figure 3 - Protection switching architectures [1].....	24
Figure 4 - Wireless Protect Link for Inter-WONU communication	30
Figure 5 - Survivable WOBAN.....	32
Figure 6 - Optical fault-tolerance provision by backup radio example	36
Figure 7 - Multi-radio multi-channel WOBAN example [20]	40
Figure 8 - Graph mapping function.....	47
Figure 9 - Reverse graph mapping function.....	48
Figure 10 - MTNF heuristic algorithm	53
Figure 11 - Closest-Gateway-First heuristic	55
Figure 12 - Simple topology illustration	56
Figure 13 - San Francisco WOBAN architecture	58
Figure 14 - Optimal results for SFNet	59
Figure 15 - MTNF result for SFNet	60
Figure 16 - Cost analysis of various approaches.....	63
Figure 17 - Differences between a random network and scale-free network	64

Figure 18 – Results of 10 experiments on networks with 100 nodes.....	67
Figure 19 - Running time for different approaches.....	67
Figure 20 - Performance comparison of three approaches.....	68
Figure 21 – Percentage of performance difference of CGF and MTNF	70
Figure 22 - Performance in large networks.....	71
Figure 23 – Performance difference with various average node degree	71
Figure 24 - Average path length for backup routes.....	73
Figure 25 – Special case when MTNF outperforms CGF.....	74

List of Tables

Table 1 - Notations.....	49
Table 2 - Backup paths for gateways in the small network	57
Table 3 – Detailed optimal result for SFNet	58
Table 4 – Detailed MTNF result for SFNet	60
Table 5 - Cost of network components in WOBAN	61
Table 6 - Deployment cost of different approaches	62

List of Symbols and Abbreviations

AP	Access Points
APS	Automatic Protection Switching
BA	Barabási–Albert model
BROF	Backup Radio for Optical Fault-tolerance (problem)
BS	Base Station
CGF	Closest-Gateway-First
CO	Central Office
DF	Distribution Fiber
EPON	Ethernet Passive Optical Network
ER	Erdős–Rényi model
FF	Feeder Fiber
FTTC	Fiber-to-the-Curb
FTTH	Fiber-to-the-Home
FTTx	Fiber To The X (X=Home/Office/Curb...)
Gbps	Gigabit per second
GPON	Gigabit Passive Optical Network
ILP	Integer Linear Programming
ISM	Industrial Scientific and Medical (band of spectrum)
LAN	Local Area Network
LOS	Line Of Sight
MAC	Media Access Control
MANET	Mobile Ad-hoc Network

Mbps	Megabit per second
MTNF	Most-Traversed-Node-First
NP	Non-Polynomial
OLT	Optical Line Terminal
ONU	Optical Network Unit
PON	Passive Optical Network
QoS	Quality of Service
RADAR	Risk-and-Delay-Aware (routing algorithm)
RL	Risk List
RN	Remote Node
SS	Subscriber Station
TDM	Time Division Multiplexing
WDM	Wavelength Division Multiplexing
WiFi	Wireless Fidelity
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
WMAN	Wireless Metropolitan Area Network
WMN	Wireless Mesh Network
WOBAN	Hybrid Wireless-Optical Broadband Access Network
WS	Watts-Strogatz model

CHAPTER 1 – Introduction

This chapter first provides background on broadband access technologies and an overview on the new architecture WOBAN. The importance of fault-tolerance and especially optical fault-tolerance in WOBAN are discussed in detail. Backup Radio placement for Optical Fault-tolerance (BROF) problem is defined. Finally, contribution and structure of the thesis are explained.

1.1 Broadband Access Network Technologies

As the Internet evolves, customers are demanding more and more bandwidth due to the strong growth of multimedia services such as emerging video-enabled applications and peer-to-peer sharing. This leads to the need for network operators to design a new and efficient “last mile” access network. The new network architecture not only has to provide enormous transport capacity but it should provide end users with mobility and convenience as well. Among the existing broadband access technologies, Passive Optical Networks (PONs) and wireless networks are the two most promising solutions for the future networks.

1.1.1 Passive Optical Network

PON is a point-to-multipoint, fiber-to-the-premise network architecture. It consists of an optical line terminal (OLT) at the telecom central office and a number of optical network units (ONUs) in premises of end-users (Figure 1). The virtually unlimited bandwidth (in range of terahertz or THz) of fiber compared to the traditional copper-based access loops makes PON able to provide very high bandwidth for data applications. Moreover, since bandwidth can be shared among

all end users, the per-user cost of PON can be reduced. As such, PON is the key technology for Fiber-to-the-Home (FTTH) and Fiber-to-the-Curb (FTTC) networks.

Passive Optical Network (PON)

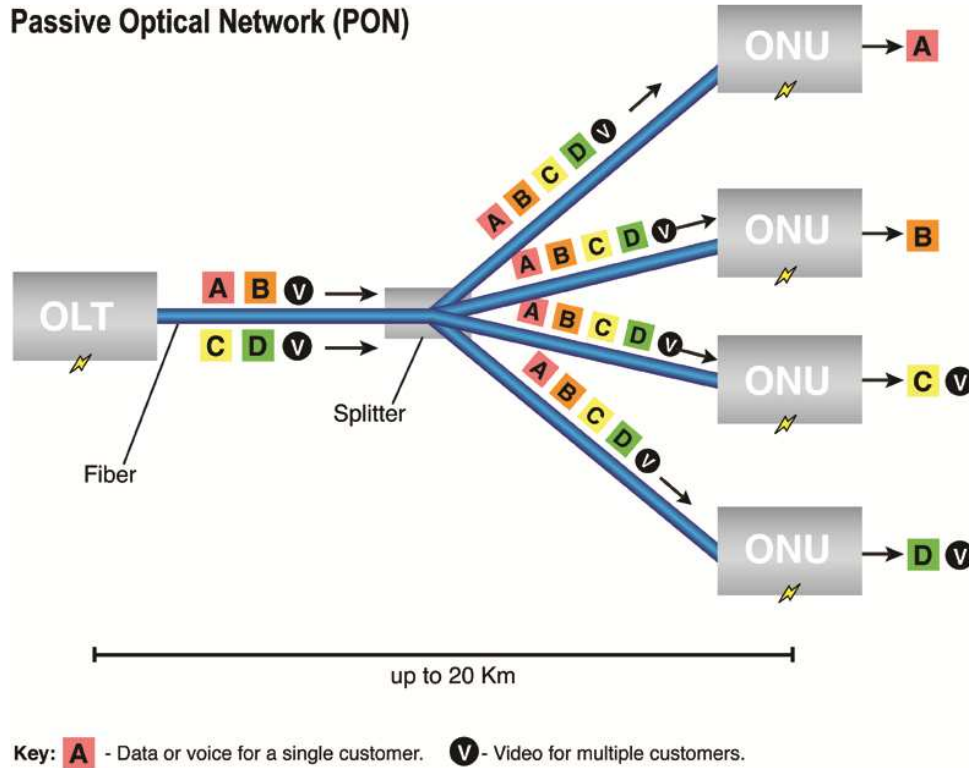


Figure 1 - Passive Optical Network Architecture

Currently, TDM-PONs (Time-division-multiplexing PONs) can provide a network capacity up to 1 Gbps (Gigabit per second) (using Ethernet PONs - EPONs) or 2.5 Gbps (using Gigabit PONs – GPONs) [1]. However, if more bandwidth is demanded, network operator can consider upgrading to Wavelength-division-multiplexing PONs (WDM-PONs).

WDM-PON increases system capacity by transmitting messages on several wavelengths simultaneously on a single fiber. The power splitter in traditional PON is replaced by a wavelength coupler. So each ONU is allocated with its own

wavelength and it can operate at a rate up to the full bit rate of a wavelength channel [2]. The link between OLT and each ONU is a point-to-point (P2P) link. That helps to achieve a system with a very high privacy. Furthermore, scalability can be supported since we can reuse the same fiber infrastructure.

1.1.2 Wireless Networks

Recently wireless networks have become a popular access solution all over the world. Wi-Fi (Wireless Fidelity), WiMax (Worldwide Interoperability for Microwave Access) and 3G (Third Generation Cellular Network) are three major techniques that are used to provide network access.

Among three of them, Wi-Fi is the most used technology for wireless Local Area Networks (LANs). Its current and most popular standards – IEEE 802.11 a/b/g – are popularly used in a lot of end user devices. Wi-Fi has two modes of operation: infrastructure mode and ad-hoc mode. In infrastructure mode, an access point works as a central authority to manage the networks. In ad-hoc mode, there is no central authority and the nodes have to agree on some protocols to manage themselves. Direct node-to-node communication allows Wi-Fi to exploit the “multi-hopping” networking where information is conveyed from a source to a destination in two or more hops. Currently, Wi-Fi offers low bandwidth (less than 54 Mbps) in a limited range (less than 100m)

WiMax, though not as popular as Wi-Fi, is gaining rapid adoption worldwide, especially in emerging countries. It operates in two modes: Point-to-Multipoint (P2MP) and Mesh Mode (MM). In P2MP mode, WiMax is essentially used for single-hop communication from users to base station (BS). On the other hand, in Mesh Mode, multi-hop connectivity is provided for user traffic delivery.

Compared to Wi-Fi, WiMax offers higher bandwidth and a much longer range. It can support bit rates up to 75Mbps in a range of 3-5km and, typically 20-30 Mbps in longer ranges [3]. Hence, WiMax is more suitable for Wireless Metropolitan Area Network (WMAN) than Wi-Fi which is a WLAN dominant technology.

The 3G cellular technology is used for low-bit-rate applications (typically 2 Mbps). The reason is because cellular networks are designed for carrying voice traffic and are not optimized for data traffic. While Wi-Fi and WiMax can use the free industrial, scientific and medical (ISM) band of spectrum, 3G users have to pay for a regulated expensive licensed spectrum.

1.2 Hybrid Wireless-Optical Broadband Access Network

Although PON and Wireless Networks are both promising solutions for broadband access networks, they have some disadvantages. First, it is very costly to deploy fiber to every home from the telecom CO. In some cases when the end-user premises are located in the central urban areas, it even becomes prohibitively expensive. Second, wireless technology can offer a much lower bandwidth compared to the optical access networks. Further, as limited spectrum is the nature of wireless communication, it is impossible to provide wireless access directly from the CO to every end-user.

Hence, a compromise to run fiber as far as possible from the CO toward the end-user, and use wireless access from there to take over can be a good solution. This is where the concept of WOBAN becomes very attractive as it tries to capture the best of both worlds.

1.2.1 Architecture

WOBAN consists of two parts: wireless mesh network at the front end and optical network at the back end (Figure 2). From the CO, each OLT drives multiple ONUs like in a traditional PON. The main difference is that ONUs do not serve end-users directly but they are connected to wireless BSs for the wireless part of WOBAN. Those wireless BSs are called wireless “gateway routers” because they function as gateways for both the optical and the wireless parts. The end users may connect to wireless mesh routers called Access Points (AP) using either Wi-Fi or WiMax. Those wireless APs together with wireless gateway routers form a wireless mesh network.

In a typical uplink of WOBAN, traffic from end-users will be sent to its neighboring AP – mesh router. This router then routes traffic in a multi-hop fashion through other mesh routers to reach one of the gateways (and to the ONU). The traffic is finally sent through the optical back end of WOBAN to OLT and consequently to the rest of the Internet. In the downlink, OLT broadcasts to all ONUs in the tree access network and from the gateways, packets are sent only to their specific destinations through wireless mesh networks.

Each mesh routers in a “Gateway group” as shown in Figure 2 forwards its traffic only to the group’s pre-assigned ONU during normal operation. However, in the event of failure, they will try to reach another active ONU in neighboring “Gateway groups” through multiple hops.

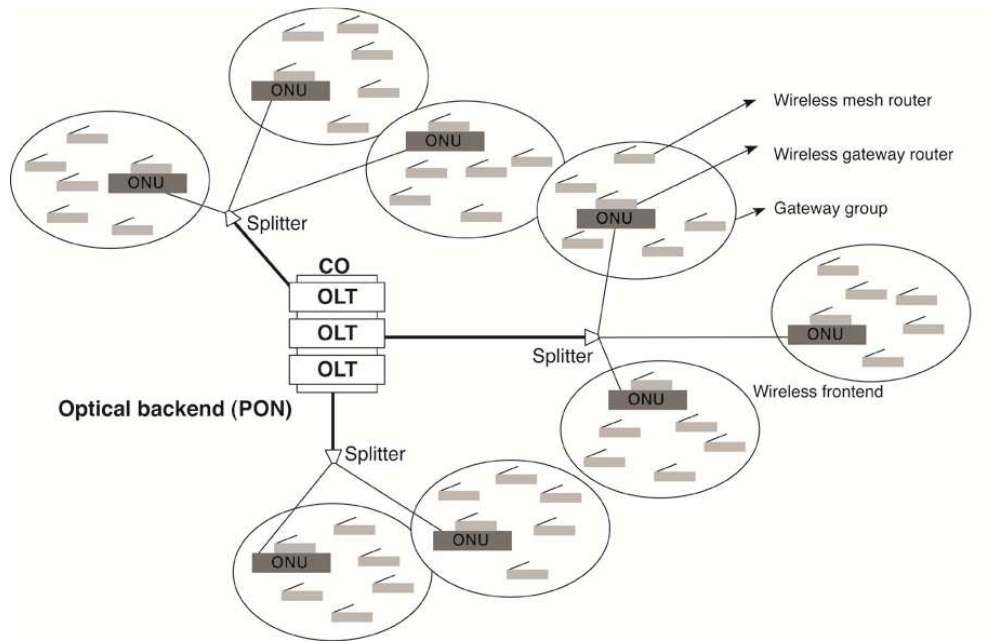


Figure 2 – A WOBAN architecture

1.2.2 Advantages

As an effective integration of high-capacity optical and untethered wireless access, WOBAN gives several advantages:

- *Cost effectiveness*: Deploying expensive FTTx technologies may cost more than \$100,000 per mile in metropolitan area because trenching and installing new duct normally cost about 85% the optical fiber installation fee [4]. WOBAN architecture helps us to get the fiber penetration as far as we can in the most economical manner and from there, we can use wireless technologies.
- *Flexibility*: the wireless part of WOBAN allows the end-users to seamlessly connect to one another.
- *Robustness*: as the users have the ability to form a multi-hop mesh topology, the wireless connectivity may be able to adapt itself in

case there is an ONU or OLT breakdown by connecting through other active neighboring ONUs.

- *Much higher capacity*: compared to the traditional wireless network thanks to its high-capacity optical trunk.

1.3 Motivation for Research

Although WOBAN can offer many advantages, it can fail at some unspecified time like any other network. As a wide range of state-of-the-art applications in WOBAN has emerged in recent years and more will be available in the future, network fault-tolerant requirements should be taken into account during the design process of WOBAN. In fact, it does not matter how attractive and potentially lucrative our applications are if the network stop functioning. A fault-tolerant network will be required to ensure efficient and stable operation, i.e., make the service of the application available in the event of faults.

