VOL. 23, NO. 3, 2024, 144-150
elektrika.utm.my
ISSN 0128-4428

ELEKTRIKA
Journal of Electrical Engineering

An Overview of Security Threats Mitigation through Dynamic Bandwidth Allocation Algorithms in Passive Optical Networks

Sumayya Bibi[1], **Nadiatulhuda Binti Zulkifli**[1*], **Farabi Iqbal**[1], **Safdar Raza**[2] and **Muhammad Amir Shafi**[3]

[1] Faculty of Electrical Engineering, Universiti Teknologi Malaysia, 81310 UTM Skudai, Johor, Malaysia.
[2] Department of Electrical Engineering, NFC Institute of Engineering and Technology, Multan, Pakistan.
[3] Department of Electrical and Computer Engineering, Comsats University, Islamabad Pakistan.

[*]Corresponding author: nadiatulhuda@utm.my

Abstract: Amid the ceaseless advancements in the telecommunication world, Passive Optical Network (PON) technologies have positioned themselves as paramount solutions in the sphere of global broadband access networks. These technologies offer several distinctive benefits, including remarkable bandwidth capabilities, impressive reach, passive nature, relative ease of maintenance and flexibility for potential future upgrades. Among these technologies, Gigabit PON (GPON) has been extensively adopted across Europe and America, while Ethernet PON (EPON) has found considerable favor in regions such as Korea and Japan. GPON, which notably functions as a potent "last-mile" communication system, leverages the unparalleled high-speed data transfer capabilities that are inherent to fiber-optic technology. However, with technological progress comes the escalating need for robust security measures. The complex landscape of network technologies has seen a rise in cyber threats, making security a paramount concern. Cyber threats can often take several forms, such as masquerading, where unauthorized entities impersonate legitimate users; packet replaying, where network packets are maliciously resubmitted; message modification, where information within network messages is unlawfully altered; and the more notorious Denial of Service (DoS) attacks. This study embarks on an exploratory journey into the impacts of these diverse security strategies on the overall performance of PON technologies. It provides an overview that considers the categorization of PON standards and scrutinizes their respective security schemes, providing insights into their effectiveness. This paper not only reviews existing methods for mitigating security threats in PONs but also introduces a novel Hybrid Security-Aware DBA (HSA-DBA) model. By incorporating machine learning, the HSA-DBA enhances adaptability and resilience in bandwidth allocation while addressing evolving security challenges. This approach ensures optimal bandwidth distribution, adheres to SLAs, and strengthens PONs against future threats, offering a significant advancement in secure and efficient PON architecture. The study examines performance metrics including upstream delay, delay variation, and frame loss across traffic classes T1, T2, T3 and T4.

Keywords: Bandwidth efficiency, dynamic bandwidth assignment, denial of service attack, next generation passive optical network, passive optical network

© 2024 Penerbit UTM Press. All rights reserved

Article History: received 30 December 2023; accepted 27 October 2024; published 30 December 2024

1. INTRODUCTION

The Passive Optical Network (PON) is a point-to multi-point access network with a tree structure. Optical Line Terminal (OLT) is the name of the terminal apparatus at the tree's base.

It is linked to a Passive Optical Splitter/Combiner (POS) situated in the distant node via an optical trunk fiber. The optical signals generated by the ONUs are merged by POS, from many fibers into one and conversely, from the trunk fiber the optical signals are split into different drop fibers to the ONUs [1]. Figure 1 demonstrates the basic PON architecture from OLT, splitter to ONU. Both data transmission upstream and downstream are feasible from the ONU to the OLT, and vice versa from the OLT to the ONU.

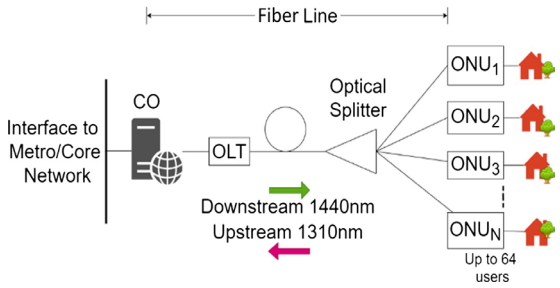

Figure 1. Basic PON Architecture [2]

Meanwhile, Information and Communication Technology (ICT) is experiencing rapid growth over time. With this increment, ICT has changed the whole world into a global village. Cyberattacks have been rising steadily along with the exponential growth in ICT infrastructure,

and they are projected to continue to rise in the future [2, 3]. Accordingly, ensuring the security of PON as the main representative of the access network domain remains a critical issue.

