SECURING PASSIVE OPTICAL NETWORK AGAINST SIGNAL INJECTION ATTACK

SALIM MOHAMMED ABDULLAH AL-HINAI

A project report submitted in partial fulfilment of the
requirements for the award of the degree of
Master of Engineering (Electronics and Telecommunications)

School of Electrical Engineering
Faculty of Engineering
Universiti Teknologi Malaysia

JANUARY 2019

DEDICATION

This project report is dedicated to my family especially my parents, and wife.

It is also dedicated to my supervisor, who guides me to achieve the target.

Thank You for Your Endless Support!

ACKNOWLEDGEMENT

I wish to express my sincere appreciation to all those who have helped me in various way, to complete this thesis. First and foremost, I thank God almighty who provided me with strength, direction and showered me with blessings throughout. My sincerest gratitude to my supervisor Assoc. Prof. Dr. Nadiatulhuda Zulkifli for her continuous guidance, encouragement and motivation.

I also recognized Universiti Teknologi Malaysia (UTM) for the facilities in the faculty and library which help me a lot in completing my thesis.

My fellow postgraduate class mates should also be recognized for their support. My sincere appreciation also extends to all my colleagues and others who have provided assistance at various occasions. Their views and tips are useful indeed. Unfortunately, it is not possible to list all of them in this limited space. I am grateful to all my family members.

ABSTRACT

Passive Optical Network (PON) is a promising solution to the last-mile problem in access networks. Security is a very crucial aspect to be considered especially in the current environments that are characterized by much larger data transport capacity. Moreover, securing the physical layer requires urgent attention as it will become more critical in future PON that has much longer distance with the involvement of more users. Thus, it is vulnerable to a variety of attacks, including denial of service (DoS) which jams a network, eavesdropping and masquerade. DoS attack can take place when a continuous upstream signal is transmitted from Optical Network Unit (ONU) to Optical Line Terminal (OLT) with high enough power, causing the OLT to receive the data with high bit error rate. This research proposes a method to secure PON from high power injection attack. The solution is based on the idea of deploying an optical attenuator in the upstream communication towards the splitter to prevent any high signal power injection attack and restrict it up to an acceptable power level. One of the most important benefits of the proposed work is its straightforward implementation in the existing GPON network with minimum cost and effort. The GPON network under studied that focuses on the upstream communication based on standard ITU-T G.984 (data rate of 1.25 Gbps) examined the effects of varied optical fiber distances and number of ONUs. The performance of the proposed method is evaluated using Optisystem to determine the feasibility of the concept. Findings from the simulation results revealed that the optical attenuator compensated the jamming degradation attack up to eight ONUs and maximum distance of 20 km. The proposed system design also found that the method has limitation to reduce the attack at higher ONU numbers e.g. 16 and 32 due to high insertion loss. The overall performance confirms that this method is useful to protect the GPON system and minimize the high power for low insertion loss power splitter.