Failures can happen anywhere in the architecture of WOBAN. However while the wireless mesh network part of WOBAN has the capability of self-healing by using alternative routing paths, the back end PONs cannot survive network element failures because a tree topology is used [5]. A study in [6] also estimated that the frequency of fiber cut events is hundreds to thousands of times higher than reports of transport layer node failures. In case there is a fiber cut, significant amount of information will be lost which leads to huge financial losses. That makes fault-tolerance in optical part more critical than in wireless part of WOBAN and it is also the reason that we are focusing only in providing optical fault-tolerance in this thesis.

There have been several works done to handle failures in WOBAN by using extra resources. In [7], Correia proposed a backup architecture with extra radios at each mesh router except gateways. Although this provides some extra bandwidth for backup traffic, it still cannot ensure full protection and at the same time requires a huge deployment cost by employing too many multi-radio interfaces. Feng et al in [5] used extra fiber to connect ONUs in different PON segments to ensure one segment is protected by spare capacity of other segments. However, they did not take into account the cost and practical difficulties of laying fiber in urban areas. This thesis is an attempt to overcome the drawbacks and limitations problems in the above approaches. We provide a new way to handle optical element failures in the back end optical access network part by using the wireless resource of WOBAN front end.

Problem definition: Given a WOBAN with known topology, find a subset of nodes among the existing nodes (wireless routers) in the Wireless Mesh Network front-end to place backup radios so that the ONUs, OLTs, fibers are fully protected against single component failures and the backup radio deployment cost is minimum.

1.4 Contribution of the thesis

In this thesis, the backup radio placement problem for providing optical fault-tolerance is addressed. The key idea is to deploy backup radios at gateways and a few selected nodes of the front-end Wireless Mesh Network (WMN) of the WOBAN so that each ONU is wirelessly connected to another ONU called backup ONU. Upon failure, traffic will be rerouted in a dedicated channel from the failed ONU through multiple hops of the WMN to reach the backup ONU.

This approach is not only easier to deploy, and more feasible but also more cost-effective than the traditional PON protection methods and other solutions proposed earlier in the literature. The problem of choosing a subset of nodes to deploy backup radios so as to minimize the deployment cost is not trivial. We formulate and prove that the problem is NP-complete. We then develop an Integer Linear Program (ILP) formulation in order to solve this problem. We obtain numerical results for networks with less than 200 nodes by solving ILP using ILOG CPLEX.

We also develop two heuristic algorithms - Most-Traversed-Node-First (MTNF) and Closest-Gateway-First (CGF). The main idea of MTNF is to find shortest backup paths from each gateway to all other gateways at first, and choose nodes that appear in most of the backup paths to place backup radios. In CGF, we do not search shortest paths between each pair of gateways. Instead, we use Dijkstra's algorithm to find all the shortest paths from each gateway to its closest gateway only. We evaluate the performance of the two heuristics on a real WOBAN as well as on random networks. Our results show that CGF provides results very close to the optimum values. We also observe that both heuristics have much smaller running time than the ILP solution.

1.5 Thesis outline

The rest of the thesis is organized into the following chapters.

In Chapter 2, we present the background and literature review on fault-tolerance provisioning in PON and WMN. We then discuss related works on fault-tolerance planning and provisioning in WOBANs and analyze their limitations.

In Chapter 3, we introduce a new way to provision optical fault-tolerance using wireless resource. Its advantages compared to the existing solutions and enabling technologies are discussed followed by the presentation of the backup radio deployment problem.

In Chapter 4, the optimization problem is formulated using graph theory. We prove that this problem is NP-complete by transforming it to an equivalent decision problem. An ILP model is developed to solve the problem.

In Chapter 5, we develop two heuristic algorithms – MTNF and CGF to solve the backup radio deployment problem. Their performance is benchmarked against the results obtained by solving ILP using ILOG CPLEX for small networks. We study the performance of the two heuristic algorithms on large random graphs as well as on SFNet – a real WOBAN deployment in San Francisco.

The final chapter concludes this thesis with some directions for future research.

CHAPTER 2 – Background and Related Work

There have been many works carried out to provide fault-tolerance in optical networks and wireless mesh networks. In this chapter, the protection methods for PONs and WMNs are reviewed, and recent research literature on fault-tolerance for WOBAN are detailed.

2.1 Fault-tolerance in traditional PON

Below are a few useful considerations in designing a PON with fault-tolerance capability:

- Protection vs. dynamic restoration: Preplanned protection offers fast restoration time but requires more resources than dynamic restoration methods.
- Network topology: tree and ring topology require different approaches for provisioning fault-tolerance than arbitrary mesh topologies.
- Network type: TDM or WDM technique is a major factor we need to take into account when designing a fault-tolerant network
- Single or multiple component failures
- Automatic Protection Switching (APS): can be done in a centralized or distributed way.
- Cost and complexity

Figure 3 shows the four most conventional protection switching architectures for TDM-PONs with tree topology. For WDM-PON, the same architectures could be employed with a small modification where the optical

power splitter at the remote node (RN) has to be replaced by a wavelength multiplexer. These architectures are suggested by ITU-T G.983.1 [8] for different levels of protections.

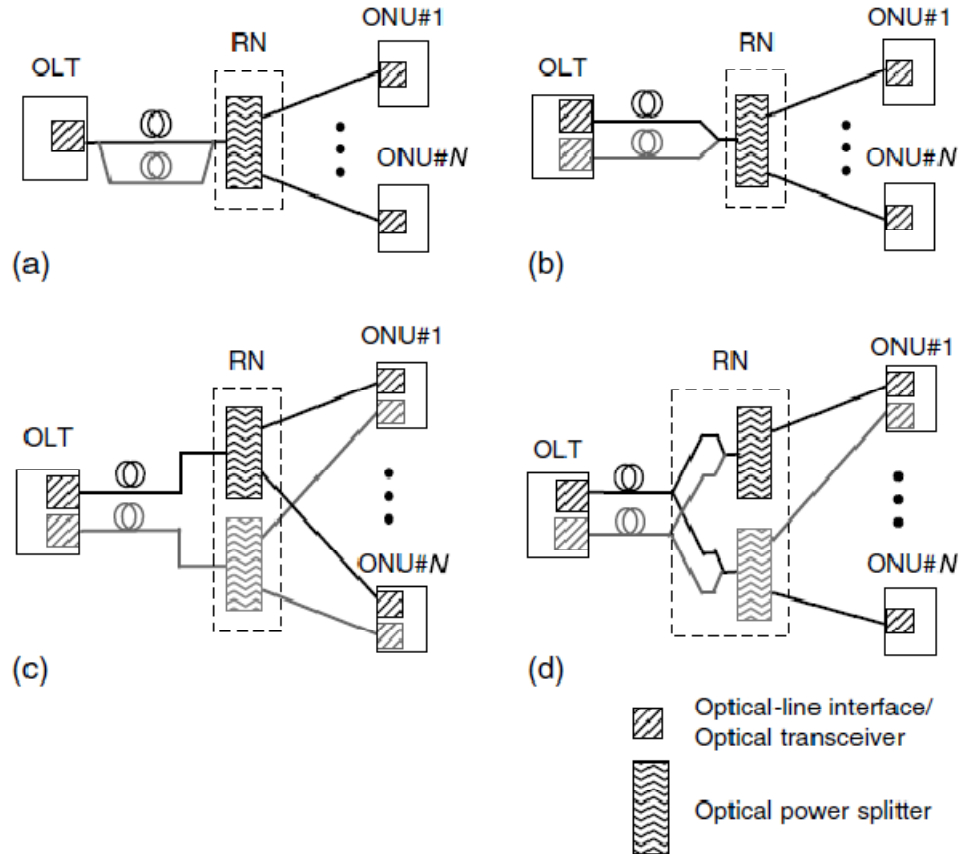


Figure 3 - Protection switching architectures [1]

Although the four protection architectures are different, they all have the same idea: provide protection by duplicating the fiber links and/or the network components. Figure 3 (a) only provides protection for the feeder fiber between OLT and RN. No switching protocol is required for OLT/ONU in this architecture. Figure 3 (b) duplicates equipment between the OLT and the RN. There are two optical transceivers at the OLT and two feeder fibers. Protection switching is done entirely at the OLT side. In Figure 3 (c), all PON equipment is

fully duplicated to provide 1+1 path protection. Figure 3 (d), which is similar to Figure 3 (c), allows for a partial duplication of resources on ONU side due to some system constraints.

In addition to the four standard protection schemes, there are several novel schemes [9-14] which are more cost-effective. Although using different architectures and switching methods, they all require duplication of equipment at some levels. Compared with transport networks, optical access network are very cost sensitive. Therefore, minimizing the cost for network protection and obtaining an acceptable level of connection availability at the same time is a real challenge that will be addressed in the next chapter.

2.2 Fault-tolerance in Wireless Mesh Networks

Although there are many works that have been done on fault-tolerance provisioning techniques in wireless sensor networks (WSNs) and mobile ad hoc networks (MANETs), they are not suitable to be applied in WMNs due to some basic differences:

- Unlike WSN, nodes in WMNs do not have energy constraint. Both mesh routers and mesh gateways are usually connected to rich power supply. That allows nodes in WMNs to run more sophisticated algorithms for routing and switching traffic.
- The location of nodes in MANETs keeps on changing because of node mobility. Therefore the topology of MANETs is very dynamic. On the other hand, mesh routers in WMNs are always fixed or with very little mobility.

- The network bandwidth in a WMN is large because each mesh router can use multi-radio interfaces and employ multiple orthogonal channels. This cannot be done in both WSNs and MANETs due to the energy constraint.

In a recent survey on WMNs [15], most of the methods to provide fault-tolerance in WMNs rely on multi-path routing protocols in network layer. Several paths between source node and destination node are selected. During the normal operation, packets can choose any path among those selected multiple paths. When a link on a path breaks due to bad channel quality or node failures, another path in the set of active paths can be chosen. However, if shortest path is taken as the routing metric, multi-path routing is not applicable. Another problem is that the multi-path routing algorithms depend on the availability of node-disjoint routes between source and destination. Despite their drawbacks, fault-tolerance provisioning methods in WMNs can be used for the frontend network of WOBAN which hold very similar characteristics.

2.3 Literature review on fault-tolerance in WOBANs

Fault-tolerance provisioning methods for PONs and WMNs have been discussed in the earlier sections. As WOBAN architecture has been proposed only recently, there have not been much research papers on WOBANs in general, and on fault-tolerance in WOBANs in particular. There are only a few works done in the area of fault-tolerance in WOBAN as follows:

2.3.1 Risk-and-Delay-Aware Routing Algorithm (RADAR)

The first work that proposed a method to protect WOBANs against failure is RADAR by Sarkar et al. [16]. According to this work, failures in WOBANs can be classified into three categories:

- Wireless router/gateway failure
- ONU failure (equivalent to distribution fiber failures)
- OLT failure (equivalent to feeder fiber failures)

The authors proposed a new routing algorithm in WOBAN called RADAR that can take into account the risk of failures as a routing metric. Each gateway is indexed and maintained in a hierarchical risk group that shows to which ONU and OLT it is connected. ONUs and OLTs are indexed in similar fashion. To reduce packet loss, each router maintains a “Risk List” (RL) with “Secondary Gateway Group” and “Tertiary Gateway Group” providing alternative paths to route packets in case of a failure. RL is a way for each router to keep track of failures. In the no-failure scenario, all the paths in RL are marked live. When there is a failure, RL will be updated with the failed path marked as “stale”. While forwarding packets, routers will only choose a “live” path.

Although RADAR offers risk awareness capability for WOBANs with the minimal cost as it makes use of the existing resources in the network, it also has some disadvantages: Firstly, when failures happen, RADAR requires an amount of time to update the state of the routing paths to all the RLs at each router. For example, if the failure happens at one ONU, failure notification message needs to be forwarded all the way from that ONU back to the original source, as well as all other nodes in the network. The mesh routers have to send a signal to reserve the

resources at each node in the new routing path before they can restore their services and traffic. Thus the restoration time of RADAR is high.

Secondly, since RADAR only reroute the traffic through another live path, there is very high probability that the rerouted traffic has to compete for bandwidth and resource with the primary traffic in that live path. In that case, congestion in some common nodes along that live path will happen. Consequently, the packet loss rate, instead of decreasing, will start to increase rapidly. In the end, more packets will be dropped and services and applications will be disrupted. It is reported in [16] that in case an OLT failure, RADAR still has a very high packet loss rate around 30%.

In short, though RARAR is one of the first approaches to deal with failures in WOBAN, it cannot ensure a full protection for WOBAN with small restoration time.

2.3.2 Fault-Tolerance using Multi-Radio

In a similar approach as RADAR, Correia et al. in [7] tried to solve the problem of planning a fault-tolerant multi-radio WOBAN while using the resources efficiently. The basic idea is to deploy at least two radios at each mesh router of the wireless mesh network while gateways are allowed to have one radio. Their solution is based on an integrating routing and channel assignment algorithm which consists of two steps:

- *Step 1:* Computation of primary and backup routes using shortest path criteria. The two routes need to be link-failure independent and backup route is activated whenever a link of the primary route fails.

- *Step 2:* Frequency assignment to wireless links (and radios, at the same time) used in primary and backup routes computed in step 1 with the condition that interfering primary and backup links use different channels. That is to ensure that they do not fail simultaneously.

The authors of [7] have been successful in providing fault-tolerance planning for both wireless and optical part of WOBANs. They also proposed a heuristic besides the optimal solution. As Correia's approach uses more radios, there are more non-overlapping channels available. That means that two nodes equipped with multi-radio interfaces can communicate with each other on two orthogonal wireless channels at the same time. Hence, the delay and packet loss rate for rerouted traffic are reduced. However, they still cannot ensure full protection for WOBANs when backup traffic from one source need to share bandwidth on the same wireless link with primary traffic from other sources. Failure notification time in this case is similar as in RADAR as the source node need to be notified before backup route can be activated. Moreover, the cost for this solution is quite high because it requires each node in the wireless mesh network to be equipped with at least two radios except gateways. The reason is that multi-radio nodes are significantly more expensive than single-radio nodes as reported in [17].

Another major drawback of the above approach is the bottleneck problem at the wireless gateway. This is due to the fact that gateways only use one radio. In a survey on WMNs in [15], Akyildiz et al. reported that although gateways have limited capability, they have to forward traffic from many other mesh routers and

can easily become a bottleneck. In the event of a failure in the network the failed traffic is rerouted to another gateway which already has its own traffic, the situation becomes worse. The gateway has to deal with more traffic using the same limited capability. Therefore, congestion is more likely to happen.