Downstream traffic in PON is broadcasted to all users simultaneously where every ONU can only read its own traffic using a mandatory encryption mechanism. Meanwhile, upstream transmission requires a media-sharing system in the shared upstream channel. Each ONU's transmission time slot is scheduled using a bandwidth allocation algorithm which can be static or dynamic. A static upstream bandwidth allotment suffers from the following drawbacks: (1) The allocation of bandwidth to heavily burdened ONUs is restricted, resulting in buffer overflow issues and delays in transmission, and (2) The efficiency of the function diminishes in achieving full bandwidth utilization because of the presence of unused bandwidth in lightly burdened ONUs. ITU-T recommends a Dynamic Bandwidth Allocation (DBA) mechanism, which is useful in the upstream channel to improve bandwidth utilization and network performance [4,5].

In the past, most reported works in PON's DBA focused on Quality of Service (QoS) improvements and ignored the security aspects. With the exception of a few where network security element is given strong emphasis due to the harmful threats by attackers in stealing network resources and affecting the network performance [1]. Two main strategies for security improvements include detection and mitigation phases to penalize the attacker.

This paper aims to provide an overview of the different methods used in these existing studies to increase readers' comprehension in this growing area. The structure of this paper proceeds as follows: Section 2 delves into primary security concerns within PON. Section 3 examines the literature review and relevant studies, followed by Section 4, which delineates the specifics of chosen detection and mitigation algorithms. The conclusion is then presented in Section 5.

2. SECURITY THREATS IN PON

The subsections that follow list the three main security risks to GPON eavesdropping, Denial of Services (DOS) attacks and spoofing attacks, and explain associated research being done to address the vulnerability issues. Our focus is solely on security enhancements for the GPON infrastructure itself, which may have minimal impact on the technology and standards already designated by machine learning schemes.

2.1 Eavesdropping

The potential for any ONU to eavesdrop on data intended for other ONUs presents a significant threat, as previously emphasized. Typically, an eavesdropping attack will listen to data supplied by other ONUs, analyse data trends, and exploit the data to get unlawful network bandwidth. Usually, it has no intention of taking down the entire network. The process of dynamically allocating bandwidth tends to favor malicious ONUs, resulting in restricted bandwidth for legitimate ONUs [6].

In addition to bandwidth theft, Theft of Service (ToS) is another possibility. A ToS attack makes use of information obtained from listening in. Because the ToS involved invoicing the victim while the malicious ONU was using/stealing the services, users had trust concerns. Figure 2 illustrates upstream transmission eavesdropping.

Given the paramount importance of security in PON deployment, ITU-T mandates the incorporation of the Advanced Encryption Standard (AES). Nonetheless, AES operates under the assumption of the integrity of the upstream channel.

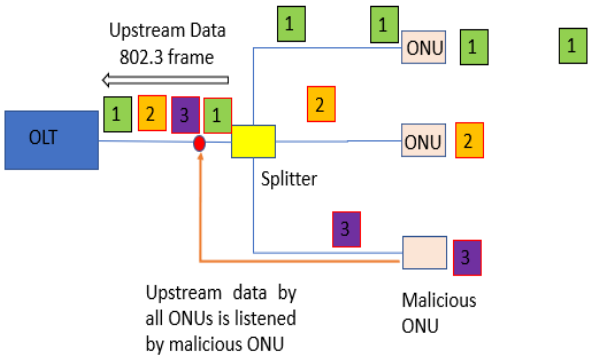

Figure. 2. Eavesdropping in Optical Network

2.2 Denial of Service (DoS) Attack

Within optical networks, the DOS attack stands out as a prevalent security concern. In Figure 3 denial of service attacks in optical networks are shown. This type of attack may crash down the whole network. The system crash occurs through the transmission of redundant data packets to targeted computers, potentially overwhelming their computational capacity and leading to a system-wide collapse[7,8]. From network and transport layer data is theft by this type of attack and it is very difficult to determine whether requested data is genuine or not [9]. Denial of service attack is very difficult to prevent because when the first attack has been stopped then the attacker can switch their destination on to a new computer and may start working there.

