Bulletin of Electrical Engineering and Informatics
Vol. 8, No. 3, September 2019, pp. 1059~1065
ISSN: 2302-9285, DOI: 10.11591/eei.v8i3.1600

Impact of security breach on the upstream delay performance of next generation gigabit passive optical networks

F. M. Atan[1], Nadiatulhuda Zulkifli[2], S. M. Idrus[3], N. A. Ismail[4], A. M. Zin[5]
[1,2,3,4,5]Lightwave Communication Research Group, Universiti Teknologi Malaysia, Malaysia
[1,4,5]Faculty of Electrical Engineering, Universiti Teknologi MARA, Malaysia

Article Info

Article history:

Received Jan 2, 2019
Revised Mar 12, 2019
Accepted Mar 29, 2019

Keywords:

Bandwidth assignment
Dynamic bandwidth allocation
Gigabit Passive Optical Network
Network security

ABSTRACT

The next generation passive optical networks (NG-GPON) such as long reach GPON is the future-proof solution to answer the continuous demands for access user bandwidth and network expansion. However, security which is yet to be addressed in NG-GPON needs urgent attention as it will become more critical due to much longer distance, denser user population and more network elements. In addition, the longer propagation delay in NG-GPON can also lead to a more complex bandwidth allocation mechanism that is expected to operate in a dynamic manner. Among the highlights of recommendations for future implementation are improvements in the security aspect and the use of dynamic bandwidth allocation (DBA) algorithm that suit the characteristics of long reach GPON. Current PON is exposed to degradation attack, a security breach that can harm how bandwidth fairness mechanism among ONUs work. Thus, this project proposes a secured DBA mechanism for NG-PON that could overcome this particular threat. In specific, a detection phase will be included in the DBA mechanism to sense and subsequently mitigate abnormal behaviours among ONUs that are harmful to the goal of DBA i.e. to ensure QoS among ONUs and traffics. At the same time, careful attention is given on the delay parameter as it is a critical parameter that can affect DBA performance in long reach GPON. In this paper, preliminary analysis is shown that reveal how possibility of threats increase with increasing of distance and network elements.

Corresponding Author:

Nadiatulhuda Zulkifli,
Lightwave Communication Research Group,
Universiti Teknologi Malaysia (UTM),
81310 Johor Bahru, Malaysia.
Email: nadiatulhuda@utm.my

1. INTRODUCTION

Future evolving PON involves longer fiber distance and more network elements especially ONUs to cater the demands for increasing number of users and bandwidth hungry applications. Increasing fiber distance can incur longer propagation delay which can significantly affect performance of the existing bandwidth allocation algorithm that is designed for conventional PON reach [1-2]. Even though a number of new DBAs have been proposed in the literature, to our knowledge, these algorithms lack security awareness [3].

Since the launch of ITU-T G.989.1, in 2013, the GPON have growth exponentianally to cater for the demand of high bandwidth, high speed data communication. It usually consists of OLT (Optical Line Terminal), ONUs/ONTs (Optical Network Units or Optical Network Terminals) and ODN (Optical Distribution Network). OLT that is located at the central office or provider's side of the access network is in control of the configuration and setup for all parameters e.g. frame duration and power level. The end unit (ONU) located at the customer's side provides the conversion from optical to electrical signal and the

conversion from GPON Transmission Convergence (GTC) frames to Ethernet frames. Generally, Internet Service Providers (ISPs) with OLT do not need to have access to subscriber networks called the last mile. Hence, the subscribers (users) use only ONUs and ISP manages only Optical Line Termination (OLT) nodes. The distribution network employs one or more passive optical splitters (POS) to broadcast information to all ONUs.

Different types of PON differ in how the resources are shared among ONUs. In a TDM-PON, bandwidth resource per fiber is shared on a time-division basis among ONUs. Traffic in the downstream direction is broadcasted by the OLT to all ONUs, with each ONU extracts traffic destined for itself. Meanwhile in the upstream transmission, each ONU is allocated specific time slots to transmit data to the OLT. The time slots can occur at irregular intervals and can have irregular durations. On the other hand, in a wavelength division multiplexed PON (WDM-PON), each ONU is allocated a different wavelength channel for communication between the OLT and that ONU. The most widely deployed PON technologies based on TDM-PON are Ethernet PON (EPON) and Gigabit PON (GPON). These technologies differ significantly in signaling rates, data formats and protocols employed [4-5].