2.3.3 Wireless Protection Switching for Video Service

Another effort to provide fault-tolerance is presented in [18] by Zhao et al. The idea is to use wireless links between two W-ONUs (an integrated device defined as ONU with wireless function) to protect video service when there is a fiber cut. As shown in Figure 4, when the fiber connected to $WONU_1$ is cut, adjacent $WONU_2$ will set up a wireless link with $WONU_1$ if it could afford the new service payload.

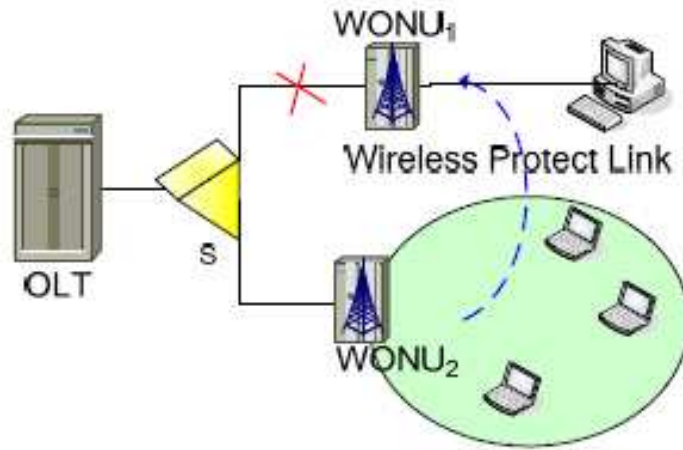


Figure 4 - Wireless Protect Link for Inter-WONU communication

Their major contribution is constructing an algorithm to allocate extra bandwidth for the corresponding backup ONUs in the event of a failure. It uses a time-domain normalized least mean square linear prediction algorithm for video traffic and Media Delivery Index as an index to measure video quality. That helps to guarantee video service quality.

The main issue of the above approach is the impractical assumption. It is nearly impossible to assure that there always exists a link between two W-ONUs. In real WOBAN deployments, ONUs are normally placed far from each other and can only be reached through several wireless hops. If the wireless link between two W-ONUs cannot be established due to the large distance or interference with other mesh routers, this scheme will not be able to function. In addition, this approach has the very same problem with two previous approaches, i.e., they cannot guarantee the wireless link's capacity to accommodate rerouted traffic.

2.3.4 Design of Survivable WOBAN

Apart from the three previous approaches, Feng's protection method in [5] tries to provide a maximum protection minimum cost solution for network element failures in the optical part of WOBANs. In each PON segment (driven by one OLT), they assign one ONU as a backup ONU. Their idea is to connect the back-up ONUs in different segments so that the traffic in one segment can be protected by the spare capacity in neighbor segments.

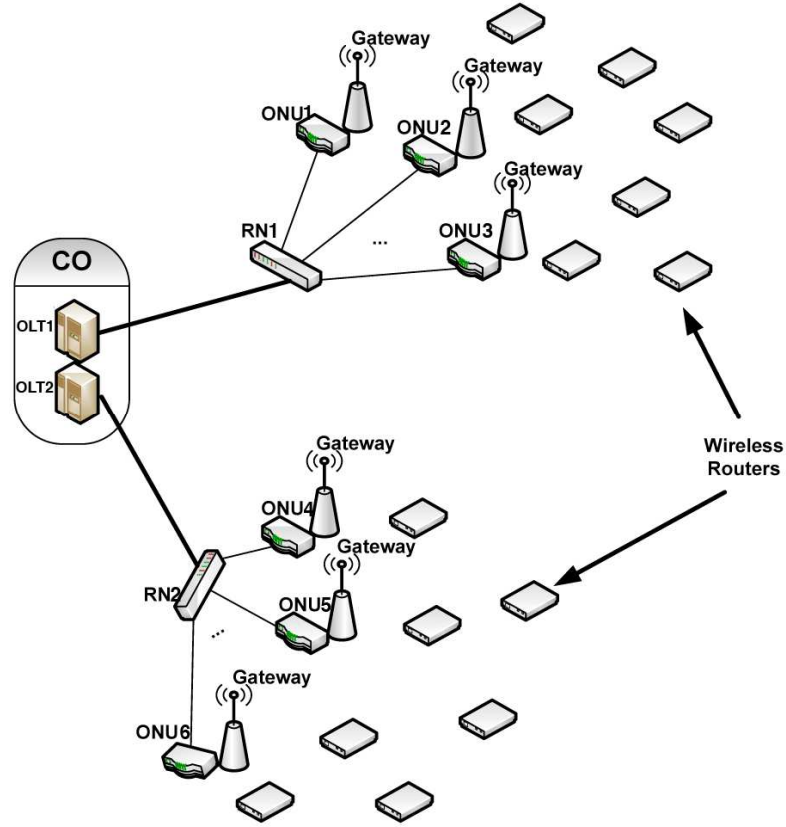


Figure 5 - Survivable WOBAN

In Figure 5, ONU₃ and ONU₄ are assigned as back-up ONUs for the segment driven by OLT₁ and OLT₂ respectively. They are called neighbors and connected with fiber. When the fiber feeder (FF) from OLT₁ to RN₁ is cut, all the traffic in segment 1 will be sent to the segment's backup ONU₃. The ONU₃ then sends the traffic to its neighbor backup ONU₄. The ONU₄ will distribute the traffic to all the ONUs in its segment via wireless gateways so that each ONU in the segment handles the traffic using its spare capacity [5].

By using the approach, Feng et al. claimed that they can achieve a smaller cost compared to the duplication of DF and FF as in normal optical access network. It is reported that the cost of their protection method is only one-tenth of

the cost of employing self-survivable PONs. However it is assumed that it is always possible to lay a fiber between any two backup ONUs which may not true. This assumption needs to be verified very carefully, especially in the urban area where normally, gateways in WOBAN are put on the roof of buildings. That makes the cost to lay the connecting fibers across the street highly prohibited.

Like other approaches mentioned in the previous section, Feng's protection method did not discuss how to deal with the bottleneck problem at gateways. We all know that the capacity of an optical network is much higher than a wireless network. Hence, when the backup ONUs distribute the rerouted traffic to all the ONUs in its segment via the wireless gateways, congestion is very likely to happen if the gateways are not equipped with extra capacity.

2.4 Summary

In this chapter, we have discussed various methods to provide fault-tolerance in optical access networks, wireless mesh networks and the combination of them: WOBANs. The current existing protection methods in WOBAN have their own advantages, but they do have many major drawbacks that need to be overcome if we want to use those solutions in real deployment. In chapter 3, we propose a new approach that attempts to solve many issues inherent in those protection methods presented in section 2.3.

CHAPTER 3 – Optical Fault-Tolerance using Wireless

Resources

In this chapter, we propose a new protecting method for optical network element failures in a WOBAN.

3.1 Basic concept

Consider a WOBAN architecture consisting of two parts: wireless mesh network part and optical access network part. Our proposed method is to provide extra radio resource in the wireless network part to provide optical fault-tolerance. We only consider single point-of-failure scenario which includes only one of the following failure types: feeder fiber cut, distribution fiber cut, OLT failure and ONU failure.

Instead of deploying extra radio at every node but gateways as in [7], our new protection method uses a different approach. We deploy extra radios at gateways and at only a few selected nodes in the wireless mesh network. We call those extra radios as backup radios because they are only used for backup purpose. If there is a fiber cut or an optical network element failure, optical fault-tolerance is provisioned by the extra capacity added to the network by backup radios. We note that a backup radio can be shared among backup paths that correspond to different optical component failures, thus facilitating backup resource sharing. We also note that our approach provides full protection guarantee, i.e., in the event of a failure the entire failed traffic is guaranteed to have a backup path.

By deploying multi-radio interfaces in WMN front-end and assigning the radios to orthogonal channels, we allow nodes to communicate simultaneously with minimal interference in spite of being in direct interference range of each other. That means more bandwidth is available to route traffic in the event of a failure.

Each ONU has its backup ONU assigned during the planning. Once the distribution fiber that connects it to its OLT is cut, its traffic will be rerouted to its backup ONU using wireless backup resources. That would be a fault-tolerance provision planning for distribution fiber cut or ONU failure. If we want to take into account feeder fiber cut and OLT failure, we have two options. First, for every ONU we can choose two backup ONUs: one in the same risk group (connected to same OLT), one in a different risk group (connected to another OLT). The second option would be the condition we set during our fault-tolerance provision planning: backup ONU and original ONU must belong to two different risk groups.

We deploy a backup radio at each node along the backup path from each ONU to its backup ONU. This creates an additional channel for rerouted traffic. So, if a failure happens, traffic from the failed ONU (a distribution fiber cut is equivalent to a failure of its corresponding ONU) will follow its backup path in the wireless mesh network of WOBAN to its backup ONU. That backup ONU will then send the traffic to its OLT.

Now, we consider an example with a WOBAN architecture shown in Figure 6. In this architecture, there are 25 mesh routers in which 5 nodes (5, 13, 16, 22 and 25) are gateways. For a simple case, backup radios can be deployed at three

nodes 16, 18, and 22 to create an additional channel from gateway/ONU 22 to gateway/ONU 16 and vice versa. If the distribution fiber from gateway/ONU 22 to its OLT is cut, the traffic can be rerouted from gateway/ONU 22 to gateway/ONU 16 along the backup path. At node 16, rerouted traffic and primary traffic of node 16 will then be combined and sent to the OLT.

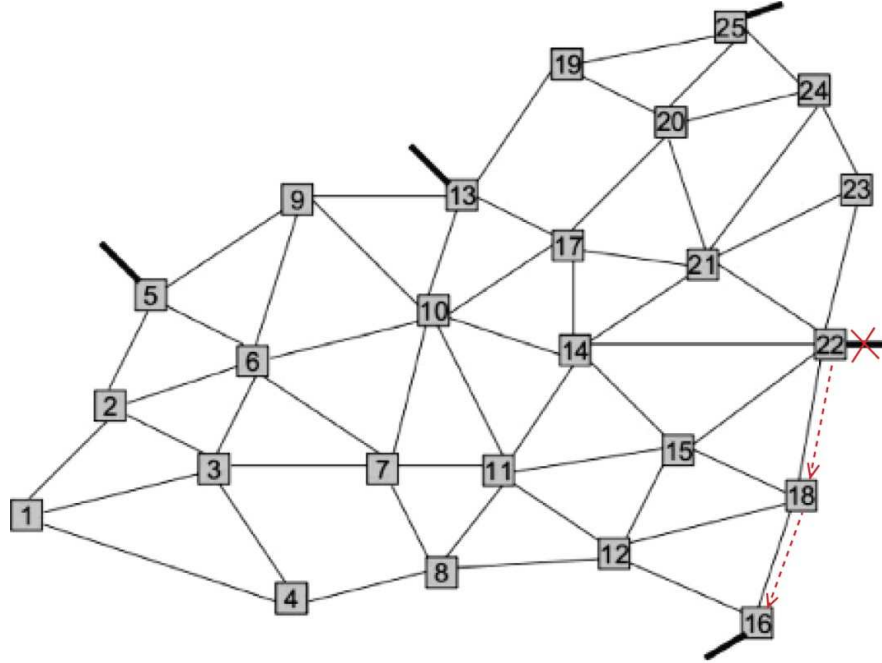


Figure 6 - Optical fault-tolerance provision by backup radio example

3.2 Advantages

Compared to other existing solutions, our new protection method has many advantages as discussed below.

3.2.1 Restoration time

Firstly, unlike other protection methods, the source node need not be notified of the failure in the optical part of WOBAN in the event of a failure. The moment the gateway detects that fiber is cut or optical element network fails, it will automatically use the channel created by the backup radios to reroute its

traffic to its pre-assigned backup ONU. As the failure is unknown to the source nodes, traffic will continue to be sent normally from source nodes to the gateways associated with the dead ONUs before they are rerouted. Some finite time is required for the gateway to switch the traffic from the primary channel to the backup channel which is usually short. The source nodes do not have to start finding an alternative route from the source to the backup gateway either. Hence restoration time will be much shorter.

3.2.2 Guaranteed bandwidth

Backup radios along backup paths use different frequencies from other mesh routers in the wireless mesh network. That helps to create a dedicated channel for backup traffic. This protection method can offer a full protection as the bandwidth is guaranteed for the entire rerouted traffic. The bottleneck problem at gateways which exists in other solutions is also solved in our proposed solution.

3.2.3 Delay performance

It is reported in [19] that there are four contributing factors to packet delay in WOBAN:

- Transmission delay: depends on the capacity of the link. If the capacity of the link is higher, the transmission delay is lower. As nodes share capacity of each links, we have transmission delay on a

link is $\frac{1}{\mu C_{uv}}$ with C_{uv} is capacity of link assigned to a particular

flow $u \rightarrow v$ and $\frac{1}{\mu}$ is the average packet size.

- Slot synchronization delay: is due to the TDMA-based operation of the wireless channel. The incoming packets need to be synchronized to their allocated time-slots for communication. The average slot synchronization delay is $\frac{1}{2\mu C_{uv}}$
- Queuing delay: depends on the service rate and packet arrival rate at the wireless nodes. It can be approximated as $\frac{1}{\mu C_{uv} - \lambda_{uv}}$ where λ_{uv} is the arrival rate of the traffic flow from $u \rightarrow v$.
- Propagation delay: can be ignored because mesh routers are quite close to one another in WOBAN

In short, the total delay on any given link $u \rightarrow v$ can be written as:

$$d_{uv} = \frac{1}{\mu C_{uv}} + \frac{1}{2\mu C_{uv}} + \frac{1}{\mu C_{uv} - \lambda_{uv}}$$

A dedicated backup channel uses extra radios to make C_{uv} larger as the entire channel can be used for rerouted traffic and does not have to share with other primary traffic flows. As C_{uv} increases, d_{uv} will decrease. In other words, our protection method can give a smaller packet delay.

3.2.4 Cost-effective

The backup radio protection method is advantageous in terms of cost. The backup radio deployment cost is less expensive than trenching and installing new fibers, especially in metropolitan areas. Moreover, our proposed method is not only less expensive than the traditional PON protection methods, but also more cost-effective than Correia's approach [7] which uses extra radios at every router

for providing protection. As we noted earlier, the multi-radio interfaces cost more than single-radio interfaces. By reducing the number of multi-radio interfaces that needs to be deployed, our protection method is able to provide a lower cost solution than Correia's method.

3.2.5 Deployment and application

Another attractive advantage to be highlighted is its simplicity in deployment and application. It can be noticed that other protection methods are not easy to deploy on existing WOBAN architectures. This is due to the fact that they either use their own protocols and routing algorithms or require special modification in WOBAN architecture. That would cause no problem if they are applied to a green field deployment. However, compatibility issues will require a lot of changes and adjustments otherwise. For example, if we want to use Correia's approach on some existing implementation of WOBAN, we need to change the entire routing algorithm and frequency channel assignment scheme of those networks which is apparently not straightforward.