ABSTRAK

Rangkaian Optik Pasif (PON) merupakan penyelesaian berpotensi kepada masalah batu-terakhir dalam rangkaian akses. Keselamatan adalah aspek yang sangat penting untuk dipertimbangkan terutamanya dalam persekitaran semasa yang dicirikan oleh kapasiti pengangkutan data yang lebih besar. Lebih-lebih lagi, lapisan fizikal yang memerlukan perhatian segera kerana ia akan menjadi lebih kritikal pada PON masa hadapan yang melibatkan jarak lebih jauh dan lebih ramai pengguna. Oleh itu, ia terdedah kepada pelbagai serangan, termasuk penafian perkhidmatan (DoS) yang meresapi rangkaian, pengintipan dan penyamaran. Serangan DoS boleh berlaku apabila isyarat hulu berterusan dihantar dari Unit Rangkaian Optik (ONU) ke Terminal Talian Optik (OLT) dengan kuasa yang cukup tinggi, menyebabkan OLT menerima data dengan kadar ralat bit yang tinggi. Penyelidikan ini mencadangkan kaedah untuk menjamin PON daripada serangan suntikan kuasa tinggi. Penyelesaian ini adalah berdasarkan idea yang menggerakkan pelemah optik dalam komunikasi huluan ke arah pembahagi untuk mengelakkan sebarang serangan suntikan kuasa isyarat tinggi dan menyekatnya ke tahap kuasa yang boleh diterima. Salah satu faedah yang paling penting dalam penyelesaian yang dicadangkan adalah pelaksanaannya yang jelas dalam rangkaian GPON yang sedia ada dengan kos dan usaha yang minimum. Rangkaian GPON yang dipelajari memberi tumpuan kepada komunikasi hulu berdasarkan standard ITU-T G.984 (kadar data 1.25 Gbps) dengan mengambilkira kesan pelbagai jarak gentian optik dan bilangan ONUs. Prestasi kaedah yang dicadangkan dinilai dengan menggunakan Optisystem untuk menguji perlaksanaan konsep tersebut. Penemuan dari keputusan simulasi menunjukkan bahawa penguat optik mampu untuk menghadapi serangan kemerosotan signal kualiti sehingga lapan ONUs dan jarak maksimum 20 km. Reka bentuk sistem yang dicadangkan juga mendapati bahawa kaedah yang dicadangkan mempunyai had untuk mengurangkan serangan bagi nombor ONU yang lebih tinggi, misalnya 16 dan 32 kerana kehilangan kuasa pembahagi kuasa yang tinggi. Prestasi keseluruhan mengesahkan bahawa kaedah ini berguna untuk melindungi sistem GPON dan meminimumkan serangan tinggi kuasa untuk kes kehilangan kuasa pembahagi yang rendah.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AAA	-	Authentication Authorization Accounting
AES	-	Advanced Encryption Standard
APD	-	Avalanched Photo Detector
APON	-	ATM Passive Optical Network
ATB	-	Access Terminal Box
APD	-	Avalanched Photo Detector
BER	-	Bit Error Rate
BPON	-	Broadband Passive Optical Network
BRAS	-	Broadband Remote Access Server
CATV	-	Cable TV
CO	-	Central office
CW	-	Continuous Wave
dB	-	Decibel
CATV	-	Community Access Television
DoS	-	Denial of Service
DS	-	Downstream
EDFA	-	Erbium Doped Fiber Amplifier
EPON	-	Ethernet Passive Optical Network
FAT	-	Fiber Access Terminal
FDT	-	Feeder Disruption Terminal
FSAN	-	Full Service Access Network
FTTB	-	Fiber to the Building
FTTdp	-	Fiber to the Distribution Point
FTTH	-	Fiber to the Home
FTTM	-	Fiber to the Mobile
FTTO	-	Fiber to the Office
Gbps	-	Gigabits per Second
GPON	-	Gigabits Passive Optical Network
GUI	-	Graphical User Interface
HFC	-	Hybrid Fiber Coaxial

IEEE	-	Institute of Electrical and Electronics Engineers
ISP	-	Internet Service Provider
ITU	-	International Telecommunication Union
KM	-	Kilometer
MAC	-	Media Access Controller
MZM	-	Mach-Zehnder Modulator
Nm	-	Nano meter
NG-PON	-	Next Generation Passive Optical Network
NRZ	-	Non Return to Zero
OCDMA	-	Optical Code Division Multiple Access
ODF	-	Optical Distribution Frame
ODN	-	Optical Distribution Network
OFDM	-	Orthogonal Frequency Division Multiplexing
OLT	-	Optical Line Terminal
ONU	-	Optical Network Unit
ONT	-	Optical Network Terminal
OOK	-	On – off keying
OTDM	-	Optical Time Division Multiplexing
OTDR	-	Optical Time Domain Reflectometer
PLOAM	-	Physical Layer Operation, Administration and Maintenance
PD	-	Photodiode
PON	-	Passive Optical Network
PRBS	-	Pseudo-Random bit sequence
PSTN	-	Public Switch Telephone Network
QoS	-	Quality of Service
RTT	-	Round Trip Time
SMF	-	Single Mode Fiber
SFP	-	Small Form-Factor Pluggable
TB	-	Terminal Box
T-CONT	-	Transmission Container
TCP	-	Transmission Control Protocol
TDM	-	Time Division Multiplexing
TDMA	-	Time Division Multiple Access