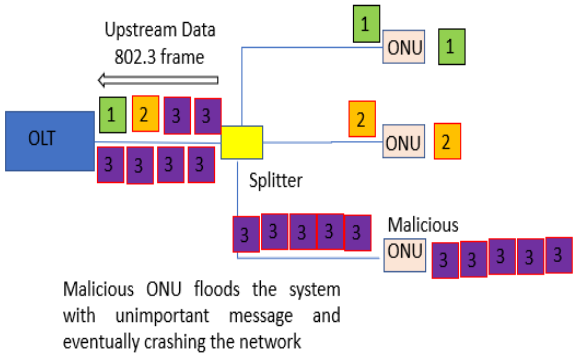

Figure 3. Denial of Service Attack in Optical Network

2.3 Spoofing Attack

As the data traffic is observed by the malicious ONU, it can steal the identity of the ONU and decode the traffic. To control the spoofing attack public key establishment and encryption are imposed on the network.

Even if a malicious ONU lacks the ability to decrypt the

data, it can still disrupt the network by relaying and replaying the signals it has intercepted. To mitigate spoofing attacks, encryption, and public key establishment can be utilized to authenticate user identity.

GPON exhibits a complex structure featuring numerous encapsulations of variable lengths. Additionally, the static bandwidth allocation algorithm employed does not comply with the NG-PON2 (Next-Generation Passive Optical Network 2) mandate for dynamic bandwidth allocation. These disparities underscore the necessity for a security-conscious DBA utilizing a Machine Learning Scheme, capable of effective application in the evolving optical access networks following the GPON roadmap's intricate structure with various encapsulations. Additionally, the static bandwidth allocation algorithm deployed fails to meet the NG-PON2 requirement for a dynamic bandwidth allocation mechanism.

3. RELATED WORKS IN SECURE DBA PON

Optical access networks are intended to increase over time as they are responsible for the maximum delay, ability, and accuracy services, having different demands. However, to handle the network operations and resources to meet the tasks machine learning has been advertised as an intelligent solution for core and metro systems [10].

A dynamic bandwidth allocation technique that is enhanced by machine learning that is both fast and self-adaptive is examined. Optical access networks have developed over the last 30 years to meet the ever-increasing demands of fixed commercial and residential as well as 4G and other networks for quality-of-service (QoS), user numbers, and capacity [11]. Variant PON technologies are listed in Table 1. In Table 2 closely related works of different authors and their techniques are discussed in detail.

These technologies influence the security mechanism in DBA using various parameters like operating wavelength, splitting ratio and data rates, etc.

Most DBAs are not security aware and ignore the possibility of an attack on the network, with the exception of just a few works as security is an emerging area in an optical access network. For instance, works by Drakulic et al [12] and Fadila et al [13,14] on secure bandwidth allocation algorithms do not deploy any ML.

The proposed security aware dynamic bandwidth algorithm (SA-DBA) technique in [15] is the first DBA that attempts to use a regression machine learning approach to handle the above DDOS issue through training traffic patterns from ONUs. Similarly, Atan et al. [13] also demonstrate the usefulness of the DBA technique which has a significant impact on enhancing gigabit passive optical networks' network performance (GPON). This work focuses specifically on loopholes within the transmission control protocol (TCP) congestion control algorithm that can be manipulated by the degradation attack, potentially affecting the targeted network users' bandwidth reception. To address this specific vulnerability, the current work sought to offer a safe DBA method termed as secured DBA. A crucial step in detecting and consequently limiting any anomalous actions seen between optical network devices was adopted at the detection phase by monitoring TCP acknowledgment (ACK) messages.

Waqar et al. [16] look at the different traffic patterns between different client types where the residential clients are anticipated to behave somewhat differently from industrial users, who are typically active during the day and dormant at night. Due to this discrepancy, the traffic load on the (time and wavelength division multiplexing) TWDM PON wavelength will be imbalanced, and numerous security vulnerabilities may materialize. Here, a machine learning method employing regression models is utilized to equitably distribute network resources among both heavily burdened and lightly burdened ONUs, forming an effective load balancing technique known as LB-DWBA (Load Balancing Wavelength and Bandwidth Assignment).