On the other hand, backup radio protection method can be applied to any existing WOBAN implementation or any variation of WOBAN architecture. It can be used on top of any hardware, routing algorithm or frequency assignment scheme. Further, while the capacity of a fiber (on a single wavelength) is in the order of tens of Gbps, capacity of wireless link is only in the order of tens of Mbps. This ensures that the link from any ONU to OLT can easily accommodate more traffic than the maximum traffic of one gateway. Thus, we do not need any bandwidth allocation scheme for ONUs at the central control as in the approach of Zhao [18].

3.3 Enabling technologies

To illustrate how flexible and easy to implement a backup radio protection method, this section introduces current wireless technologies that can be used in practical implementation.

3.3.1 Multi-radio Multi-channel WOBAN

Multi-radio Multi-channel WOBAN is the key radio technology used in our backup radio protection method. In order to fully understand why multi-radio multi-channel WOBAN allows us to provide extra capacity, we consider a wireless mesh network example with five nodes as shown in Figure 7 [20].

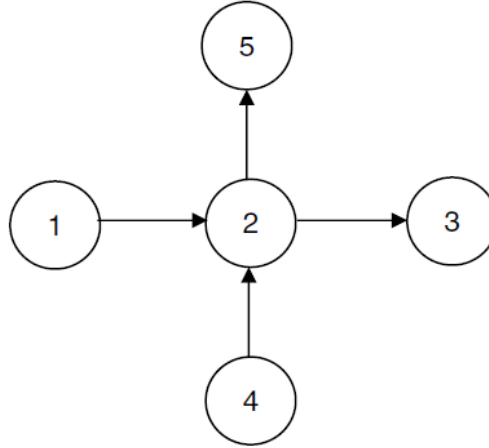


Figure 7 - Multi-radio multi-channel WOBAN example [20]

Let R denote the maximum possible transmission rate over one hop (for example, $1 \rightarrow 2$). We want to study the throughput of traffic traversing through path $1 \rightarrow 2 \rightarrow 3$:

- Single-radio single-channel: with one radio, node 2 spends roughly half the time receiving from node 1 and the other half the time transmitting to node 3 with a TDMA-based operation. Hence, if the

source node (node 1) has a transmission rate of R bps, the average throughput at the destination node (node 3) is approximately $R/2$ bps.

- Multi-radio multi-channel: if node 2 has two radios and there are two orthogonal channels available in the network, radio 1 can be tuned to channel 1 and radio 2 can use channel 2. In this case, the throughput at node 3 will be equal to R bps.

Now, we study the case of two concurrent traffic flows $1 \rightarrow 2 \rightarrow 3$ and $4 \rightarrow 2 \rightarrow 5$:

- Single-radio single-channel: with one radio, node 2 spends quarter of its time receiving from node 1 and 4 and transmitting to node 3 and 5. The average throughput at the destination nodes (node 3 and 5) is approximately $R/4$ bps. In this case, even if we have multiple orthogonal channels, the throughput will not improve as only one radio is available at node 2.
- Multi-radio multi-channel: if node 2 has two radios, by similar reasoning as above, the throughput for each flow is $R/2$ bps.

In summary, we can see that multi-radio multi-channel systems outperform single-radio single-channel systems in terms of bandwidth and performance.

3.3.2 Off-the-shelf technology and equipment

In practice, we have three basic types of wireless mesh network configurations [21]:

- 1-Radio Mesh: this configuration has only one radio to serve both clients and provide the mesh backhaul. This architecture has poor

performance among all options because both backhaul and client service compete for bandwidth.

- Dual-Radio with 1-Radio backhaul mesh: one radio is used to provide service for client, and the other is used to provide mesh network for backhaul traffic. These two radios can operate in the same or different bands. For example a 2.4 GHz IEEE 802.11b/g radio can be used for providing service while 5 GHz IEEE 802.11a radio can be used exclusively for backhaul.
- Multi-radio: one radio is used to provide service for mesh clients while other radios are used only for the backhaul network. This gives the best performance among all configurations but also is the most expensive one. The number of extra radios that can be used at one node is bounded by the number of orthogonal channels available in the network. For example, according to [22], IEEE 802.11b/g has three non-overlapping channels while IEEE 802.11a can provide up to 12 or 13 non-overlapping channels depending on each country's regulation. IEEE 802.11n, a new standard which is currently in adoption phase, can provide many more non-overlapping channels as it uses both 2.4 GHz and 5 GHz bands.

In addition to the well-defined and popular standard, many commercial products have been available in the market. Many companies are now offering a variety of multi-radio-interface wireless mesh routers with not so expensive price. Among them Cisco, Belair and Tropos are three key players in the equipment market [23-25]. A full survey on current implementation of WOBAN can be

found in [26] which shows the availability of multi-radio multi-channel radio technology.

All the enabling technologies discussed above are the premises allowing backup radio protection method to work effectively in a real deployment and application.

3.4 Backup radio Placement problem

Our objective is to select a subset of wireless routers to place backup radios (in addition to the gateways/ONUs) so that we can provide full protection guarantee in the event of a single optical component failure. It is evident that we do not need to deploy extra radios along all the backup paths. The reason is because, if the backup paths (corresponding to different component failures) have some common routers, they can share the same extra radios for the single-component-failure scenario. As the multi-radio interfaces are expensive, we need to minimize the number of multi-radio interfaces deployed. Hence, we can summarize our problem statement as follows:

Given a hybrid wireless-optical access network (WOBAN) with known topology comprising of N nodes and M gateways. Using the backup radio protection method, determine the subset of routers in the wireless mesh network part of WOBAN to place backup radios such that:

- *WOBAN is fully protected against optical component failures and*
- *the deployment cost (in terms of the total number of backup radios) is minimized*

CHAPTER 4 – Problem Formulation and Complexity

Analysis

4.1 Graph Modeling and Problem Definition

In this section, we present the graph modeling of the network and the problem definition of the Backup Radio placement for Optical Fault-tolerance problem (BROF). An instance of the BROF problem is represented by a graph $\langle G, V, E, V_g, C \rangle$ where

- G : graph that represents the network topology
- V : set of nodes where each node is a mesh router or gateway in the WOBAN. Each node is equipped with one or more interface cards (radios). In the BROF problem, we only count the number of radios used for backhaul traffic.
- E : set of feasible transmission link in the network
- V_g : subset of V , where each element represents a gateway
- C : a cost function represents the cost to deploy backup radio at each node:

$$C : V \rightarrow R^+ \\ u \rightarrow f(u) = c_u$$

The objective of the BROF problem is to find a sub-graph of nodes that needs to be deployed backup radio, $G_1 = (V_1, E_1, V_g)$, such that:

- $V_g \subset V_1$. Every gateway in WOBAN needs to have at least one backup radio to avoid the bottleneck problem.

- $\forall i \in V_g, \exists j \neq i \text{ and } j \in V_g$ such that i and j are connected in G_I . In other words, this means each ONU will have at least one backup ONU and they are connected by a dedicated backup path using extra radio resource.
- $\sum_{i \in V_1} c_i$ is minimized because we want to minimize the deployment cost. c_i is the cost to deploy a backup radio at node i .

4.2 NP-completeness proof

Theorem 1: *The backup radio placement for optical fault-tolerance problem (BROF) in WOBAN is NP-Complete*

Proof: The proof for theorem 1 is given in the following subsections

4.2.1 Problem transformation

We consider a special case of our problem where we choose the backup ONU for each ONU in advance. Without loss of generality, the cost of deploying a radio at each node in the network is taken as unity. We also want to transform the BROF problem from an optimization problem to an equivalent decision problem. So, we can write its decision version:

Instance: Given an undirected and unweighted graph $G = \{V, E\}$ with a gateway subset $V_g \subset V$ and an integer K .

Question: Is there any sub-graph $G_I = (V_I, E_I)$ of G , where each pair of vertices (a gateway and its backup gateway) belonging to V_g is connected, and the total number of nodes in G_I is at least K ($|V_I| \geq K$) ?

4.2.2 Polynomial-time verification

In order to prove the decision version of the BROF problem belonging to NP , we must prove there is a solution verification algorithm that can run in polynomial time. Assuming that we have a solution for our BROF decision problem, it is easy to see whether the solution is correct or not. By subsequently removing one node at a time from the resulting graph G_I , we can verify in polynomial time whether each pair of vertices in V_g is still connected in the new graph with an integer $L = K - I$.

Hence, our BROF decision problem is in NP .

4.2.3 Reducibility

For NP-hard proof, we can reduce the well-known Steiner Forest problem [27] to the BROF decision problem. Steiner Forest problem is a generalization of Steiner Tree problem with its formal decision version given as below:

Instance: Given an undirected and weighted graph $G' = (V', E', w)$, a collection of disjoint subset of V' : $S_1, S_2 \dots S_k$ and an integer K' . w is a cost function for the edges in the graph.

Question: Is there any sub-graph $G'_1 = (V'_1, E'_1)$ in which each pair of vertices belonging to the same set S_i is connected, and the number of nodes in $G'_1 : |V'_1| \geq K'$?

The reduction algorithm is done by constructing a mapping function. We have to map the weighted graph G' into an unweighted graph G . For all edges in G' with weight of N , we can replace this edge by N new nodes. That means that there will be $(N+1)$ new edges with weight of 1 between the two original nodes

for each edge. As shown in Figure 8, edge $A - B$ has a weight of 4 in the original graph G' . By using our mapping function, edge $A - B$ becomes 5 edges $A - C_1 - C_2 - C_3 - C_4 - B$ in the equivalent graph G .

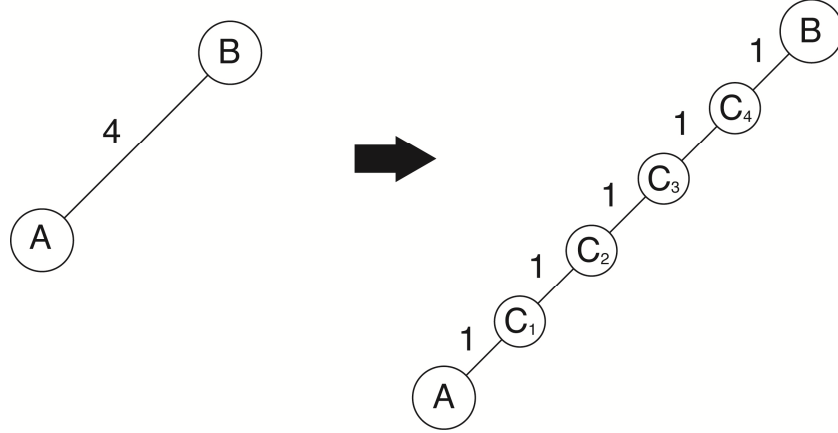


Figure 8 - Graph mapping function

The collection of subset $\{S_1..S_k\}$ in Steiner Forest problem can be mapped to gateway subset V_g in BROF decision problem:

$$V_g = \bigcup_{i=1}^k S_i$$

The integer K in BROF decision problem can be simply set to be equal K' in Steiner Forest problem.

The last step needs to be done to prove the solution of our BROF decision problem is also the solution of the Steiner Forest problem. Assuming that we have a “yes” answer solution for BROF decision problem, we have to map the result graph G_I of BROF decision problem back to a graph G'_I and prove G'_I is indeed the solution of the original Steiner Forest problem.

For transforming the unweighted solution graph G_I to the corresponding weighted graph G'_I , we can use a reverse function of the graph mapping function given above. For each pair of connected original nodes, we replace all N new

nodes between them by an edge with weight of N . However, we have to apply an additional rule here:

If $A, B \in S$ and A and B are connected by new nodes $C_1, C_2 \dots C_k$

If $\exists C_i \in G_1 : \text{solution subgraph}, 1 \leq i \leq k \Rightarrow C_j \in G_1, 1 \leq j \leq k, j \neq i$

In other words, if a path connecting two nodes in V_g passes through one of the new nodes, it has to pass through all other new nodes between the two original nodes. This rule is to avoid the solution where only parts of the weighted edges in the graph G'_1 are obtained from the reverse mapping function of G_1 . It is not desirable to have this type of solution because in that case G'_1 is not a sub-graph of G' . An example of the reverse graph mapping function is shown in Figure 9.

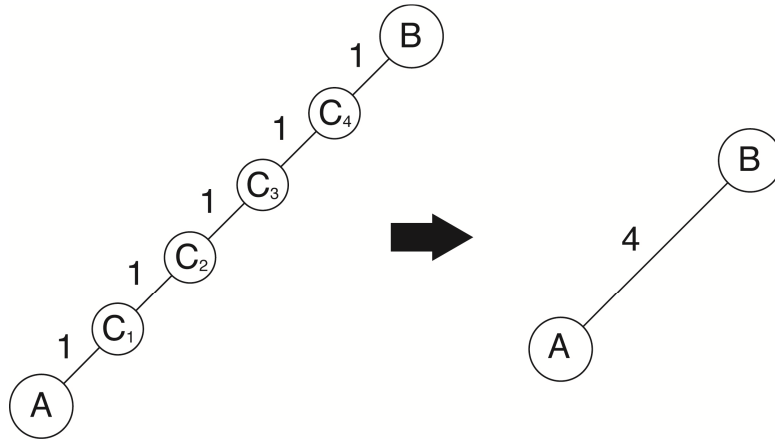


Figure 9 - Reverse graph mapping function

Now, we want to prove that solution sub-graph G'_1 is the solution for Steiner forest problem.

- First, we assume there does not exist a sub-graph G'_1 of G' that satisfies the connection constraint and has a total number nodes at least K' for the Steiner forest problem.

- Hence, there exists another solution graph for the Steiner forest problem with smaller K' . If we transform this solution graph to an unweighted graph using mapping function rule from weighted to unweighted graph as before, we will get an unweighted graph with the total number of nodes smaller than K , the solution for our BROF decision problem.
- This is in contradiction with our assumption since $|V_1| \geq K$.

\Rightarrow Solution sub-graph G_1' is indeed the solution for Steiner forest problem.

Conclusion: BROF decision problem can be verified in polynomial time and is reducible, so it is in NP and it is NP-hard at the same time. In other words, BROF decision problem and its optimization equivalent are NP-Complete problems.