US	-	Upstream
VDC	-	Voltage Direct Current
VOA	-	Variable Optical Attenuator
OTDM	-	Wavelength Division Multiplexer
WJ	-	With Jamming
WOA	-	With Optical Attenuator
WOJ	-	Without Jamming
XOR	-	Exclusive OR Gate

LIST OF SYMBOLS

B	-	Bit Data Rate
I	-	Sequence of Channel
N	-	Total Number of Channel
P_b	-	Power Budget
PT_{in}	-	Transmitted Power
PR_{min}	-	Minimum Receiver Sensitivity
P_o	-	Received Optical Power
P_M	-	Power Margin
C_l	-	Channel Losses
JPT_{in}	-	Jamming Power
$MaxPT_{in}$	-	Max Range of ONU Transmitted Power

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Overview

Nowadays, most high-speed optical access network operate base on in Passive Optical Network (PON) technology which is a promising solution to the last-mile problem in the access networks as shown below in Figure 1.1. The optical fiber network offers a higher capacity to the subscribers compared to other access technologies such as coaxial, copper or hybrid fiber-coaxial (HFC). PONs are widely implemented due to the absence of the active devices in Optical Distribution Network (ODN). The subscribers use device called Optical Network Units (ONUs). Meanwhile, another device called Optical Line Termination (OLT) is located in the central office and is operated by service provider.

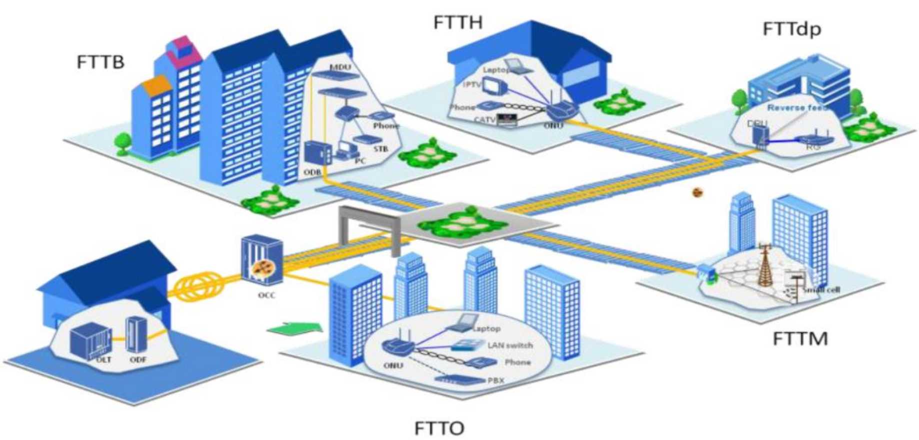


Figure 1.1 Scenarios of XG-PON1 with GPON [1]

Similar to other access network technologies, security is a very crucial aspect to be considered especially in the modern communication networks that are distinguished by large amount of data and high speeds. Moreover, securing the physical layer issues need urgent attention as it will become more critical in future PON that has much longer distance with the involvement of more users. One of the critical issues is the ONU users can intercept the data that sent to other ONUs due to the broadcasting mechanism in Time Division Multiplexing – Gigabit Passive Optical Network (TDM-GPON) as shown in Figure 1.2.

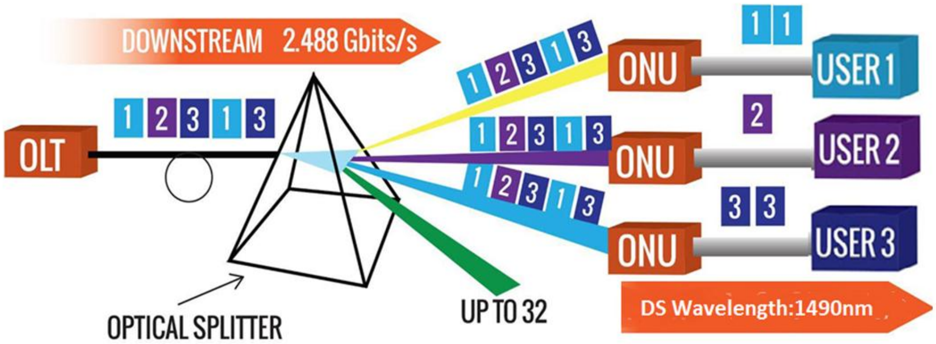


Figure 1.2 Broadcasting mechanisms in TDM-GPON [2]