As more end users are supported over a shared physical medium in future optical networks, access network security should be a greater importance as a single attack can affect a great number of users that may involve nearly hundreds of Gbps transmission [6]. GPON does offer security features such as data encryption, authentication and key establishment. However, since GPON has strong reliance on the assumption that all the GPON elements will be physically protected, its security mechanism is largely relaxed. Both authentication of ONUs and encryption of downstream traffic are optional while upstream traffic is not encrypted assuming high directionality of PON where other ONUs cannot sniff traffic sent by an ONU to OLT.

Security is a ticking time bomb issue in the existing GPON that does not have a robust security measures as it relies on the assumption that all the GPON elements are physically protected. The fact that all ONUs can listen to data sent to other ONUs apart from their own is a potential threat that requires encryption and authentication to take place [7]. However, in the current GPON implementation, authentication and encryption are optional where encryption is only for the downstream communication from OLT to ONU using merely a plain text key that is exchanged earlier during initialization. Meanwhile, upstream communication from ONU to OLT are not encrypted assuming high directionality that makes sniffing difficult.

These flaws lead to the call for stronger security measures in future PON. It is even more critical for long reach PON as the involvement of more GPON elements increase possibility of threats and the large number of users that can be affected [8]. In response, researches have proposed a number of encryption and authentication techniques for future PON [9-10]. However, as mentioned before, DBA mechanism which is an essential process in GPON lacks security awareness. In DBA process, attack by a malicious ONU takes place not to sabotage the whole GPON operation but instead to gain more bandwidth at the expense of other ONUs. The attacker basically exploits two features by sending GPON upstream signals out of its given slots and cause other ONUs to experience packet loss; (1) The TCP mechanism that reduces an ONU's requested bandwidth in response to packet loss and (2) DBA's bandwidth assignation that is done dynamically in accordance to ONU's requested bandwidth.

In research report by [11], cyber-attack incidents have increased on the recent years. However due to multilayer operation and standards, there is no clear-cut understanding of the attacks. This includes the source, the organization or complexity of the attack, and means to stop and counter the attacks. There are numbers of typical attack within the PON system. For example, the Denial of Service, (DoS) attack, spoofing attack, eavesdropping and degradation attack [12]. Generally, botnet or bot launched the attack in the network [13-14], however locating the bots is proven a great difficult as proven by [15] as they can change rapidly and sporadically. This further complicated by the fact the attack can be launched from multiple puppets controlled by a single master bot and these puppets are unaware that they are being used as puppets. Complication further arises because there is no way for certain to predict when this attack happened and their magnitude of destruction. In 2016, an attack using Mirai Botnet successfully knockdown an entire county internet connection. To make matter worst, the attack in such magnitude is launched offline [16]. Even if the attack is launched on small country such as Liberia (only 10 percent of the people have access to internet), the hypothesis is that the attacker is testing the capabilities of the bot. Once the attack is perfected, it might be countries or entire continent hence, the damages will be unthinkable.

However, when the attack is becoming more frequent, a trend can be mapped from them. When a network is under attack, the bandwidth of the network increased rapidly [11]. There are number of ways to predict an attack of the network. Common way to detect DoS attack is signature detection and traffic anomaly detection [17]. A signature detection scans based on malformed packets and protocol; a common signature of DoS attack. A traffic anomaly detection scans deviation on the traffic against normal condition.

Which is why the second detection protocol is preferred because the increased-on bandwidth can demonstrate the degree of attack in the network. At its peak, Mirai Botnet was hammering the servers with 620 gigabits of garbage traffic every second [18].