4.3 ILP model

Since the BROF problem is NP-Complete, we use Integer Linear Programming (ILP) approach to solve it. We first give notation of variables in Table 1

Table 1 - Notations

V	set of nodes (routers), each equipped with one or more interfaces card (radio) (We only take into account the radio used for backhaul network)
E	set of feasible transmission link
V_g	Gateway set in the network, a subset of V
λ_{ij}^u	binary variable, when traffic is gateway is rerouted to its backup ONU: $\lambda_{ij}^u = 1$ if there is a flow from node i to node j , 0 otherwise
x_i	binary variable, $x_i = 1$ if we place a backup radio at node i , 0 otherwise

c_i	cost of deploying a backup radio at node i in the network
-------	---

Our objective is to minimize the total deployment cost of backup radio in the network:

$$\min \sum_{i \in V} c_i x_i$$

In order to provide full protection for optical fault-tolerance, each ONU needs to establish a backup path to another ONU, either in the same risk group or in a different risk group depending on the type of failure. As the backup ONU for each ONU is not known in advance, we introduce a pseudo node u' for each gateway u . Pseudo-node u' will be then connected to all other gateway nodes that are different from u to represent a virtual backup ONU for the gateway u . In case the ONU that is connected to gateway u fails, the traffic will be rerouted towards pseudo-node u' through multiple wireless hops. The gateway through which the rerouted traffic passing by before reaching u' is the real backup ONU of u .

Define a new graph constructed from $G = (V, E) : G' = (V', E')$ in which

- $V' = V \cup V'_g$ where we have a mapping function for pseudo-node

$$\begin{aligned} f : V_g &\rightarrow V'_g \\ u &\rightarrow u' \end{aligned}$$

- $E' = (v, u') \cup E$ where $v = V_g \setminus \{u\}$

We can write the constraints formally:

$$\forall u \in V_g : \sum_{i, (u, i) \in E} \lambda_{ui}^u = 1 \quad (1)$$

$$\forall u \in V_g : \sum_{i, (u', i) \in E'} \lambda_{iu'}^u = 1 \quad (2)$$

$$\forall i \neq u, u': \sum_{j, (i, j) \in E} \lambda_{ij}^u = \sum_{j, (i, j) \in E} \lambda_{ji}^u \quad (3)$$

$$x_i \in \{0, 1\} \quad (4)$$

$$\lambda_{ij}^u \in \{0, 1\} \quad (5)$$

$$x_i \geq \lambda_{ij}^u \quad \forall j \quad (6)$$

$$x_i \geq \lambda_{ij}^u \quad \forall j \quad (7)$$

Constraint (1) ensures that there is only one traffic flow leaving from the gateway. This is the rerouted traffic flow in case there is a failure (either gateway/ONU failure or the distribution fiber to the gateway is cut). Constraint (2) makes sure that each pseudo gateway can only have one traffic flow enters as each gateway only requires one backup ONU. Constraint (3) is the flow conservation constraint where the total in-flow equals to the total out-flow at any node different from gateways and pseudo-gateways. We have a different set of constraints from (1) to (3) for each gateway.

Constraints (4) and (5) are conditions for binary variable λ_{ij}^u and x_i . Finally constraint (6) and (7) ensure that at any node that has either an outgoing flow or incoming flow, an additional backup radio will be deployed.

We note that by changing the objective or constraints of the ILP model, we can provide a fault-tolerant network with high throughput and low delay using the throughput-delay ratio presented in [28]. Or, by setting the objective to be the average number of hops of backup paths, we can also minimize service restoration time. However, since our objective is to minimize the total radio deployment cost in the network, we mainly focus on utilizing the wireless resources efficiently. Throughput, delay and restoration time issues are beyond the scope of the thesis.

CHAPTER 5 – Heuristic Algorithms and Performance

Evaluation

Since the computation to solve NP-Complete problems is intensive, the ILP based solution is not scalable. In this chapter, we develop two heuristic algorithms to solve the problem even for large networks.

For each gateway/ONU in the wireless mesh network of WOBAN, the heuristics should select a backup gateway/ONU to protect against any single ONU failure or fiber cut. The main concept of the heuristics is to find a shortest backup path from each gateway to all other gateways at first, and choose nodes that appear in most of the backup paths for placing backup radios. Without loss of generality, the cost can be taken as the total number of nodes.

5.1 Most-Traversed-Node-First (MTNF) heuristic

The Most-Traverse-Node-First heuristic aims to reduce the total number of backup radios by making use of nodes that are traversed the most by all possible backup paths. The input of MTNF algorithm are the known topology matrix E of the network, the total number of nodes (N) in the network and a set of gateways with M elements. Figure 10 gives the details of MTNF algorithm. Shortest paths between each pair of gateways can be easily computed using Dijkstra's algorithm (step 2-4). C_k is the set to store all the nodes that we need to deploy backup radios. For initialization, C_k is set to include the entire gateway set according to our backup radio protection method. $\overline{C_k}$ is the set to store all the candidate nodes for the heuristic to examine whether it should be included in C_k or not. Step 6 to step

12 are the main part of MTNF heuristic. Three conditions for the **while** loop to stop are:

- $k = |V|$: all the nodes in the network have been examined
- $\overline{C}_k = \emptyset$: all of possible candidate nodes have been examined
- $\sum_{i,j} |N_{ij}| = M$: there is only one backup path for each gateway in the

network. The objective is met; so we do not have to continue examining other candidate nodes.

Most-Traversed-Node-First Heuristic

Inputs: topology matrix E , N nodes, M gateways,

Outputs: a subset C_k of nodes where to put backup radio and at least one backup path for each gateway

```

1:  Begin
2:    for  $i = 1$  to  $M$  do
3:      Using Dijkstra's algorithm to find  $N_{ij}$  = set of shortest paths
        from gateway  $i$  to gateway  $j$ , for all  $j \neq i$ 
4:    end for
5:      Set  $k = 0$ ,  $C_k = \{\text{all the gateways}\}$ ,  $\overline{C}_k = \bigcup_{i,j} N_{ij} \setminus C_k$ 
6:    While ( $k \leq |V|$  and  $\overline{C}_k \neq \emptyset$  and  $\sum_{i,j} |N_{ij}| > M$  )
7:      Increase  $k$ 
8:      Find node  $x \in \overline{C}_k$  that used the most in all  $N_{ij}$ 
9:      For all  $N_{ij}$  that ( $x \in N_{ij}$  and  $\sum_j |N_{ij}| > 1$  ) remove all paths
        that don't go through  $x$ 
10:     Update:  $C_k = C_{k-1} \cup x$ ,  $\overline{C}_k = \overline{C}_{k-1} \setminus x$ 
11:     For all  $N_{ij}$  that  $\sum_j |N_{ij}| = 1$  &  $|N_{ij}| = 1$  :
         $C_k = C_k \cup N_{ij}$ ,  $\overline{C}_k = \overline{C}_k \setminus N_{ij}$ 
12:    End While
13:    Deploy additional radios at all nodes in  $C_k$ 
14:  End

```

Figure 10 - MTNF heuristic algorithm

In step 8, among the candidate nodes in $\overline{C_k}$ we find x , the most traversed node in all possible backup paths. The main idea of MTNF is to make use of node x as much as possible. That means that after finding x , we eliminate all the possible backup paths between each pair of gateways that does not use x in step 9. However, when there is only one backup path left for a certain gateway, we do not remove the path from the list even if it does not pass through x . This is to satisfy the connection constraint: each gateway/ONU is always connected to at least one of the other gateways to be fully protected from failure.

In step 10, set C_k gets updated by adding x to the list of nodes that we will deploy backup radio later. Node x is also removed from list so that it will not be examined again. Finally step 11 helps to speed up the MTNF heuristic algorithm. It can be seen that if there is only one backup path exists between two gateways, we have no other choice but to put backup radios at each node along that path to ensure two gateway stay connected. Hence, at the end of each **while** loop, MTFN checks if any gateway has only one backup path, the heuristic then adds every nodes in that path to C_k and at the same time remove them from $\overline{C_k}$.

5.2 Closest-Gateway-First (CGF) heuristic

Closest-Gateway-First (CGF) heuristic algorithm is similar to MTNF. We try to find the common nodes in all the possible backup paths. However, in CGF, we do not search shortest paths between each pair of gateways. Instead, for each gateway we use Dijkstra's algorithm to find all the shortest paths from it to its closest gateway. Therefore, MTNF and CGF are only different in the first phase:

searching for candidate nodes. CGF algorithm is described formally in Figure 11.

The input and output of the algorithms are the same as that of MTNF.

Closest-Gateway-First Heuristic

Inputs: topology matrix E , N nodes, M gateways,

Outputs: a subset C_k of nodes where to put backup radio and at least one backup path for each gateway

```

1:  Begin
2:    for  $i = 1$  to  $M$  do
3:      Using Dijkstra's algorithm to find  $N_i =$  set of shortest paths
      from gateway  $i$  to its CLOSEST gateway
4:    end for
5:      Set  $k = 0$ ,  $C_k = \{\text{all the gateways}\}$ ,  $\overline{C_k} = \bigcup_i N_i \setminus C_k$ 
6:    While ( $k \leq |V|$  and  $\overline{C_k} \neq \emptyset$  and  $\sum_i |N_i| > M$  )
7:      Increase  $k$ 
8:      Find node  $x \in \overline{C_k}$  that used the most in all  $N_i$ 
9:      For all  $N_i$  that ( $x \in N_i$  and  $|N_i| > 1$  ) remove all paths that
      don't go through  $x$ 
10:     Update:  $C_k = C_{k-1} \cup x$ ,  $\overline{C_k} = \overline{C_{k-1}} \setminus x$ 
11:     For all  $N_i$  that  $|N_i| = 1$ :  $C_k = C_k \cup N_i$ ,  $\overline{C_k} = \overline{C_k} \setminus N_i$ 
12:   End While
13:   Deploy additional radios at all nodes in  $C_k$ 
14: End

```

Figure 11 - Closest-Gateway-First heuristic

5.3 Performance Evaluation

We carry out the performance study of the proposed backup radio based protection mechanism for optical fault-tolerance in WOBAN through simulations. The optimization result is obtained through ILOG CPLEX 9.0. Various topologies are used for simulation.

5.3.1 Performance on a small network

In order to illustrate how BROF works, we consider a simple network of 9 nodes with 5 gateways as shown in Figure 12. In the figure, squares represent gateways/ONUs while circles represent mesh routers.

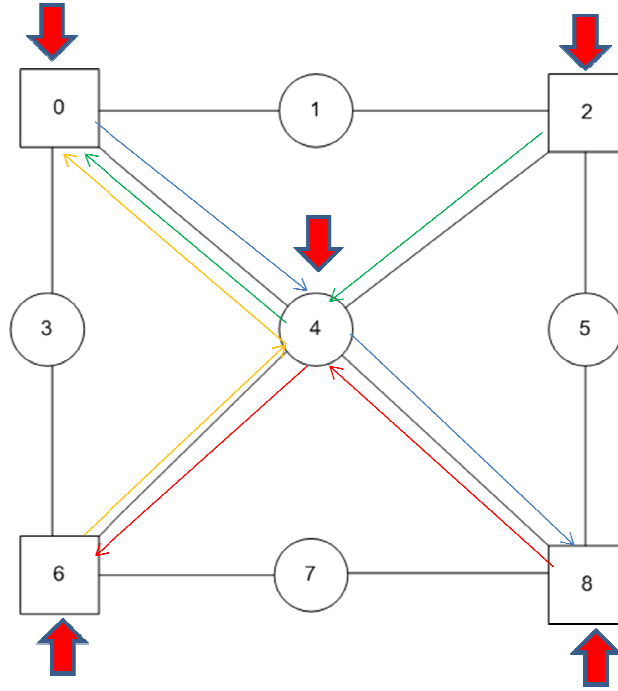


Figure 12 - Simple topology illustration

The optimal total number of backup radios to be deployed is equal to 5 according to the result of the CPLEX program. The four gateways 0, 2, 6, 8 and node 4 are the places we need to put backup radios in order to ensure a full protection against optical network element failures. It is easy to verify that this solution is indeed the optimal solution for our problem. Table 2 shows the backup paths that each gateway will use in the event of a failure.

Table 2 - Backup paths for gateways in the small network

Gateway/ONU	Backup gateway/ONU	Backup path
0	8	0 – 4 – 8
2	0	2 – 4 – 0
6	0	6 – 4 – 0
8	6	8 – 4 – 6

It can be noted that gateway/ONU 0 is used as backup gateway/ONU for both gateway/ONU 2 and 6. This is possible since we only consider single component failure, so gateway 2 and gateway 6 do not fail simultaneously. The same explanation can be applied for node 4 which appears in the backup paths of all the four gateways/ONUs.

We also run MTNF and CGF on this small network and obtained very similar results with an exact radio distribution as in optimal solution. Although the backup paths and backup gateways assignment are different, they do not affect the final result as our objective is to minimize the number of backup radios.

5.3.2 Performance on San Francisco WOBAN

5.3.2.1 Performance comparison

In this section, we are going to compare the performance of our heuristic algorithms on a real WOBAN implementation to the ILP optimal results obtained by CPLEX. Figure 13 shows a part of the city of San Francisco, California, from approximately (N 37°46'43.39'', W 122°26'19.22'' [Golden Gate Avenue and Divisadero Street intersection]) to (N 37°46'51.78'', W 122°25'13.27'' [Golden Gate Avenue and Van Ness Avenue intersection]) and from (N 37° 47'32.57'', W 122°26'28.90'' [Divisadero Street and Pacific Avenue intersection]) to (N 37°47'41.390'', W 122°25'23.71'' [Van Ness Avenue and Pacific Avenue

intersection]) [26]. The wireless part of San Francisco WOBAN (SFNet) consists of 25 mesh routers, among them 5 functioning as gateways (5, 13, 16, 22, and 25) and connecting to the optical back end of WOBAN which is placed at the edges of SFNet. The area over which this SFNet is deployed is about 1mi².

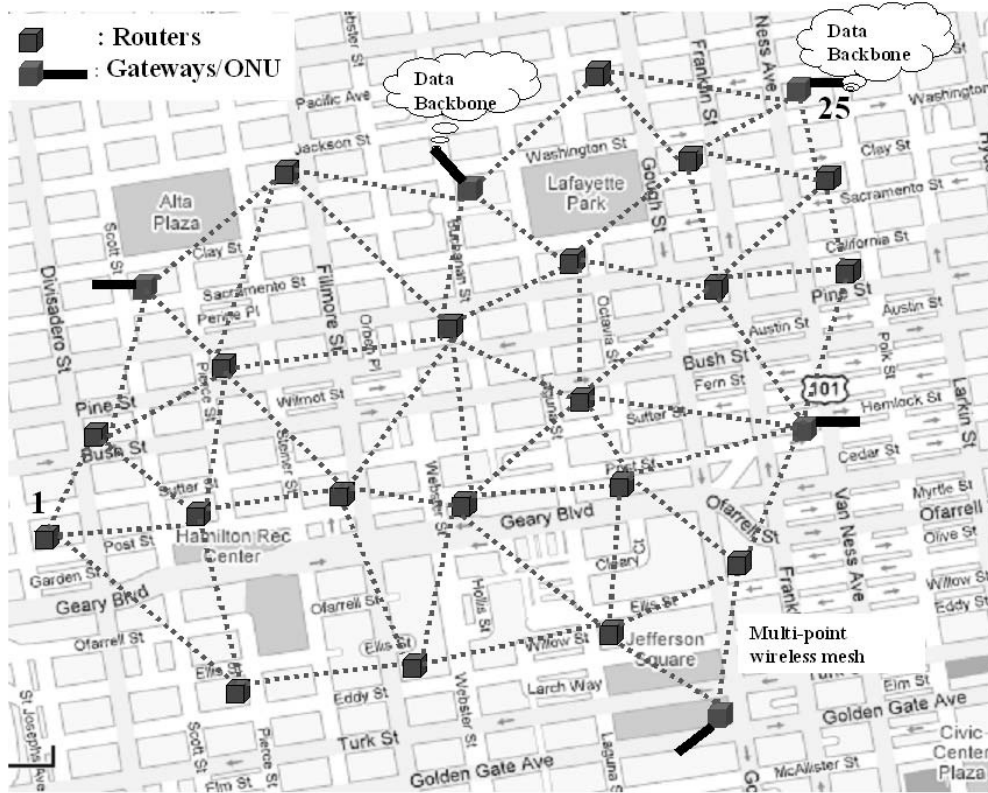


Figure 13 - San Francisco WOBAN architecture

The ILP results obtained by CPLEX on SFNet are shown in Figure 14 and Table 3 – Detailed optimal result for SFNet.

