SINERGI Vol. 29, No. 1, February 2025: 185-196
http://publikasi.mercubuana.ac.id/index.php/sinergi
http://doi.org/10.22441/sinergi.2025.1.017

Support Vector Machine (SVM) based Detection for Volumetric Bandwidth Distributed Denial of Service (DVB-DDOS) Attack within Gigabit Passive Optical Network

Sumayya Bibi[1], Nadiatulhuda Zulkifli[1*], Ghazanfar Ali Safdar[2], Sajid Iqbal[3]
[1]Faculty of Electrical Engineering, Universiti Teknologi Malaysia, Malaysia
[2]Universiti of Bedfordshire, United Kingdom
[3]King Faisal University, Saudi Arabia

Abstract
The dynamic bandwidth allocation (DBA) algorithm is highly impactful in improving the network performance of gigabit passive optical networks (GPON). Network security is an important component of today's networks to combat security attacks, including GPON. However, the literature contains reports highlighting its vulnerability to specific attacks, thereby raising concerns. In this work, we argue that the impact of a volumetric bandwidth distributed denial of service (DVB-DDOS) attack can be mitigated by improving the dynamic bandwidth assignment (DBA) scheme, which is used in PON to manage the US bandwidth at the optical line terminal (OLT). Thus, this study uses a support vector machine (SVM), a machine learning approach, to learn the optical network unit (ONU) traffic demand patterns and presents a hybrid security-aware DBA (HSA-DBA) scheme that is capable of distinguishing malicious ONUs from normal ONUs. In this article, we consider the deployment of the HSA-DBA scheme in OMNET++ to acquire the monitoring data samples used to train the ML technique for the effective classification of ONUs. The simulation findings revealed a mean upstream delay improvement of up to 63% due to the security feature offered by the mechanism. Moreover, significant reductions in upstream delay performance, including 63% for TCONT2, 65% for TCONT3, and 95% for TCONT4, along with a reduction in frame loss rates for normal ONU traffic, were observed. This research provides a significant stride towards secure GPONs, ensuring reliable defense mechanisms are in place, which paves the way for more resilient future broadband network infrastructures.

Keywords:
Attack detection system;
Dynamic Bandwidth Assignment;
Machine learning;
Passive optical Network;
Kernel SVM;

Article History:
Received: April 24, 2024
Revised: June 24, 2024
Accepted: July 21, 2024
Published: January 4, 2025

Corresponding Author:
Nadiatulhuda Zulkifli
Universiti Technologi Malaysia,
81310 UTM, Johor, Malaysia
Email: nadiatuhuda@utm.my

INTRODUCTION

The adaptation of passive optical networks (PONs) has been dramatically increasing because of their ability to provide higher transmission speeds, guaranteed quality of service (QoS), cost effectiveness, and a preferred fiber-access network solution [1][2].Conventional methods of strengthening network security by using encryption and cryptography are frequently applied at the network's foundational layers. However, even with all the proposals for optimizing security, vulnerabilities still frequently surface during the network installation stage, particularly when performing optical network unit (ONU) discovery and identification.

Numerous issues with the physical layer of the GPON compromise data transport reliability and security. These problems therefore get addressed at a lower level and are unrelated to the current topic. Among these difficulties is signal

attenuation. Over extended distances, the optical signal can weaken and lead to degradation and information degradation. Using optical amplifiers and repeater devices at the necessary, precise intervals solves this problem. The GPON's physical layer may face several challenges affecting security and data transmission integrity. These challenges include:

Fiber tapping: A malicious user could become capable of intercepting or injecting unsafe information into the signal by gaining unauthorized physical access to the fiber optics. Measures of physical security like locked enclosures and regular inspections reduce the threat from the article.

Optical Reflection and Dispersion: Data integrity issues can arise from signal reflections and dispersion caused by defects or damage to the optical cable. Reducing these issues requires ensuring that fiber installation and maintenance adhere to the highest standards in line with industry recommendations.

Temperature Variation: Propagation faults can occur when exceptionally high temperatures negatively impact the efficiency of the fiber's optical layer. Implementing climate monitoring systems and temperature-stable components can help manage these issues. In GPON networks, several critical factors influence successful data transmission, as demonstrated in the research.

Long Lengths: Signal degradation and latency become more pronounced as the distance between the OLT and ONUs increases. Adjusting delay-sensitive parameters and using amplifiers to minimize losses are necessary to maintain signal quality.

Increasing ONUs: Adding more ONUs on the same network segment can lead to increased collision occurrences and spectrum contention within the time division multiplexing (TDM) upstream.

To ensure reliable and secure fiber optic networks, several mitigation and optimization techniques are essential. Signal degradation can be addressed by using high-quality fiber optics, installing amplifiers or repeaters where necessary, and carefully adjusting power levels to minimize losses. Additionally, employing DBA alongside effective bandwidth distribution methods can significantly enhance resource utilization and reduce contention, particularly in TDM systems. These techniques are critical as network demands increase and more ONUs are added to network segments.