Bear in mind that the attack could happen in each layer of the network [19]. DoS attack for example are generally happened in network layer or application layer [11, 20]. In network layer, the attacker normally tries to exhaust the available bandwidth in the network. Shrinking the bandwidth of the network provider or the server to the point where total network would crush. Application layer attack would include attacking the processing capabilities of the server or router. Such attack would include flooding the server with unimportant or empty packets, so much so that the server would be too busy to handle meaningful packet [21]. In this paper we only focus on security improvements in the GPON infrastructure itself that potentially have low impact on the already assigned technology and standard. In specific, physical layer-based security measures using passive or active devices are left out in order not to increase operational or capital expenditures. Moreover, gap in the GPON security standard might lead to new definitions based on proprietary solutions [22].

Existing work that looks at this particular issue during bandwidth allocation algorithm is conducted on EPON standard which is inherently different from GPON, and it is also based on short PON reach. GPON has more complicated structure with many encapsulations with variable lengths of parts. Furthermore, static bandwidth allocation algorithm that is deployed in this work also does not adhere to the long reach GPON requirement of dynamic bandwidth allocation mechanism [1].

For the purpose of this paper, we will only consider the form of DoS attack known as degradation attack that happens in the network. The malicious ONU targets on stealing bandwidth from another ONUs by reducing their throughput [6]. In this case, this ONU is not fake and physically valid. This is done by sending signals out of their allocated time using other ONU's timeslot which leads to collision. As a result, the affected ONU will experience frame loss and request lesser bandwidth. The attacker could easily exploit bandwidth sharing algorithm to gain an unfair amount of bandwidth as bandwidth allocation algorithm typically works on available capacity and request bandwidth. [6] proposed a technique to detect and thus improve fairness in the allocation algorithm. However, the work is conducted on EPON standard which is inherently different from GPON and is based on small PON infrastructure. GPON has more complicated structure with many encapsulations with variable lengths of parts. Furthermore, static bandwidth allocation algorithm that is deployed in this work also does not adhere to the GPON requirement of dynamic bandwidth allocation mechanism [2], [23]. All these gaps lead to the call for a security-aware DBA that can be applied effectively in the evolving optical access networks that are based on Long Reach Passive Optical Network (LR-PON) roadmap.

2. RESEARCH METHOD

The research starts with the modelling of the attack. To model the attack first target is determined. For this experiment, the bandwidth is the target; or to be specific to exploit the vulnerability of limited bandwidth assigned to the network. In order to do so, heavy TCP traffic (packets) of legitimate-like headers and random payload is sent towards victim. The result is massive traffic generated, leading in bandwidth saturation and degradation of server's CPU consumption. To add to the effect, once the malicious ONUs launched the attack, lawfull ONUs will experience bandwidth reduction due to automatic assigned DBA in PON.

A simulation is done in the OMNeT++ platform. Standard PON architecture is defined and simulated. A single OLT is connected to varied amount of ONUs. The number of ONUs differed from 8, 16, 32, and 64. ITU-T compliant DBA considers type of traffic by categorizing it to four classes as in Table 1. A PON network has to support different broadband services like video conferencing, leased lines, and VoIP in addition to basic voice and data services, each with different delay and bandwidth requirements. ITU-T categorizes PON traffic in 4 classes type 1 (T1) to type 4 (T4) as shown in the Table 1. These traffic classes handle multiple traffic types by mapping to a suitable class. A traffic bearing entity is represented by a transmission container (TCONT), which carries the particular traffic class frames. Each TCONT has a unique identifier (Alloc-ID) that is assigned by optical line terminal (OLT) in the ONU initialization phase.

In the DS direction, the traffic pattern is broadcasted, but in the US case, the media is shared by all the optical network units (ONUs) in a time division multiplexed manner as the US transmission of all ONUs is on the same wavelength. Therefore, a bandwidth management scheme is necessary for efficient and fair distribution of US bandwidth.

The simplest scheme could be a fixed bandwidth assignment (FBA) for all the ONUs. However, this scheme not only causes bandwidth wastage by ONUs, which have low traffic load, but it also results in increased delays for the heavily loaded ONUs as they do not get the desired bandwidth. If a dynamic

bandwidth assignment (DBA) scheme is used instead, then the available bandwidth can be efficiently used as it can assign bandwidth to all the ONUs fairly as per their demand and in compliance to the service level agreements (SLAs). The DBA scheme also allows the network operators to oversubscribe customers on the best effort (BE) basis to enhance the revenues The DBA scheme at OLT assigns bandwidth to each traffic class as per its demand and its SLA.