Security mechanism (threat detection and mitigation techniques) is based on collision monitoring per ONU. Since attacks will cause collision and losses to the other ONUs, the ONU with the lowest collision is detected as the threat and penalized. Moreover, the solution is only exclusive to TCP traffic environment as the mechanism relies on TCP window behavior. Meanwhile, work by Rizwan et al [15] does not consider specific traffic types and ignores the effect of higher layers like TCP and threat detection based on the ONU traffic demand using a simple ML technique i.e. regression analysis.

Table1. Variant PON Technologies [1]

PON Technology	G-PON	XG-PON	XG(S)-PON
Standard	ITU-T G.984 (2003)	ITU-T G.987 (2010)	ITU- T G.9807.1 (2016)
Data Rate (DS/US)	2.5/1.25G bps	10/2 Gbps	10/10 Gbps
Operating Wavelength (DS/US) (nm)	1480-1500 / 1290 - 1330	1575-1580 / 1260 - 1280	1570-1580 / 1260- 1280
Splitting Ratio	Up to 1:64	Up to 1:128	Up to 1:128
Coexistence	N/A	GPON	GPON

The standards for PON technologies are detailed in Table 1. The GPON standard can be found within ITU-T G.984(2003). The split ratios for a single fiber are 1:32, 1:64, or occasionally 1:128, indicating that each fiber can serve up to 32, 64, or 128 users respectively. The downstream wavelength measures 1480-1500nm, while the upstream wavelength registers at 1290-1330 nm. This system has the capacity to support a maximum of 256 connections [17].

XG-GPON exhibits comparable traits to the existing GPON, albeit with certain alterations at the physical layer that contribute to significant enhancements in performance. These adjustments include factors like split ratio, power budget, and reachability. Moreover, there have been no alterations to the data link layer framing and

management process, thereby reducing the complexity associated with migration.

The XG-GPON system comprises two distinct classes. The initial class, referred to as XG-GPON1, offers asymmetrical transmission rates of 10 Gbps downstream and 2.5 Gbps upstream. On the other hand, the second class, XG-GPON2, delivers symmetrical transmission at 10 Gbps. Information regarding the physical layer specifications for XG-GPON1 has been delineated in ITU-T G.987.2. Conversely, the standard for the physical layer of XG-GPON2 is yet to be finalized.

As per the G.987.1 recommendation for XG-GPON1, two migration approaches have been suggested to facilitate the transition from GPON to XG-GPON1. The first approach involves green-field migration, entailing the substitution of copper connections to premises with optical connections. Alternatively, the PON brown-field migration scenario involves upgrading the current GPON system, which may entail the replacement or enhancement of certain network components like ONU units or OLT modules if required. The downstream wavelength band chosen for XG-GPON1 spans from 1575 to 1580 nm, while the upstream wavelength band ranges from 1260 to 1280 nm. The primary objective of XG-GPON2 is to provide symmetrical transmission by elevating the upstream transmission to 10 Gbps.

Table 2. Related Works on PON Security System

Ref	DBA Algorithm	Key Features	Remarks
[13]	New Security Aware DBA (SA-DBA) to detect the aggressive ONU and restrict its bandwidth demand.	• Use of regression ML technique to recognize the pattern of ONU traffic demand pattern. • Mitigation by halting malicious ONU to operate.	• XGPON • 10 Gbps DS, 2.5 Gbps US • 16 ONUs • Reduced the delay variances and frame loss when malicious ONUs are penalized
[14]	A specialized algorithm is deployed to safeguard the network from degradation attacks.	• Crucial role in detecting and mitigating threats or malicious activities that could potentially degrade the performance or reliability of the network.	• XGPON • 10 Gbps DS, 2.5 Gbps US • 16 ONUs • The algorithm effectively reduces the maximum throughput, thereby mitigating the impact of attacks.
[15]	SE-Dynamic Bandwidth Assignment (DBA) mechanism is leveraged as a secure method to tackle threats.	• Effectiveness of the SE-Dynamic Bandwidth Assignment (DBA) mechanism in securely addressing threats.	• XGPON • 10 Gbps DS, 2.5 Gbps US • 4 ONUs. • Improved throughput and delay of other ONUs when malicious ONUs are penalized.
[16]	To manage the load between heavily and lightly burdened ONUs, an approach called Load Balancing Dynamic Wavelength and Bandwidth Assignment (LB-DWBA) is introduced for PON.	• The method known as Load Balancing Dynamic Wavelength and Bandwidth Assignment (LB-DWBA) is designed specifically for Passive Optical Networks (PONs).	• XGPON • 10 Gbps DS, 2.5 Gbps US • 64 ONUs • This scheme is helpful in maintaining the balancing of load among the mildly and heavily loaded ONUs
[19]	To merge several individual virtual bandwidth maps into a solitary physical bandwidth, map an algorithm is used known as the Load Adaptive Merging Algorithm (LAMA) is used.	• Application of the Load Adaptive Merging Algorithm (LAMA) to merge several individual virtual bandwidth maps into one cohesive physical bandwidth map.	• XGPON • 10 Gbps DS, 2.5 Gbps US • 16 ONUs • Notice an efficient allocation of bandwidth