Furthermore, in the current PON implementation, security requirements such as authentication and encryption are optional and, in the downstream communication from OLT to ONU, the secret encryption key is sent as sent as plain texts according to the ITU-T G.984 standard [3]. Meanwhile, the upstream communication link from ONU to OLT is not encrypted, and it is vulnerable to a variety of attacks, including denial of service (DoS) which jams a network, eavesdropping and masquerade that is also known as reply attack. Moreover, DoS attack can take place when a continuously transmitting upstream signal with high enough power at an Optical Network Unit (ONU) is injected to block all other ONUs from getting their data as illustrated in Figure 1.3 [4]. Furthermore, the attacker can exploit any reflection signal from the ODN splitter to eavesdrop the data of victim ONU [5]. Therefore, malicious in the upstream channel is difficult to identify due to passive nature elements in the optical network.

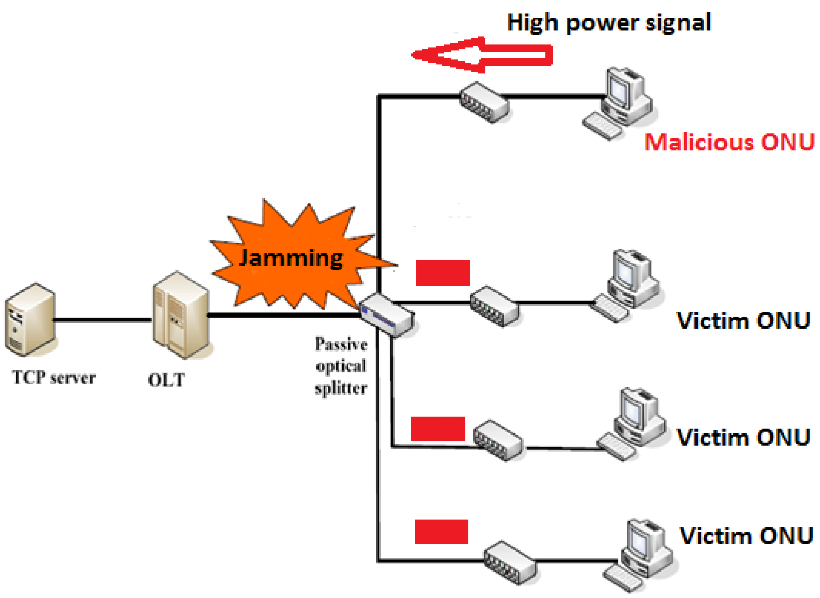


Figure 1.3 Scenario denial of service attack [4]

Based on the fact, this research aims to investigate the security issues and weaknesses in PON and to enhance the network security by deploying a passive device called optical attenuator in the upstream directions towards the splitter that thwart high power signal attack. By using a passive optical attenuator, the injection of higher power signal can be restricted up to an acceptable power level without any denial of service (DoS). The vest of this chapter describes the overview of the problem statements, objectives, the scope of work, work schedule and thesis outline.

1.2 Problem Statement

Passive optical networks come up with the standard security for data encryption, authentication, and key establishment. In the physical layer of the GPON, the upstream transitions from ONU to OLT are vulnerable to several attacks, including denial of service (DoS) which jams a network and prevent communication in a specific link. Therefore, Dos happens when an attacker injects a continuously signal with high power at a particular wavelength into the fiber to prevent other ONUs from getting their data and degrading the service. It is more serious for in-band jamming attack which occurs when the jamming wavelength is similar to the legitimate frequency. However, an out-of-band jamming attack can also degrade the quality or even denial the service of legitimate signal due to injection of high power wavelength that had a different frequency from the legitimate signal and cause the denial of service due to the inter crosstalk and adjacent channels. Therefore, both attacks can jam the network and degrade the performance of the signal.