In order to distribute bandwidth fairly, scheduling mechanism for bandwidth allocation is done based on TCONT type. Each TCONT has a unique allocation ID (Alloc-ID) to identify different traffic types [24]. For this simulation, DS traffic load is fixed to 0.1 and US traffic load is fixed to 0.8 Since T-CONT type 1 is allocated for static bandwidth, T1 is not considered in this paper.

Table 1. TCONT reference model [24]

TCONT	Type of Bandwidth	Description
1	Fixed bandwidth	VoIP, live video streaming
2	Assured bandwidth	Minimum guaranteed bandwidth
3	Non-assured bandwidth	From underloaded IDs
4	Best effort bandwidth	Lowest priority

It is an improvement to [24] where it divides the remaining unassigned bandwidth equally to all ONUs and the bandwidth assignment for T2, T3 and T4 is 40%, 35% and 25% respectively. If there is still remaining bandwidth, it will be uniformly distributed among T4 classes. According to ITU, T4 cannot be given priority over T2 and T3 during service interval (SI), over allocates bandwidth to a traffic class only if total available byte counter for each traffic class of each ONU is positive [25].

For the first part of simulation, the network is run with all the ONUs obeying the predetermined timeslot allocated for them. The value of average mean delay is recorded for each experiment. Next, one ONU is set as malicious node that will run in 50% of all the bandwidth of the entire network. Hence leaving every other ONUs (the obedient ones) to share remaining 50% of the bandwidth. Again, the value of average mean delay is recorded.

Figure 1 shows the simulation setup for the experiment. In each experiment, the number of ONUs is set to be varied from 8,16,32, and 64. This is to demonstrate the degree of damage to the network once the attack started. The server act as traffic generator using poison distribution which connected to OLT and then splitter. The splitter is connected to various nodes which in this case acted like the ONUs. For simplicity of simulation only one host and one user are configured per ONU.

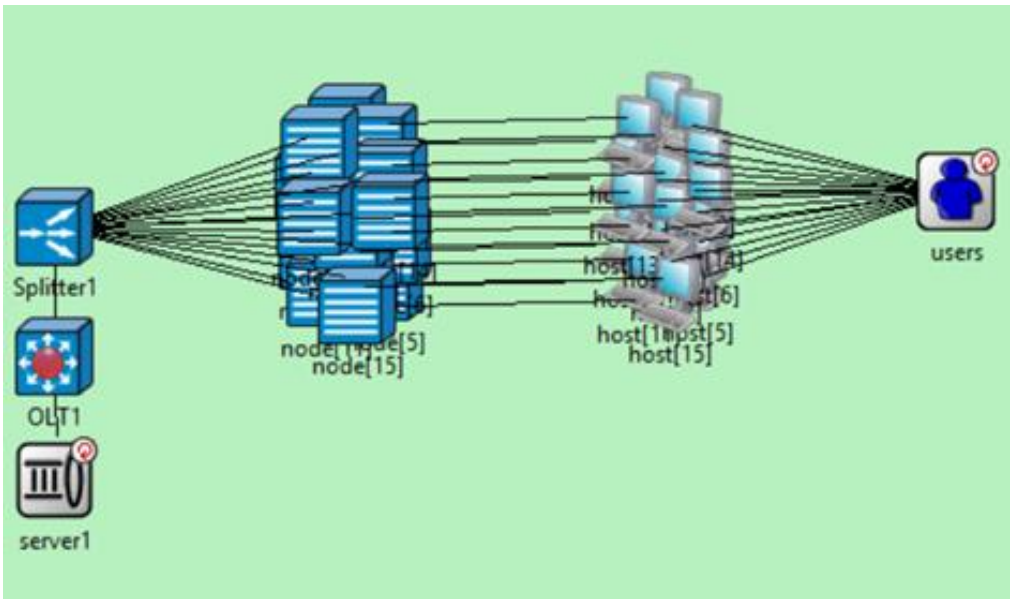

Figure 1. Simulation setup for 16 ONUs [24]