Normally, there are a lot of challenges for PON Security the Transmission control protocol (TCP) which is the Congestion Control Algorithm, can affect the received bandwidth of targeted network users is the major problem

for PON Security. In X-GPON the degradation attack normally affects the network's upstream transmission. The denial of service attack is more harmful and leads to crash the network.

The optical networks like NG-PON2 should more emphasis on access network security because the users are served over a single physical medium. This is because a single attack can affect the large no of users including hundreds of Gbps of transmission.

NGPON2 (Next-Generation Passive Optical Network 2) is a technology that employs TWDM (Time and Wavelength Division Multiplexing) to deliver high-speed broadband services over fiber-optic networks. While NGPON2 offers several advantages. With the growing utilization of fiber-optic networks in dispensing essential services like telecommunications, healthcare, and finance, safeguarding the security of NGPON2 networks becomes imperative. The defense against unauthorized access, eavesdropping, and various security risks like DOS attacks necessitates sturdy encryption, authentication mechanisms, and network security protocols. There is a lack of work in TWDM (NGPON2) [18]. In this research only, investigations are done on different strategies of NGPON2. There is a need to do more work in this area.

Security capabilities including data encryption authentication, and key formation are available with GPON. However, because GPON places such a high emphasis on the idea that all of its components will be physically secure, its security measures especially upstream are mostly slack. Upstream communication is not encrypted assuming high directionality of PON where other ONUs cannot sniff traffic sent by an ONU to OLT. Upstream traffic authentication and encryption are both optional.

4. EXISTING DETECTION AND MITIGATION ALGORITHMS

There are different types of schemes presented by different researchers that are helpful in ensuring PON security. This section discusses in detail two representatives of recent secure-based DBA where the first is based on regression technique while the second DBA focuses on cross-layer effect between the TCP layer and PON's MAC layer.

4.1 Dynamic Bandwidth Assignment (DBA) Scheme

The current DBA techniques lack the capacity to defend against a security assault. In order to identify rogue (attacker) ONUs from their traffic demand patterns, limit their unauthorized bandwidth demands, and only permit bandwidth assignment to them in accordance with the agreed-upon service level agreements. The machine learning approach is used to calculate the ONU traffic demand patterns (SLA). Figure 4 shows the DOS attack scenario in PON.

For a complex learning model, each ONU has a specific bandwidth usage. However, a linear regression model is used in the SA-DBA scheme to differentiate between a normal and faulty ONU. The bandwidth utilization trend of each ONU is specific. To achieve this purpose SA-DBA scheme collects the buffer occupancy report of the T2, T3, and T4 traffic classes of each ONU.

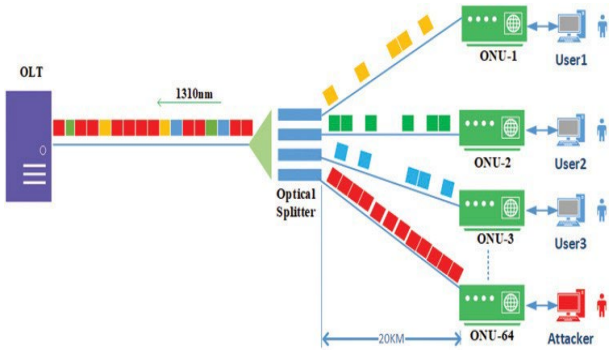

Figure 4. DOS Attack scenario in PON [15]

Then ONU bandwidth demand is calculated. The average recorded ONU bandwidth demand trend from simulation and the corresponding trend line predicted by the regression model is compared for low and high traffic load conditions. The ONUs with high DOS attacks have high bandwidth as compared to all others. This causes the error value positive and very high in the threshold value range. The threshold value is set. This also shows how many ONUs are suffering the DOS attacks.