1.3 Objectives

The objectives of this research are:

1- To investigate the security issues and weaknesses in the physical layer of the GPON.
2- To simulate the deployment of a passive optical attenuator in the GPON in an upstream direction towards the splitter to prevent any high power signal injection attack.
3- To evaluate the feasibility and transmission performance of the proposed design.

1.4 Scope of Work

The scope of this research concentrates on three parts:

1. Simulation:
    - The design and simulation of the GPON system based on TDM.
    - The simulation tool that used to achieve the objectives is optisystem software.
2. System Parameters:
    - ONU transmitted power range 0-5 dBm.
    - Upstream wavelength 1310nm with the data rate 1.25 Gbps.
    - Continuous wave attacker signal.
    - Distance: 1 km, 10 km, 20 km, and 30 km.
    - Receiver sensitivity -28 dBm.

3. Result Analysis:

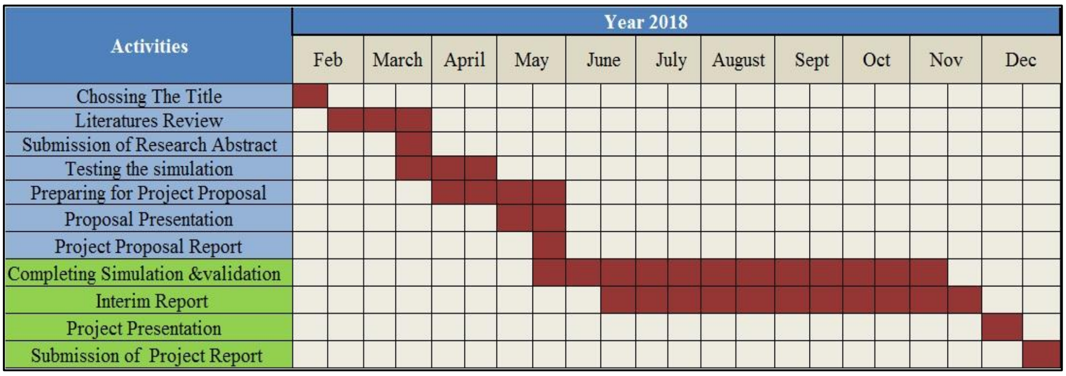
   - Evaluate correctness of GPON operation and evaluate the feasibility of an optical attenuator.
   - Assess signal quality through BER and Q-factor.

1.5 Research Methodology

1.5.1 Work Schedule

- Research planning and schedule (Gantt chart)

Table 1.1 Project Schedule



1.6 Thesis Outlines

The project report comprises five chapters which describe the overall project progress and implementation. Each section discusses the different topics related to this project.

Chapter 1 briefly introduces an overview of this project, problem statement, objectives, the scope of work, research methodology and report outlines.

Chapter 2 discusses the literature review on the study of this project. It will include the GPON architecture. Besides that, it introduces the various types of attack, threats, and weakness in GPON. Lastly, review of the previous work which relates to this project is provided.

Chapter 3 focuses on the methodology used throughout this project and presents the design and simulation based on OTDM- GPON architecture for different models. The simulation tool that will be used to achieve the objectives is Optisystem software.

Chapter 4 discusses the evaluation and the results of the proposed system's security and transmission performances parameters for other models. The performance parameter involves Eye diagram, Q factor, and BER and power budget.

Chapter 5 focuses on the conclusion of the whole project and recommendations for future development are given to enhance the security in PON.