3. RESULTS AND ANALYSIS

We considered a network with maximum of 1 malicious node. The attack of the network will start after 2 second from the start of simulation time. When the attack starts, the poison distributed traffic will automatically take over 50% of the entire network throughput. Hence remaining ONUs will have to sustain with just 50% of bandwidth. The Figure 2, 3 and 4 shows the average delay of the packet arriving in upstream connection. The average upstream delay results for T2, T3 and T4 traffic are illustrated in Figure 4. ITU-T G.987.1 recommends that GPON system must accommodate services that require a maximum mean delay of 1.5ms [25].

As general representation, the average delay increases when the number of ONU is increase regardless of traffic type. However, the percentage of difference on the delay between 64 ONU is much larger compared to small number of ONUs; for example, 8 ONUs. For 8 ONUs the difference in delay is 8% and 648 ONUs is 21%. Since the Dynamic Bandwidth Allocation is applied in the network, an unused bandwidth by the well behaved ONU will be further manipulated by the malicious ONU. Hence the increase in ONU numbers will also means the increase in unused bandwidth by the well behave ONUs. As the number of subscribers will only keep on increasing over the time, this is some serious complication to be solved in terms of optical network security

In Figure 2, T2 traffic class shows the least delay as network load increases due to its highest priority. This proves that the algorithm satisfies ITU standard which T2 and T3 are supposed to be given priority bandwidth allocation and T4 has the least priority. As shown in Figure 4, T4 traffic class has the highest upstream delay and as the network being attack it will have the most significant delay at 64 ONUs compared to T2 and T3 traffic type. The increased of delay for T4 starts at network load 0.8 where it is already beyond XGPON requirement. This is expected because T4 is best effort type of bandwidth and given the lowest priority with 25% of bandwidth assignment. T2 and T3 have the average upstream delay less than ITU-T recommendation.

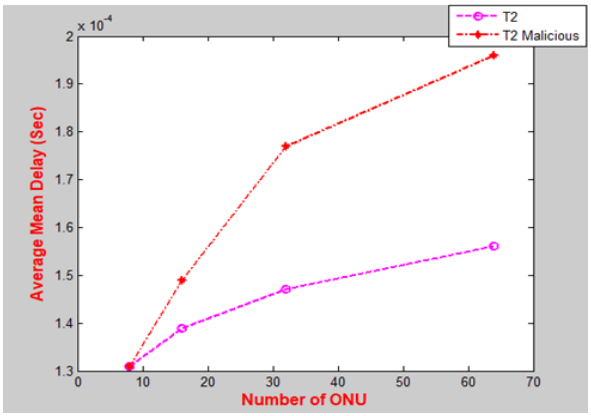

Figure 2. Comparison of T2 type traffic

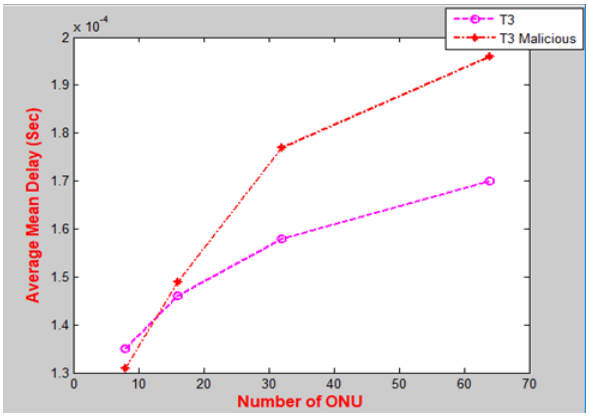

Figure 3. Comparison of T3 type traffic

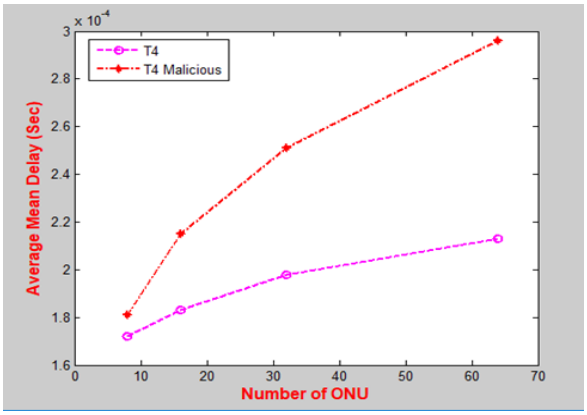

Figure 4. Comparison of T4 type traffic

In general, in normal DBA operation, the average delay performance is as expected:

a. Delay increases when the number of ONU increases indicating more bandwidth competition.
b. For all ONU range from 8 to 64, TCONT2 has the lowest delay, followed by TCONT3 and TCONT4 as DBA treats classes differently.
c. Delay increment between min ONU, 8 and max ONU, 64; ~20% for TCONT2, ~24% for TCONT3 and ~27% for TCONT4.

In scenario where malicious ONU floods the network:

a. Delay increases drastically as a result of disruption to service that reduces the available bandwidth that can be assigned to well-behaved ONUs.
b. For all ONU range from 8 to 64, TCONT2 and TCONT3 have almost similar delay performance.
c. Delay increment between min ONU, 8 and max ONU, 64; ~50% for TCONT2 and TCONT3, and ~65% for TCONT4.
d. The best effort traffic is highly affected in the event of attack.

4. CONCLUSION

We have studies the impact of malicious ONU that attack the network in terms of upstream delay. A dynamic bandwidth allocation implement in the network will further favour the malicious node as they continue to take up the unused bandwidth from lawful ONUs. As the number of ONUs increased, the effect of the attack become more severe. Here however, the attacker is limited to be one malicious whereby in real life the attack could be launched from various sources. Next plan of action is to further study the impact of attack in larger network and find out suitable punishment to the attacker without compromising the network bandwidth and other well-behaved ONUs.

ACKNOWLEDGEMENTS

The work described in this paper was carried out with the support by a research management center (RMC) of Universiti Teknologi Malaysia (UTM). The authors acknowledge the Ministry of Higher Education Malaysia (MOHE) and the administration of UTM for the project financial support through the cost center number Q. J130000.2523.18H19 and R.J130000.7851.5F086.

REFERENCES

[1] P. D. Townsend *et al*., "Long Reach Passive Optical Networks," *LEOS 2007 - IEEE Lasers and Electro-Optics Society Annual Meeting Conference Proceedings*, Lake Buena Vista, FL, 2007, pp. 868-869.
[2] ITU-T G. 984.1, Gigabit-capable Passive Optical Networks (GPON): General characteristics, 2008, with amendment 1 (2009) and 2 (2012).
[3] H. Song, B. Kim and B. Mukherjee, "Long-reach optical access networks: A survey of research challenges, demonstrations, and bandwidth assignment mechanisms," in *IEEE Communications Surveys & Tutorials*, vol. 12, no. 1, pp. 112-123, First Quarter 2010.
[4] F. Effenberger, H. T. Us, D. Cleary, O. Haran, P. M. C. Sierra, G. Kramer, R. D. Li, M. Oron, T. Pfeiffer, and A. Germany, "An Introduction to PON Technologies," *IEEE* Communications Magazine: Topics in Optical Communications, pp. 17–25 March, 2007.
[5] K. Tanaka, A. Agata, and Y. Horiuchi, "IEEE 802.3av 10G-EPON Standardization and Its Research and Development Status," *J. Light. Technol*., vol. 28, no. 4, pp. 651–661, Feb. 2010.
[6] L.G Kazovsky, S.W Wong, V Gudla, P.T Afshar, S.H Yen, S Yamashita, et al, "Challenges in next-generation optical access networks: addressing reach extension and security weaknesses," *Iet Optoelectron*. 5(4):133–43, 2011
[7] S. Drakulic, M.Tornatore, G. Verticale., "Degradation attacks on Passive Optical Networks", *2012 16th Int Conf Opt Netw Des Model ONDM 2012*. Mar. 2012
[8] R. Gu, X. Liu, and Y. Ji, "Physical-aware long reach PON planning," *Telecommun*. Syst., vol. 60, no. 3, pp. 367–379, Nov. 2015.
[9] L. Malina, T. Horvath, P. Munster, and J. Hajny, "Security Solution With Signal Propagation Measurement For Gigabit Passive Optical Networks," *Optik*, vol. 127, no. 16. pp. 6715–6725, 2016
[10] M. S. Kiaei, K. Fouli, M. Scheutzow, M. Maier, M. Reisslein and C. Assi, "Delay analysis for ethernet long-reach passive optical networks," *2012 IEEE International Conference on Communications (ICC)*, Ottawa, ON, 2012, pp. 3099-3104.
[11] K. M. Carley, W. K. V. Chan, A. D'Ambrogio, G. Zacharewicz, N. Mustafee, G. Wainer, and E. Page, "Simulating DDoS Attack on the US Fiber-Optics Internet Infrastructure", *Proceedings of the 2017 Winter Simulation Conference*, pp. 1228–1239, 2017.
[12] D. Dahan and U. Mahlab, "Security threats and protection procedures for optical networks," in *IET Optoelectronics*, vol. 11, no. 5, pp. 186-200, 10 2017.