Due to the improved bandwidth available, the SA-DBA scheme also lowers the standard ONUs' frame loss rate when compared to the EBU [19]. By successfully fighting against DDOS attacks on any ONU and limiting ONU's bandwidth demand so that the bandwidth assignment to other ONUs is not disrupted, the SA-DBA scheme demonstrates its security as a DBA for PON.

4.2 Secured DBA Schemes

A new scheme is presented for defense against the degradation attack that manipulates loopholes in TCP, it follows two steps. When an attack takes place then Alloc ID is captured in the detection method which describes that this ONU has the lowest frame loss and the second step starts which is the mitigation method, in which ONU bandwidth request is denied.

After identifying the attacker, the Alloc ID associated with it goes through mitigation processes, starting with the DBA rejecting its bandwidth request during the next upstream polling and scheduling cycle. A detailed explanation of these detection and mitigation methods is provided in the following sections.

4.2.1 Detection Method

The first step in this scheme is the detection method which is explained by the flow chart as presented in Figure 5. Moreover, the mitigation procedure facilitates additional bandwidth allocation for legitimate ONUs in the subsequent cycle, thereby reinstating equilibrium within the network following an attack and all is described in Figure 5. Additionally, it impedes the incentive behind malicious ONUs' attacks, as the detection method renders masking ineffective [20]. Furthermore, the initiation process incorporates threshold calculations, significantly reducing the likelihood of false alarms.

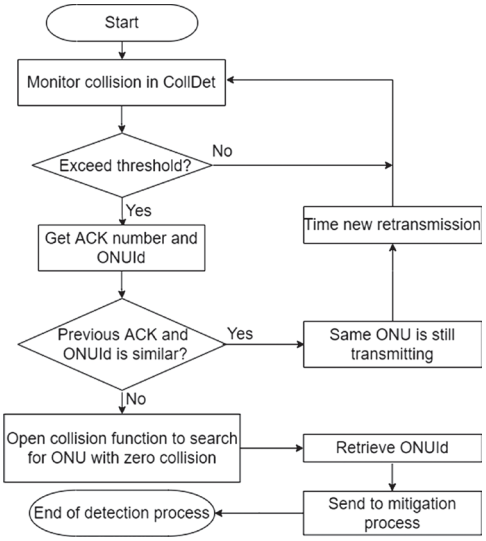

Figure 5. Flow Chart of Detection Method [13]

4.2.2 Mitigation Method

The second step is the mitigation method and the working of this method is explained in the following flow chart as represented in Figure 6. Illustrates the flowchart outlining the mitigation approach. When receiving the Alloc ID, the mitigation process examines the network's Dynamic Bandwidth Allocation (DBA), which registers bandwidth requests from all ONUs, irrespective of the traffic conditions.

Moreover, the mitigation procedure facilitates additional lawful ONUs to utilize the surplus bandwidth allocation in the subsequent cycle, thereby reinstating a degree of equilibrium in the network following an attack [19]. Additionally, it obstructs the incitement behind the attack for malicious ONUs, as the detection method renders the attack untraceable.

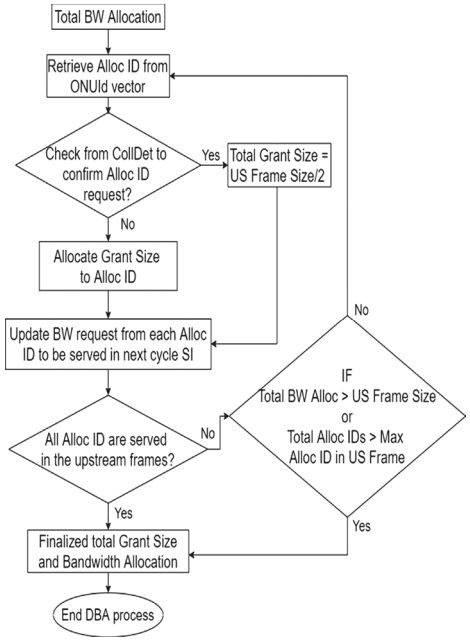

Figure 6. Flow chart of Detection Method [13]