REFERENCES

1. "XG-PON1 Solution Increases QoE and Enhance competitiveness - ZTE Corporation," *Flexible Displays in the Future - ZTE Corporation*. [Online]. Available: http://wwwen.zte.com.cn/en/solutions/access/201405/t20140520_424068.html. [Accessed: 04-April-2018].
2. "How GPON Works," *Gigabyte Passive Optical Network (GPON)*. [Online]. Available: http://www.gpon.com/how-gpon-works. [Accessed: 04-April-2018].
3. L. Malina, P. Munster, J. Hajny and T. Horvath, "Towards secure Gigabit Passive Optical Networks: Signal propagation based key establishment," *2015 12th International Joint Conference on e-Business and Telecommunications (ICETE)*, Colmar, 2015, pp. 349-354.
4. S. Drakulic, M. Tornatore and G. Verticale, "Degradation attacks on Passive Optical Networks," *2012 16th International Conference on Optical Network Design and Modelling (ONDM)*, Colchester, 2012, pp. 1-6
5. D. Gutierrez, J. Cho and L. G. Kazovsky, "TDM-PON Security Issues: Upstream Encryption is Needed," *OFC/NFOEC 2007 - 2007 Conference on Optical Fiber Communication and the National Fiber Optic Engineers Conference*, Anaheim, CA, 2007, pp. 1-3
6. M. P. Fok, Z. Wang, Y. Deng and P. R. Prucnal, "Optical Layer Security in Fiber-Optic Networks," in *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 725-736, Sept. 2011
7. R. S. Kaler and R. Kaler, "Simulation of Fiber to the Home at 10 Gbit/s using GE-PON architecture," *Optik - International Journal for Light and Electron Optics,* vol. 122, no. 15, pp. 1362-1366, 2011
8. S. Al-Chalabi, "Optically powered telephone system over optical fiber with high service availability and low risk of investment in FTTH infrastructure," *IEEE Communications Magazine*, vol. 50, no. 8, pp. 102-109, 2012.
9. D. Chrissan, "Uni-DSLT: One DSL for universal service," *Texas Instruments White Paper (Spay018)*, 2004.

10. M. Chardy, M. C. Costa, A. Faye, and M. Trampont, "Optimizing splitter and fiber location in a multilevel optical FTTH network," *European Journal of Operational Research,* vol. 222, no. 3, pp. 430-440, 2012
11. J. S. Malhotra, M. Kumar, and A. K. Sharma, "Low cost solution to high capacity 32× 32 channel FTTH duplex link employing triple play services," *Optik-International Journal for Light and Electron Optics,* vol. 125, no. 1, pp. 93-96, 2014.
12. J. R. Schneir and Y. P. Xiong, "Economic implications of a co-investment scheme for FTTH/PON architectures," *Telecommunication Policy,* vol. 37, no. 10, pp. 849-860, 2013.
13. N. Massa, "Fiber optic telecommunication," *Fundamentals of Photonics. University of Conneticut,* 2000.
14. D. Kocher, R. S. Kaler, and R. Randhawa, "Simulation of fiber to the home triple play services at 2 Gbit/s using GE-PON architecture for 56 ONUs," *Optik,* vol. 124, no. 21, pp. 5007-5010, 2013.
15. J. S. Shaik and N. Patil, "FTTH deployment options for telecom operators," *Sterlite Optical Technologies Ltd., White Paper,* pp. 1-9, 2005
16. S. Katlay and A. Balagoni, "Technological and Cost based Analysis of Future-Proof Fiber Access Passive Networks: GPON and WDM PON," *arXiv preprint arXiv:1308.5356,* 2013.
17. Y. Qiu, "Availability Estimation of FTTH Architectures Based on GPON," *2011 7th International Conference on Wireless Communications, Networking and Mobile Computing*, 2011.
18. B. Kim, W. Lee, and J. Han, "Outside plant architecture of fiber-based access network*," Digest of the 9th International Conference on Optical Internet (COIN 2010)*, 2010.
19. M. M. Al-Quzwini, "Design and Implementation of a fiber to the home FTTH access network based on GPON," *International Journal of Computer Applications,* vol. 92, no. 6, 2014.