[13] Y. Ji, L. Yao, S. Liu, H. Yao, Q. Ye and R. Wang, "The Study on the Botnet and its Prevention Policies in the Internet of Things," *2018 IEEE 22nd International Conference on Computer Supported Cooperative Work in Design ((CSCWD))*, Nanjing, 2018, pp. 837-842.
[14] N. Hoque, D. K. Bhattacharyya and J. K. Kalita, "Botnet in DDoS Attacks: Trends and Challenges," in *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2242-2270, Fourthquarter 2015.
[15] S. Kumar and K. M. Carley, "DDoS cyber-attacks network: Who's attacking whom," *2016 IEEE Conference on Intelligence and Security Informatics (ISI)*, Tucson, AZ, 2016, pp. 218-218.
[16] A. Stavrou, J. Voas, and I. Fellow, "DDoS in the IoT ," Computer (Long. Beach. Calif)., vol. 50, pp. 80–84, 2016.
[17] M. Alenezi and M. J. Reed, "Denial of service detection through TCP congestion window analysis," *World Congr. Internet Secur.*, pp. 145–150, 2013.
[18] J. Margolis, T. T. Oh, S. Jadhav, Y. H. Kim, and J. N. Kim, "An In-Depth Analysis of the Mirai Botnet," *Proc.-2017 Int. Conf. Softw. Secur. Assur. ICSSA 2017*, pp. 6–12, 2018.
[19] 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.
[20] G. Kumar, "Understanding Denial of Service (Dos) Attacks Using OSI Reference Model," *Int. J. Educ. Sci. Res. Rev.*, no. 5, pp. 10–17, 2014.
[21] H. A. Herrera, W. R. Rivas, and S. Kumar, "Evaluation Of Internet Connectivity Under Distributed Denial Of Service Attacks From Botnets Of Varying Magnitudes," *Proc.-2018 1st Int. Conf. Data Intell. Secur. ICDIS 2018*, pp. 123–126, 2018
[22] M. Ruffini, D. Mehta, B. O'Sullivan, L. Quesada, L. Doyle, and D. B. Payne, "Deployment Strategies for Protected Long-Reach PON," *J. Opt. Commun. Netw.*, vol. 4, no. 2, p. 118, 2012.
[23] ITU-T G. 989. 1, 40-Gigabit-capable passive optical networks (NG-PON2): General requirements, 2013 with amendment 1, 2015
[24] R. A. Butt, M. W. Ashraf, M. Faheem, A. G. Universitesi, and S. M. Idrus, "A Survey of Dynamic Bandwidth Assignment Schemes for TDM-Based Passive Optical Network," *Journal of Optical Communications.* 2018.
[25] M. S. Han, H. Yoo, and D. S. Lee, "Development of Efficient Dynamic Bandwidth Allocation Algorithm for XGPON," *Etri J.*, vol. 35, no. 1, pp. 18–26, 2013.