5. HYBRID SECURITY AWARE DBA

Machine Learning (ML) is increasingly being explored for network management in PON with a focus on enhancing security. ML algorithms can help analyze traffic patterns, detect anomalies, and predict potential security threats, offering a more proactive approach to protecting PON infrastructure. As optical networks evolve, integrating ML into PON security measures could play a key role in addressing emerging threats and maintaining network integrity. In this work, we introduce the hybrid security-aware DBA (HSA-DBA) which involves two main steps: identifying malicious ONUs and implementing defenses against attacks. These are detailed in the next sections.

5.1 Method for Identifying Malicious ONUs

Each ONU has a distinct bandwidth usage pattern, analyzed using a deep learning model. A support vector machine helps differentiate normal ONUs from those under attack. The HSA-DBA gathers buffer occupancy data from traffic classes T2, T3 and T4, computing load (i) during the Service Interval (SI). Malicious ONUs demand significantly more bandwidth, resulting in error rates between 30% and 80%. Detection is based on three thresholds: 30%, 50% and 80%.

5.2 Method for Attack Mitigation

The key task is to prevent further attacks on the DBA, as such attacks cause excessive bandwidth loss. To address this, bandwidth allocation can be restricted for the affected ONU and other ONUs with the same SLA in both GPA and SPA phases.

5.3 Method for Surplus Bandwidth Allocation

The third step assigns surplus bandwidth by withholding it from malicious ONUs. This increases the bandwidth available to another ONUs.

6. CONCLUSION

This study offers an insightful analysis into the future landscape of passive optical networks, with a particular focus on the next generation of GPON, which is poised to be the predominant solution for future networks due to its unparalleled security measures, vast bandwidth capacity, and exceptional quality of service. The research provides an extensive examination of GPON security vulnerabilities, categorizing and scrutinizing various threat types, and highlights related work on Dynamic Bandwidth Allocation (DBA) PON security to provide a comprehensive understanding of security frameworks within the GPON domain. In this context, machine learning-based GPON schemes play a crucial role in enhancing security measures. To further improve the adaptability and security of DBA algorithms, we propose a Hybrid Security-Aware DBA (HSA-DBA) model that integrates machine learning techniques. This approach enables traffic demand analysis and ensures more effective bandwidth allocation while adhering to Service Level Agreements (SLAs), thereby enhancing resilience and security against evolving threats. Furthermore, the paper elucidates GPON security architectures, methodologies, and their associated limitations, offering detailed strategies

to address these constraints especially improvement of traffic handling by reducing delays and minimizing frame loss but also provides a dynamic response to emerging security threats. The expected outcomes are increased network efficiency, resilience, and a more secure and adaptive PON infrastructure effectively.

ACKNOWLEDGMENT

This work was supported/funded by the Ministry of Higher Education under Fundamental Research Grant Scheme (FRGS/1/2023/TK07/UTM/02/8).

REFERENCES

[1] H. S. Abbas and M. A. Gregory, "The next generation of passive optical networks: A review," *Journal of Network and Computer Applications*, vol. 67. Academic Press, pp. 53–74, May 01, 2016.

[2] J. F. Balarezo, S. Wang, K. G. Chavez, A. Al-Hourani, and S. Kandeepan, "A survey on DoS/DDoS attacks mathematical modelling for traditional, SDN and virtual networks," Eng. Sci. Technol. an Int. J., vol. 31, p. 101065, 2022

[3] F. Obite, E. T. Jaja, G. Ijeomah, and K. I. Jahun, "The evolution of Ethernet Passive Optical Network (EPON) and future trends," *Optik*, vol. 167. Elsevier GmbH, pp. 103–120, Aug. 01, 2018.

[4] ITU-T Recommendation G.987.3. 10-Gigabit-capable passive optical networks (XG-PON): Transmission convergence (TC) layer specification. vol. 2.0. 2014:1–146.

[5] A. Rufini, E. Tego, F. Matera, V. Policlinico,M. Mellia, and P. Torino, "Bandwidth measurements and capacity exploitation in gigabit passive optical networks," in Fotonica AEIT Italian Conference on Photonics Technologies (2014).