20. M. Chardy, M. C. Costa, A. Faye, and M. Trampont, "Optimizing splitter and fiber location in a multilevel optical FTTH network," *European Journal of Operational Research*, vol. 222, no. 3, pp. 430-440, 2012.
21. Marija D. Mraković and Petar S. Matavulj, "Analysis of Coexisting GPON and NG-PON1 (10G-PON) Systems," *Telfor Journal*, vol. 3,no.1, 2011.
22. H. Rohde and D. A. Schupke, "Securing Passive Optical Networks Against Signal Injection Attacks," *Optical Network Design and Modeling Lecture Notes in Computer Science*, pp. 96–100,2006.
23. L. G. Kazovsky et al., "Challenges in next-generation optical access networks: addressing reach extension and security weaknesses," in *IET Optoelectronics*, vol. 5, no. 4, pp. 133-143, August 2011.
24. P. Laka and L. Maksymiuk, "Steganographic transmission in optical networks with the use of direct spread spectrum technique," *Security and Communication Networks*, vol. 9, no. 8, pp. 771–780, 2015.
25. Zhenxing Wang and Mable P Paul R. Prucnal, "Physical Encoding in Optical Layer Security," *Princeton University, Princeton*, NJ, 08544, USA, 2012.
26. F. S. Team, "Fiber optic attenuator, optical variable attenuator," *Data Center, Enterprise & ISP Netwok Solutions*. [Online]. Available: https://www.fs.com/basics-of-fiber-optic-attenuator-aid-344.html. [Accessed: 25-Jul-2018].
27. Kevin Cyrus Robinson, "US6137941A - Variable optical attenuator," *Google Patents*. [Online]. Available: https://patents.google.com/patent/US6137941A/en. [Accessed: 25-Jul-2018].
28. Stephen Cohen, "Novel VOAs provide more speed and utility," *Penn Well Corporation*, Nov. 2000.
29. Konstantinos Manousakis and Georgios Ellinas, "Design of Attack-Aware WDM Networks Using a Meta-heuristic Algorithm," *Artificial Intelligence Applications and Innovations (HAL)*, pp. 1–11, Sep. 2013.
30. Er. Tajinder Kaur and Er. Gaurav Soni, "Performance Analysis of Optical Time Division Multiplexing Using RZ Pulse Generator," *International Journal of Computer Science and Mobile Computing*, vol. 04, no. 10, pp. 40–45, Oct. 2015.

31. Arpana Mishra and Arpana Mishra, “Optical Communication with Time Division Multiplexing (OTDM) and Hybrid WDM/OTDM PON,” *International Journal of Science and Research (IJSR)*, vol. 03, no. 12, pp. 1681–1684, Dec. 2014.
32. Huawei Company, “GPON OLT SFP,” *GPON data sheet*. [Online]. Available: https://www.championone.com/uploads/datasheets/Huawei/SFP GPON.pdf. [Accessed: 20-Nov-2018].
33. S.Srinath, “Performance Analysis of 2.5 Gbps GPON,” *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering*, vol. 3, pp. 10148–10155, Jun. 2014.
34. “What is Q-factor?,” *Simplifying what and why of Raman Amplifier. MapYourTech.com*,17-Jun-2014.[Online].Available: http://mapyourtech.com/entries/general/what-is-q-factor-and-what-is-its-importance-. [Accessed: 20-Nov-2018].
35. “Fiber Optics Attenuators - The Ultime Guide on How they work?,” *Beyondtech*. [Online]. Available: https://beyondtech.us/blogs/beyond-blog/optical-attenuator. [Accessed: 25-Nov-2018].
36. H. A. Bakarman, S. Shaari, and M. Ismail, “Simulation of 1.25 Gb/s downstream transmission performance of GPON-FTTx,” *International Conference On Photonics 2010*, 2010.
37. Wolfgang Moench, Douglas Clague, and Viavi Solutions, “Challenges in Next-Gen PON Deployment,” *lightwaveonline.com*, 28-Jun-2017. [Online]. Available: https://www.lightwaveonline.com/articles/2017/06/challenges-in-next-gen-pon-deployment.html. [Accessed: 02-Dec-2018].
38. “xPON Comparison Standard Packet Size,” *SlidePlayer*. [Online]. Available: https://slideplayer.com/slide/3417654/. [Accessed: 02-Dec-2018].