Table 3 – Detailed optimal result for SFNet

Gateway/ONU	Backup gateway/ONU	Backup path
5	13	5 – 9 – 13
13	25	13 – 19 – 25
16	22	16 – 18 – 22
22	16	22 – 18 – 16
25	13	25 – 19 – 13

From the results, we can observe that for a network of 25 nodes with 5 gateways, to provide a full protection against optical network element failures, we only need to deploy a total of 8 backup radios out of which 5 are placed at the 5 gateways and 3 are placed at nodes 9, 18 and 19.

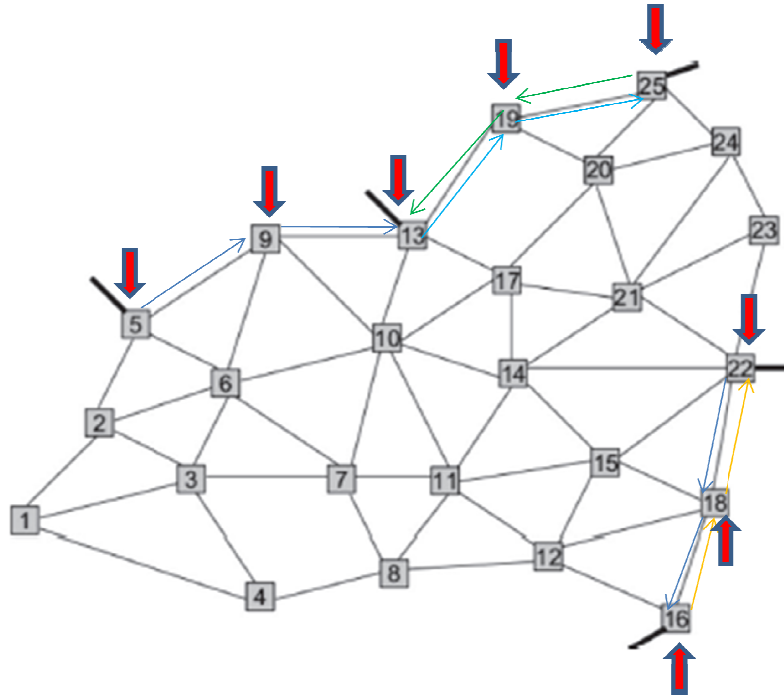


Figure 14 - Optimal results for SFNet

Algorithm CGF gives us a similar result as the optimal solution with the exact radio distribution. However, algorithm CGF uses different backup paths for each gateway. While CGF has a very good performance, MTNF performs not very well. Figure 15 shows the backup radio distribution when we use MTNF on SFNet. The detailed results are shown in Table 4.

Table 4 – Detailed MTNF result for SFNet

Gateway/ONU	Backup gateway/ONU	Backup path
5	16	5 – 6 – 10 – 11 – 12 – 16
13	16	13 – 10 – 11 – 12 – 16
16	5	16 – 12 – 11 – 10 – 6 – 5
22	13	22 – 14 – 10 – 13
25	22	25 – 24 – 23 – 22

For the same network configuration, MTNF requires 12 backup radios (at 5 gateways and 7 additional nodes: 6, 10, 11, 12, 14, 23, 24) compared to 8 in optimal solution.

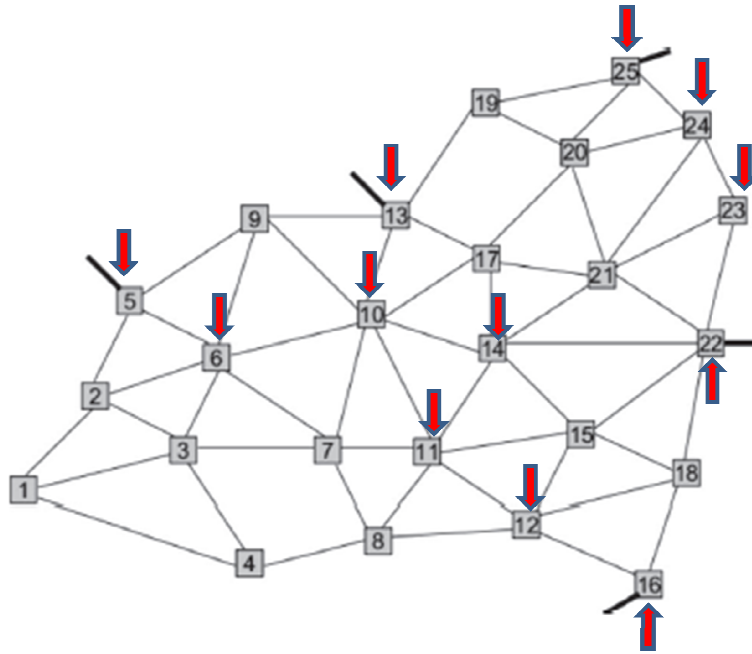


Figure 15 - MTNF result for SFNet

The poor performance of MTNF compared to the optimal result, and CGF can be explained by its method of choosing candidate nodes to place the backup radios. With the small network topology in section 5.3.1, all the three approaches more or less give the same result. However, when the network topology grows larger, MTNF performs poorly. This is due to the fact that MTNF's objective is

trying to maximize the use of most common nodes. Intuitively it sounds very reasonable. But, when from one gateway there are paths with different hop lengths to other gateways, nodes that belong to longer paths will have a higher chance to appear in other possible backup paths because they also belong to longer backup paths of other gateways. This explanation holds true as we can observe in Figure 15. For example, by using MTNF node 10 and node 11 appear the most since most of the long backup paths have to pass through them. When node 10 and node 11 are selected and added to radio deployment set (C_k), all other shorter backup paths that do not traverse node 10 and node 11 are eliminated. This can explain why among all the three approaches, MTNF gives the worst result with highest total number of radios and longer backup paths.

5.3.2.2 Cost analysis

While providing the fault tolerance in the optical access network, our objective is always to minimize the cost. We evaluate the performance of ILP model and two heuristic algorithms in terms of cost. Table 5 - Cost of network components in WOBAN shows the cost of major components involved for WOBAN and PON setup, normalized to the cost of one ONU unit which is taken to be USD 100 as quoted in [4].

Table 5 - Cost of network components in WOBAN

Device	Cost (1 ONU unit)
ONU	1
OLT	50
Fiber (trenching + material + labor and installation)	1000/mile
Wifi AP/Router – single backhaul radio	60
Wifi AP/Router – dual backhaul radio	120
Customer Premise Equipment (CPE)	1

Using the device and fiber layout expenses in Table 5, we obtain the deployment cost of different approaches for our illustrative simple topology and SFNet as shown in Table 6 with the assumption that it is possible to lay fiber between any two points in SFNet.

Table 6 - Deployment cost of different approaches

Approach	Simple topology	SFNet
Traditional PON	n.a	$(1+0.5+0.25+0.25+0.3) \times 1000 = 2300$
Correia's planning	$10 \times 120 = 1200$	$20 \times 120 = 2400$
Feng's approach	n.a	$(0.375 + 0.375 + 0.375) \times 1000 = 1125$
Optimization (BROF)	$5 \times 120 = 600$	$8 \times 120 = 960$
MTNF	600	$12 \times 120 = 1440$
CGF	600	$8 \times 120 = 960$

It can be observed that our protection mechanism using backup radios outperform all other approaches in term of cost. For example, in Figure 16 we can see that the traditional PON protection mechanism by duplicating fiber costs more than twice compared to our method due to high fiber installation cost. Correia's planning method [7] also uses extra radios but its cost is very high. The reason for this would be Correia's planning use too many multi-radio interfaces. In SFNet, while our approach uses only 8 multi-radio interfaces for node with backup capability, Correia's planning method uses up to 20 multi-radio interfaces.

Although Feng's approach [5] costs more than ours, it also has a lower cost than the rest. However, this has some practical difficulties as discussed in Chapter 2. In reality, the cost for deploying a new fiber in downtown San Francisco is prohibitively expensive. Hence, we conclude that our backup radio protection mechanism is the most cost-effective way for providing fault-tolerance.

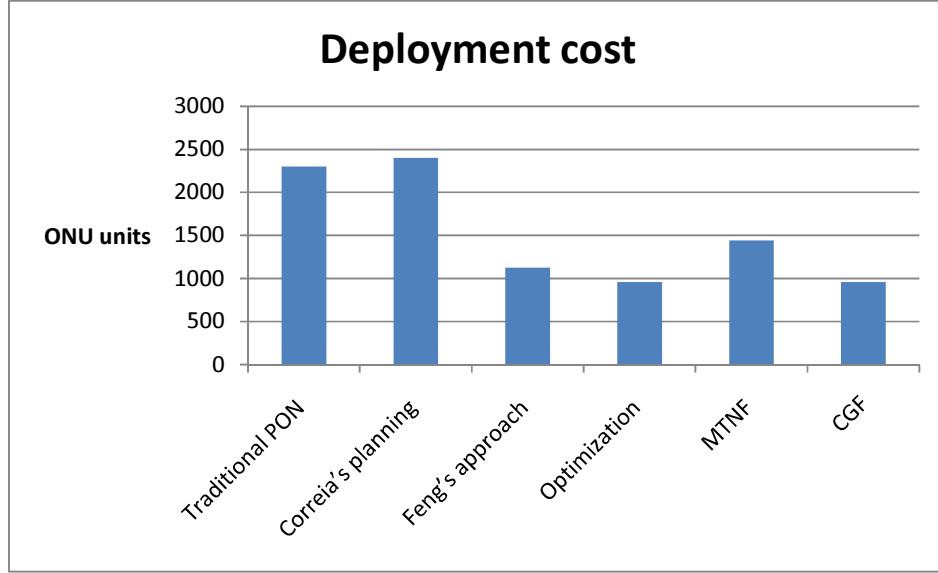


Figure 16 - Cost analysis of various approaches

Further, among the optimal solution (BROF), MTNF and CGF we observe that while CGF has the same cost as the optimal solution, MTNF costs around 1.5 times more. The reason has been discussed in the previous section and this will be verified again for the random networks in the next section.

5.3.3 Performance on random networks

The performance of all the three implementations for our BROF protection mechanism (ILP optimization, MTNF and CGF) has been verified in the previous section. Now, in order to further validate their general performance, we extensively simulate all three of them in randomly generated networks.

5.3.3.1 Graph generation

There are a lot of models available in the literature to generate graphs randomly, among which, Erdős–Rényi (ER), Barabási–Albert (BA) and Watts-Strogatz (WS) are the three most popular models. Choosing the correct model that

can generate graphs which resemble the wireless mesh network frontend of WOBAN is very important.

While ER is a very simple model to create random graphs [29], WS model is more effective in producing graphs with small-world properties, including short average path lengths and high clustering [30]. However both the models cannot describe the realistic characteristic of WOBAN networks where the WMNs are often inhomogeneous in degree, having hubs (such as gateways and ONUs in WOBAN) and a scale-free degree distribution. BA model, on the other hand, can describe such networks better as it has been used extensively in generating graphs for many scale-free networks including computer networks like the Internet, the world wide web, citation networks and some social networks [31].

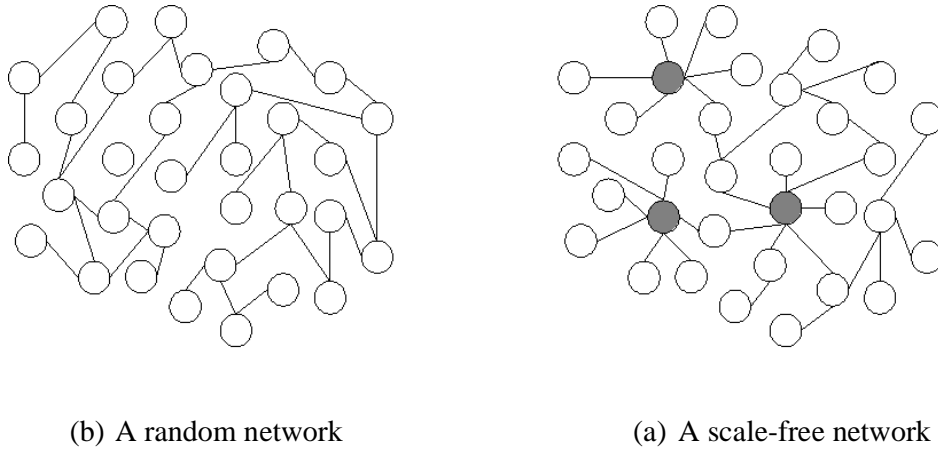


Figure 17 - Differences between a random network and scale-free network

Figure 17 shows the difference between a random network (a) and scale-free network (b). The black dots represent the hub (likely to have the same function as ONU in WOBAN) to interconnect different segments of the network. That allows for fault-tolerant behavior in the event of failures and the network will remain connected by the remaining hubs. This characteristic is very similar to what we

have in WOBAN. The validity of BA model applied in WOBAN will be verified in the simulation.

We use a network generation algorithm provided in [32] which is also based on the BA model. This algorithm can be summarized as follows:

- First we initialize the network with m_0 nodes, where $m_0 > 1$
- Degree of each node in the initial network has to be larger than 0 to avoid being always disconnected
- New nodes are added to the network one at time. Each new node is connected to node i with a probability p_i

$$p_i = \frac{k_i}{\sum_j k_j}$$

where k_i is the degree of node i which follows a power-law distribution:

$$P(k) \sim k^{-\gamma} \text{ with } 2 < \gamma < 3$$

We choose $\gamma=3$ for all the experiments in this work

- When the networks are created, we select gateways randomly among nodes via a random number generator using atmospheric noise [33]. This is better than other computer programs using pseudo-random number algorithms and can give us true random numbers.