[6] M. Rizvi, S. Singh, and S. Agrawal, *Improved Support Vector Machine for Cyber-attack Detection*. 2011. [Online]. Available: https://www.researchgate.net/publication/277636116.

[7] Y. Wang, C. Lin, Q. L. Li, and Y. Fang, "A queueing analysis for the denial of service (DoS) attacks in computer networks," *Computer Networks*, vol. 51, no. 12, pp. 3564–3573, Aug. 2007

[8] V. Spurny, P. Dejdar, A. Tomasov, P. Munster, and T. Horvath, "Eavesdropping Vulnerabilities in Optical Fiber Networks: Investigating Macro-Bending-Based Attacks Using Clip-on Couplers," in *2023 International Workshop on Fiber Optics on Access Networks, FOAN 2023*, Institute of Electrical and Electronics Engineers Inc., 2023, pp. 47–51.

[9] K. H. Mohammadani, R. A. Butt, W. Nawaz, S. Faizullah, and Z. A. Dayo, "Energy-Efficient Sleep-Aware Slicing-Based Scheduler (SA-SBS) for Multi-Operators Virtualized Passive Optical Networks," *IEEE Access*, vol. 11, pp. 48841–48859, 2023.

[10] M. Furdek, C. Natalino, A. Di Giglio, and M. Schiano, "Optical network security management: Requirements, architecture, and efficient machine learning models for detection of evolving threats [Invited]," *Journal of Optical Communications and Networking*, vol. 13, no. 2, pp. A144–A155, Feb. 2021.

[11] A. Echraibi, J. Flocon-Cholet, S. Gosselin, and S. Vaton, "Deep Infinite Mixture Models for Fault Discovery in GPON-FTTH Networks," *IEEE Access*, vol. 9, pp. 90488–90499, 2021.

[12] S. Drakulic, M. Tornatore, and G. Verticale, "Degradation attacks on Passive Optical Networks," in 2012 16th International Conference on Optical Networking Design and Modelling, ONDM 2012, 2012.

[13] F. M. Atan *et al.*, "Security enhanced dynamic bandwidth allocation algorithm against degradation attacks in next generation passive optical networks," *Journal of Optical Communications and Networking*, vol. 13, no. 12, pp. 301–311, Dec. 2021.

[14] F. M. Atan, N. Zulkifl, S. M. Idrus, N. A. Ismail, and A. M. Zin, "Understanding Degradation Attack and TCP Performance in Next Generation Passive Optical Network," in *Journal of Physics: Conference Series*, IOP Publishing Ltd, Jun. 2021.

[15] R. A. Butt, M. Faheem, M. W. Ashraf, A. Khawaja, and B. Raza, "Attack-Aware Dynamic Upstream Bandwidth Assignment Scheme for Passive Optical Network," *Journal of Optical Communications*, vol. 44, no. 4, pp. 485–493, Oct. 2023.

[16] R. A. Butt, M. Faheem, A. Arfeen, M. W. Ashraf, and M. Jawed, "Machine learning based dynamic load balancing DWBA scheme for TWDM PON," *Optical Fiber Technology*, vol. 52, Nov. 2019.

[17] Effenberger and T. S. El-Bawab, "Passive Optical Networks (PONs): Past, present, and future," Opt. Switch. Netw., vol. 6, no. 3, pp. 143–150, 2009.

[18] S. Rahman, N. Zulkifli, and A. H. Sham, "Physical Layer Investigation on the Coexistence Strategies of GPON, NGPON1 and NGPON2," in *International Conference on Software, Knowledge Information, Industrial Management and Applications, SKIMA*, Institute of Electrical and Electronics Engineers Inc., 2023, pp. 154–158.

[19] S. H. Mohammad, N. Zulkifli, and S. M. Idrus, "Dynamic bandwidth allocation algorithm for long reach passive optical network," *Telkomnika (Telecommunication Computing Electronics and Control)*, vol. 19, no. 3, pp. 738–746, Jun. 2021.

[20] Y. Cui, Q. Qian, C. Guo, G. Shen, Y. Tian, H. Xing, and L. Yan, "Towards DDoS detection mechanisms in software-defined networking," *Journal of Network and Computer Applications*, vol. 190, p. 103156, 2021.