5.3.3.2 *Simulation setup*

For each simulation, we set up a set of parameters for both the graph generation and gateway selection phases: $\langle N, M, GATEWAY, min, max, avg \rangle$ in which:

- A degree distribution for N nodes from 0 to $N-1$ taken in $[min, max]$ from a power-law distribution of exponent = 3 and an average = avg .
- A network graph with N nodes and such degree distribution is created using the aforementioned algorithm.
- Among N nodes, choose M gateways randomly and put into *GATEWAY* set.

For each set of parameters, we run 10 times independently with 10 different network graphs and 10 different sets of *GATEWAY* to evaluate all the three approaches. The ratio of the number of total routers (N) and number of gateways (M) in a network is always kept as 5 to 1, unless stated otherwise.

5.3.3.3 *Performance on networks of 100 nodes*

Figure 18 shows the result of three approaches for a network with 100 nodes and parameters set:

$$\langle N, M, GATEWAY, min, max, avg \rangle = \langle 100, 20, GATEWAY, 1, 8, 4 \rangle$$

An observation from the result is that the performance of CGF is very close to the optimal solution obtained by our CPLEX program as in the case of San Francisco WOBAN. On the other hand, although MTNF has similar performance as optimal solution in a few graphs, it requires more backup radios in several cases.

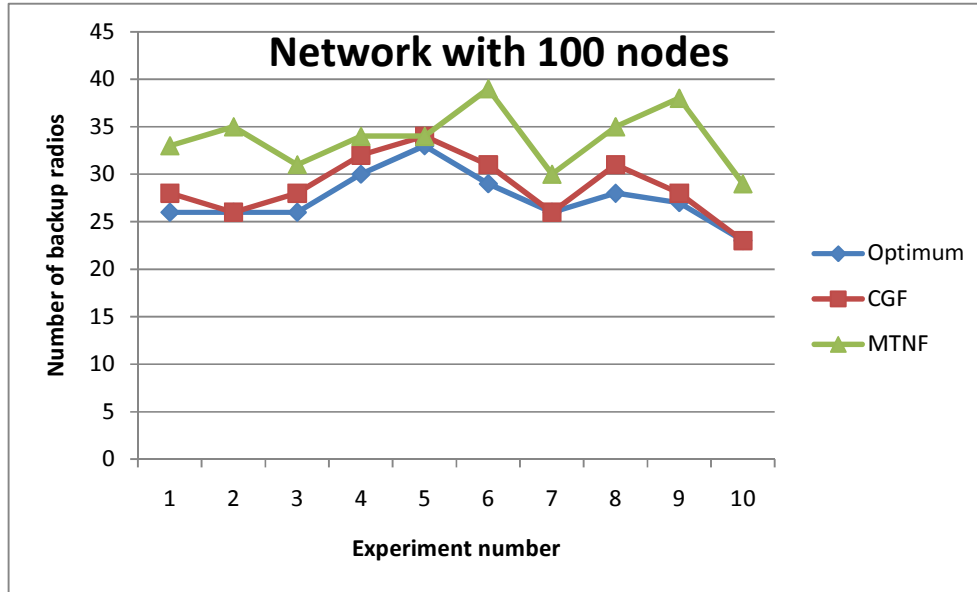


Figure 18 – Results of 10 experiments on networks with 100 nodes

5.3.3.4 Running time

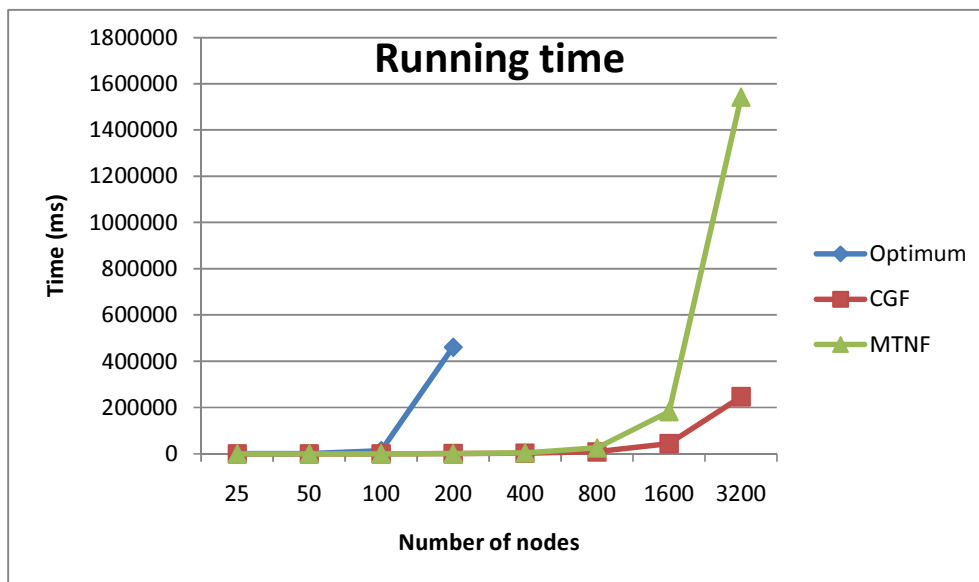


Figure 19 - Running time for different approaches

Figure 19 shows the time it takes to obtain results for ILP optimum, CGF and MTNF on networks with increasing number of nodes. While the difference in running time between the optimization approach and our two heuristics is not

significant in small networks with the total number of nodes less than 100, it becomes a major issue with larger network. For example, in a network of 400 nodes, it takes more than 23 hours to obtain the optimal solution but it only needs less than 2s using CGF or less than 4s using MTNF. Therefore, for larger networks ($N > 100$), we study the performance of heuristic algorithms only.

We can also notice that it takes both CGF and MTNF about the same amount of time with small networks. However when the number of nodes increases, CGF can run much faster. Apparently, the reason would be that CGF only has to search in a much smaller set of possible backup paths than MTNF.

5.3.3.5 Performance comparison of MTNF and CGF

In this part, scale-free networks with 25, 50 and 100 nodes are used to evaluate the heuristic algorithms. We fix the network degree to be from 1 to 8 with average of 4 then generate 10 different networks randomly and random gateway sets.

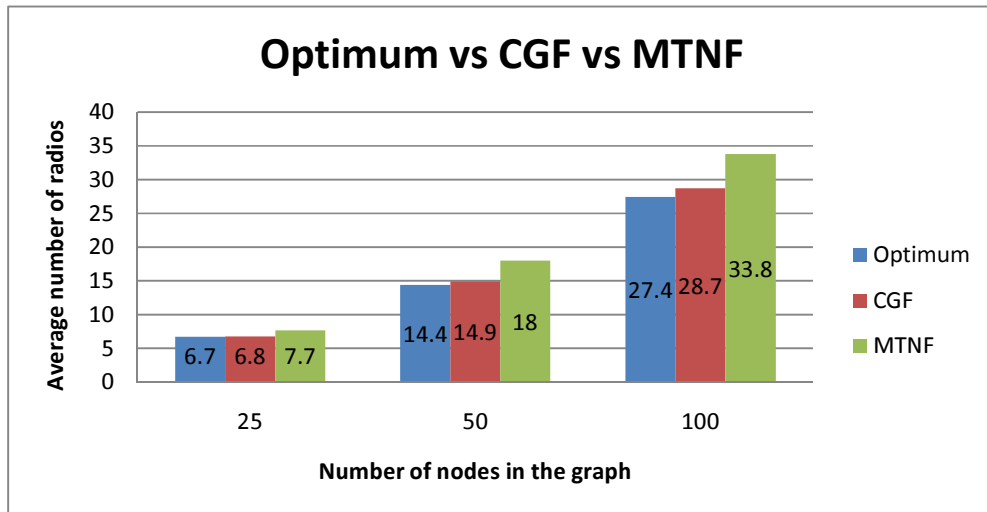


Figure 20 - Performance comparison of three approaches

When the number of network nodes increases, the required number of backup radios also increases as illustrated in Figure 20. In all the three networks, CGF always performs better MTNF and its results are very close to the optimal solution. This can be verified again in Figure 21 with the percentage of performance difference of CGF and MTNF compared to optimal solution. We can define this metric as the difference between the number of backup radios of the heuristic algorithm and the number of backup radios of ILP optimum divided by the number of backup radios of ILP optimum.

We observe that when there are more nodes in the network, the deviation of CGF from the real optimal value also increases. It can be attributed to the fact that with more nodes, it is possible that there exists an optimal group of nodes that do not belong to any possible shortest path. However while the deviation of MTNF is always high (more than 15%), CGF's performance is close to the optimal solution in less than 5%. That can be considered good given the shorter running time of the CGF heuristic.

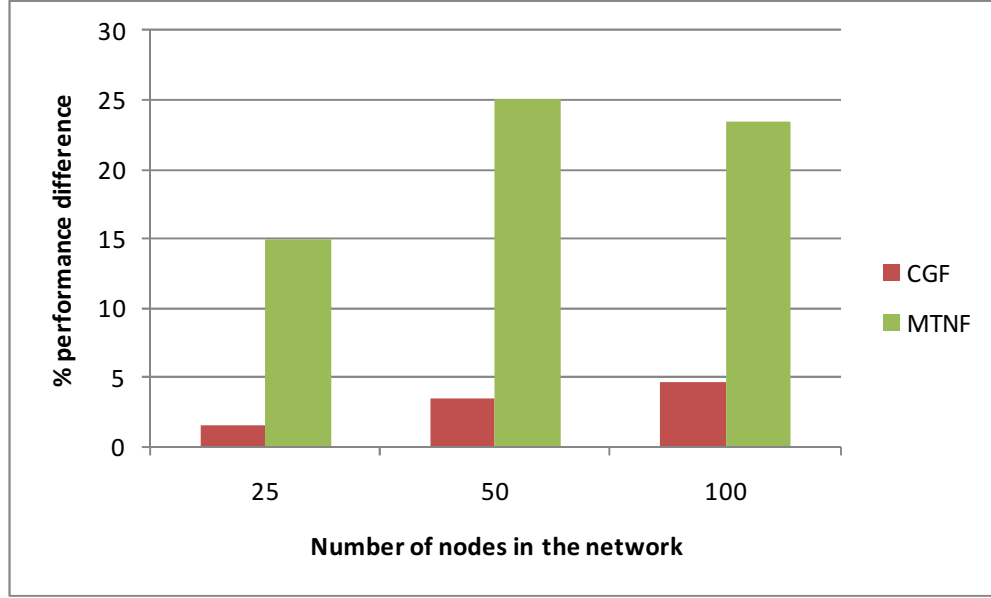


Figure 21 – Percentage of performance difference of CGF and MTNF

5.3.3.6 Performance gap in large networks

For large networks, we evaluate only the heuristic algorithms for the reason of scalability. We have shown that MTNF has poor performance in small networks. Figure 22 also shows that CGF gives better results even in large networks. The same reason stated in the simulation part of SFNet earlier can be used to explain the increasing performance gap between CGF and MTNF as N increases.

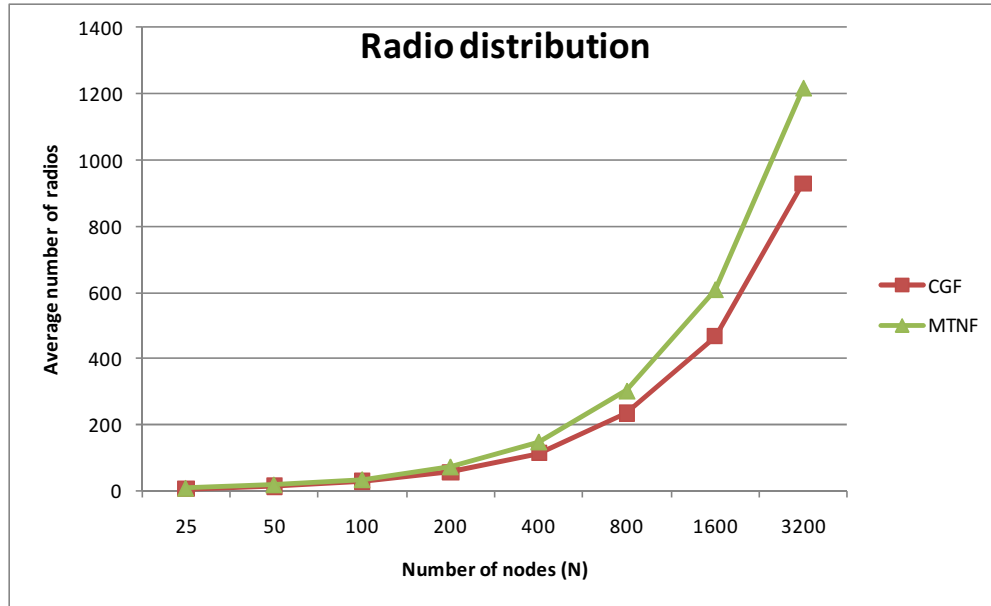


Figure 22 - Performance in large networks

5.3.3.7 Network density

We run the simulation for a network of 50 nodes including 10 gateways with various average node degrees.

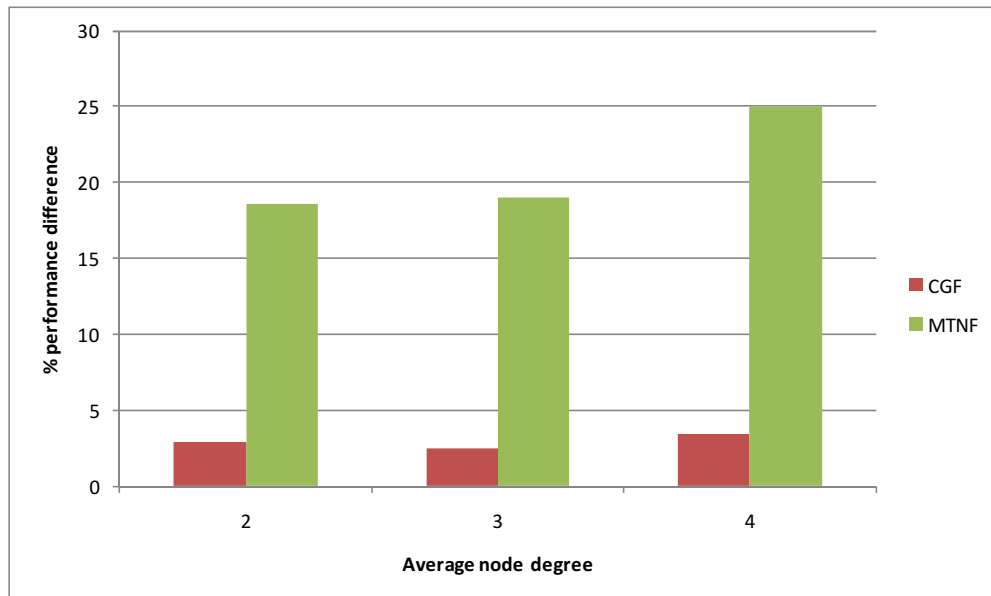


Figure 23 – Percentage of performance difference with various average node degree

We can observe in Figure 23, CGF outperforms MTNF in all cases with different average node degrees. When the node degree increases, both heuristics tend to use more backup radios than the optimal solution. The reason for this can be explained by considering the network density. If the network becomes denser, there will be more possible backup paths between one ONU to another. Hence, the deviation of both heuristics from optimal solution increases. However, similar to previous simulation scenarios, our CGF heuristic is more than 95% close to the optimal results.

5.3.3.8 Delay in backup paths

Another important issue is the delay that may accumulate in the backup path. In a wireless environment like the front end network of WOBAN, this delay is proportional to the number of hops along the routing path. The longer the path, the more the delay packets will experience. By reducing the number of hops that backup traffic must travel before reaching the backup gateway or ONU, we can effectively reduce the delay. Figure 24 shows the average path length of all the backup paths when the number of nodes in the network increases. The result demonstrates the effectiveness of the CGF heuristic with a consistent average path length even when the network becomes very large. An average path length of less than 3 required in most of the networks indicates that the rerouted traffic need to travel at most 3 hops only on the average from its original gateway/ONU before reaching its assigned backup gateway/ONU.

By observing Figure 24, we can also reach a conclusion that our choice of Barabási–Albert model for generating scale-free networks is valid. In section 5.3.2, we have seen the San Francisco WOBAN implementation – with all the

gateways are deployed only 2 or 3 hops away from another gateway. The simulation in this section again validates that even when the number of nodes increases to 3200 and all the gateway sets are selected randomly, BA model distributes gateways in a very similar way to real WOBAN implementations.

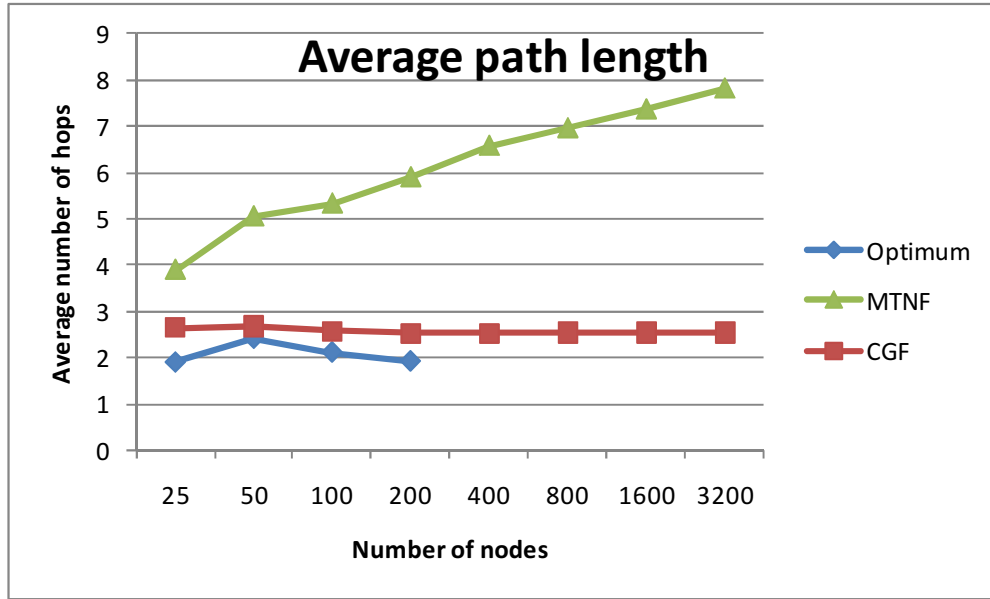


Figure 24 - Average path length for backup routes

5.3.4 A special case

In all the simulation cases presented in section 5.3.2 and 5.3.3, the CGF heuristic always outperforms the MTNF heuristic not only in terms of cost (number of radios), but also in term of delay and running time. The reason for this is attributed to the way CGF and MTNF choose their list of candidate nodes to put backup radios. Indeed, there is some specific scenarios in which MTNF has better performance than CGF as shown in Figure 25.

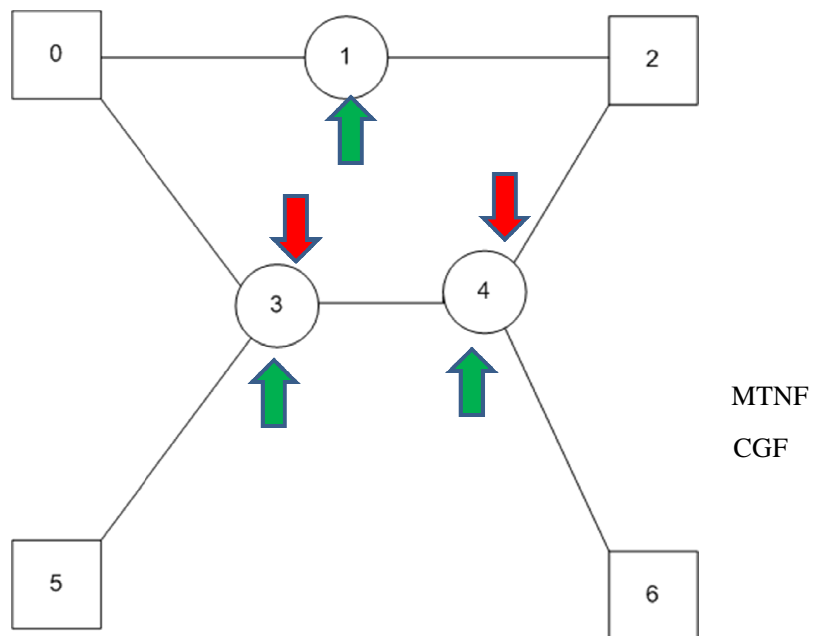


Figure 25 – Special case when MTNF outperforms CGF

Figure 25 represents a part of the WMN front end of WOBAN where we have 7 mesh routers, among which there are 4 gateways (node 0, 2, 5 and 6). In addition to 4 backup radios that have to be deployed at 4 gateways, MTNF only requires 2 additional backup radios while CGF needs 3. However, this is only one of the very few cases that MTNF has a slightly better performance than CGF. All our extensive simulations confirm that CGF is more effective in most of the scenarios than MTNF.

CHAPTER 6- Conclusions

Bandwidth demand continues to grow rapidly due to the ever-increasing rich-media applications and technology-savvy users. Thus, WOBAN is a promising architecture for last-mile access networks to bring operational efficiencies and sufficient bandwidth to end users. To ensure the functioning of the critical applications in WOBAN and to provide user satisfaction with high service availability, this thesis has developed a new scheme to protect the WOBAN against both fiber cuts and network element failures.

The basic idea is to provide extra capacity for wireless nodes in the front end network of WOBAN to create a dedicated backup channel that can be activated when optical component failures happen. By assigning backup radios to all the gateways/ONUs and a few selected wireless routers, we can provide full traffic protection against optical failures while minimizing the deployment cost. Each gateway/ONU is associated with another gateway/ONU termed as backup gateway/ONU. In the event of a failure, the entire failed traffic is rerouted to the pre-assigned backup gateway/ONU. Compared to the existing protection methods and particularly the PON protection architectures, our proposed scheme is cost-effective providing full protection guaranteed. By using a dedicated channel, the proposed scheme achieves fast failure recovery.

We proved that our backup radio placement for optical fault-tolerance (BROF) problem is NP-complete. In addition to developing an ILP formulation to solve BROF, we also developed two heuristic algorithms called CGF and MTNF. Although MTNF has better performance than CGF in some special cases, in

general CGF has performance closer to the optimal solution. We demonstrated the effectiveness of the proposed scheme and heuristic algorithms by numerical results obtained by solving ILP formulation using CPLEX and simulations on real networks and random networks.

The following issues remain open for future investigation:

- As we deploy backup radios on existing nodes of the network and using orthogonal channels, signal interference is not an issue. However, in some cases if the path between a gateway/ONU and its backup gateway/ONU traverses many hops, we can place additional nodes to connect them directly. Choosing such additional nodes would not be straightforward because frequency assignment and bandwidth allocation must be taken into account to avoid interference. Possible solutions are employing a dynamic frequency assignment algorithm or making use of unoccupied orthogonal frequencies in WiMax for additional nodes. This challenging problem requires further study and investigation.
- Although the proposed protection scheme ensures full protection for optical access network, backup wireless resource is not utilized efficiently as they are not activated when there is no failure. A study can be carried out to make use of the backup radios for primary traffic. If we want to ensure full protection, we can set a rule such that primary traffic on those backup channels can be preempted if failure happens. Otherwise by dynamically assigning bandwidth for backup channels, we can define a resilience differentiation scheme for the backend network of WOBAN.

LIST OF PUBLICATIONS

H.N. Truong and M. Gurusamy, “Backup Radio Placement for Optical Fault Tolerance in Hybrid Wireless-Optical Broadband Access Networks”, to be submitted to *IEEE/OSA Journal of Lightwave Technology*, 2010

REFERENCES

- [1] C. F. Lam, *Passive Optical Networks: Principles and Practice*. San Diego, California: Elsevier, 2007.
- [2] G. Maier, *et al.*, "Design and cost performance of the multistage WDM-PON access networks," *Journal of Lightwave Technology*, vol. 18, pp. 125-143, Feb. 2000.
- [3] "IEEE Standard for Local and Metropolitan Area Networks Part 16: Air Interface for Fixed Broadband Access Systems, IEEE Std 802.16-2004," ed, 2004.
- [4] S. Sarkar, *et al.*, "Hybrid wireless-optical broadband access network (WOBAN): network planning and setup," *Selected Areas in Communications, IEEE Journal on* vol. 226, pp. 12-21, Aug. 2008.
- [5] T. Feng and L. Ruan, "Design of Survivable Hybrid Wireless-Optical Broadband-Access Network," presented at the IEEE International Conference on Communications, 2009. ICC '09., Dresden 14-18 June 2009
- [6] A.J.Vernon and J.D.Portier, "Protection of optical channels in all-optical networks," in *18th Annual National Fiber Optic Engineers Conference*, September 2002, pp. 1695–1706.
- [7] N. Correia, *et al.*, "Fault-Tolerance Planning in Multiradio Hybrid Wireless-Optical Broadband Access Networks," *IEEE/OSA Journal of Optical Communications and Networking*, vol. 1, pp. 645-654, December 2009
- [8] "Broadband optical access systems based on Passive Optical Networks (PON)," in *ITU-T Recommendation G.983.1*, ed, 1998.
- [9] D. J. Xu, *et al.*, "Proposal of a new protection mechanism for ATM PON interface," presented at the International Conference on Communications (ICC), Helsinki, Finland, 2001.
- [10] W. T. P'ng, *et al.*, "A novel protection scheme for Ethernet PON FTTH access network," presented at the International Conference on Networks, Malaysia, Nov. 2005.
- [11] M. K. Abdullah, *et al.*, "FTTH access network protection using a switch," presented at the Asia Pacific Conference on Communications (APCC), Penang, Malaysia, 2003.

- [12] A. J. Philips, *et al.*, "Redundancy strategies for a high splitting optically amplified passive optical network," *IEEE/OSA J. Lightwave Technol.*, vol. 19, pp. 137-149, 2001.
- [13] N. Nadarajah, *et al.*, "Protection switching and local area network emulation in passive optical networks," *IEEE/OSA J. Lightwave Technol.*, vol. 24, pp. 1955-1967, 2006.
- [14] N. Nadarajah, *et al.*, "Self-protected Ethernet passive optical networks using coarse wavelength division multiplexed transmission," *IEE Elect. Lett.*, vol. 41, pp. 866-867, 2005.
- [15] I. F. Akyildiz, *et al.*, "Wireless mesh networks: a survey," *Computer Networks* pp. 445-487, 2005.
- [16] S. Sarkar, *et al.*, "RADAR: Risk-and-Delay Aware Routing Algorithm in a Hybrid Wireless-Optical Broadband Access Network (WOBAN)," presented at the Optical Fiber Communication and the National Fiber Optic Engineers Conference, Anaheim, CA 25-29 March 2007
- [17] A. Reaz, *et al.*, "Hybrid Wireless-Optical Broadband Access Network (WOBAN): Capacity Enhancement for Wireless Access," presented at the Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. , Nov. 30 2008-Dec. 4 2008
- [18] Z. Yubin, *et al.*, "Wireless protection switching for video service in wireless-optical broadband access network," in *2nd IEEE International Conference on Broadband Network & Multimedia Technology*, Beijing 18-20 Oct. 2009 pp. 760-764.
- [19] A. Reaz, *et al.*, "CaDAR: An Efficient Routing Algorithm for a Wireless-Optical Broadband Access Network (WOBAN)," *IEEE/OSA Journal of Optical Communications and Networking*, vol. 1, pp. 392-403, Oct. 2009
- [20] Y. Zhang, *et al.*, *Wireless Mesh Networking: Architectures, Protocols and Standards*: Auerbach Publications, 2007.
- [21] I. F. Akyildiz and X. Wang, *Wireless Mesh Network*, 1st ed.: Wiley, 2009.
- [22] IEEE, "IEEE 802.11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," ed, 2007.
- [23] <http://www.belairnetworks.com/>.
- [24] <http://www.tropos.com>.
- [25] <http://www.cisco.com/>.

- [26] S. Sarkar, *et al.*, "A novel delay-aware routing algorithm (DARA) for a hybrid wireless-optical broadband access network (WOBAN)," *IEEE Networks*, vol. 22, pp. 20-28, May/June 2008.
- [27] C. W. Duin and A. Volgenant, "Some generalizations of the steiner problem in graphs," *Networks*, vol. 17, pp. 353-364, 1987.
- [28] C. Kolias and L. Kleinrock, "The power function as a performance and comparison measure for ATM switches," in *IEEE Globecom*,, Sydney, Australia, Nov. 1998, pp. 381-396.
- [29] P. Erdos and A. Renyi, "On the evolution of random graphs," *Publ. Math. Inst. Hung. Acad. Sci*, vol. 5, pp. 17-61, 1960.
- [30] D. J. Watts and S. H. Strogatz, "Collective dynamics of 'small-world' networks," *Nature*, pp. 440-442, 1998.
- [31] R. Albert and A.-L. Barabási, "Statistical mechanics of complex networks," *Reviews of Modern Physics* vol. 74, pp. 47-97, 2002.
- [32] F. Viger and M. Latapy, "Efficient and simple generation of random simple connected graphs with prescribed degree sequence," presented at the Computing and Combinatorics Conference, COCOON'05, Kunming, Yunnan, 2005.
- [33] <http://www.random.org>