Security at the network and transport layers (Layers 3 and 4) is also vital for maintaining performance and protecting data. At the network layer, IP spoofing is a significant risk, where intruders use malware to impersonate legitimate devices. This can be mitigated with IP authentication and filtration systems, helping ensure only trusted sources communicate on the network. In the transport layer, TCP/UDP flood attacks can overwhelm network resources by sending large volumes of packets, but rate-limiting and anomaly-detection systems are effective at minimizing this threat. Additionally, unauthorized access to ongoing sessions (connection hijacking) poses privacy risks, which can be countered by secure session management and encryption protocols like TLS and SSL.

In PON, encryption protocols are used to prevent eavesdropping, data tampering, and denial-of-service (DoS) attacks. The PON specification supports the advanced encryption standard (AES) with asymmetric keys to secure data transmission [3][4]. However, a potential vulnerability remains in the key distribution process, as it is not encrypted, leaving a gap for possible exploitation. Addressing these security challenges across different network layers is crucial for the robustness of modern fiber optic networks, ensuring both optimal performance and resilience against cyber threats.

PON provides customers with access via a point-to-multipoint tree structure. Traffic from the OLT and distribution network can be routed across a single fiber in a typical broadcasting and time-division multiplexed manner, respectively [1]. The communication lines connecting these components often operate at different wavelengths, using the 1520 to 1540 nm range exclusively for upstream transmission [5].

A volumetric attack originating from an ONU stem from the network and transport layers. This type of attack at the network and transport layers has the potential to cause a notable surge in traffic frames on both the downstream (DS) and upstream (US) links of the PON. Specifically, a targeted ONU may experience heightened upstream bandwidth demand, leading to an uneven distribution of bandwidth among the remaining ONUs [6, 7, 8].

A volumetric attack can cause an ONU to exhaust its bandwidth continuously, consuming a substantial portion of available network resources. Consequently, other ONUs experience reduced bandwidth, leading to increased upstream latency and significant fluctuations in performance [9][10]. While most DBA techniques were designed without consideration for network attacks, security has recently become a priority in optical access networks. However, few DBA approaches actively address this concern. Notably, machine learning

(ML) has not yet been explored in studies on secure bandwidth allocation methods. Instead, current security protocols rely on threat detection and mitigation through collision monitoring at each ONU [11]. This approach focuses on threat detection and mitigation through collision monitoring at each ONU where ONU with the fewest collisions is identified as a potential threat and assigns penalties accordingly. Moreover, because it depends on TCP window behavior, this method is effective only in TCP traffic environments where TCP window behavior can be analyzed.

Another study employs regression analysis to identify threats based on the traffic demand of ONUs in PON [10]. However, this method has limitations as it overlooks certain types of traffic and the impacts of higher-layer protocols, such as TCP. Thus, the current study suggests enhancing the DBA scheme by integrating machine learning techniques beyond regression analysis to better analyze ONU traffic patterns. Overall, most DBA algorithms are not security conscious, thus, they tend to overlook potential network attacks, with only a few exceptions as described above since security is an emerging topic in optical access networks.

The aforementioned researchers primarily concentrated on specific types of threats and network events. However, ML has recently demonstrated significant potential in enhancing QoS, interoperability, and resource utilization in optical networks. To assess the impact of attacks, a new DBA scheme, referred to as HSA-DBA, was implemented in the PON. The initial training datasets were derived from the OMNET++ modeling framework for GPON. Using OMNET++ simulations as the experimental testbed, the DBA extracted data from ONUs to determine their bandwidth consumption. This generated data was then analyzed using a kernel-based method, specifically Support Vector Machine (SVM), to differentiate between malicious and normal ONUs.

Non-linear correlations among the input feature labels and labels for output are easily captured by SVM. In cases of security, where the accurate distinction between malicious and lawful behaviors is crucial, regularization parameters used by SVM help prevent over-fitting and ensure that the algorithm generalizes to new information well, particularly in complex and highly dimensional cases. Furthermore, SVM's kernel approach enables it to handle data with high dimensions effectively by explicitly shifting variables into higher-dimensional spaces, where non-linear correlations are simpler to detect.

The standard DBA technique is inadequate for addressing the current challenges posed by volumetric attacks on malicious ONUs. This paper focuses on developing a security-aware DBA strategy combined with a machine learning-based detection scheme to identify these malicious ONUs. By limiting bandwidth assignments to detected threats, this approach aims to mitigate the impact of volumetric attacks. To ensure the mechanism's validity and reliability amidst rapid changes in data distributions and features, the integration of anomaly detection techniques is essential. The work utilizes SVM as a classifier, leveraging datasets generated within the OMNET++ simulation environment. Implementing a robust security system that can detect various threats in the GPON FTTX network is crucial. While existing strategies, such as identifying IP packets and tracing their origin at the edge router, can help counter IP spoofing DDoS attacks, they fall short in addressing the effects on the PON's MAC layer.

The primary contributions of this research are as follows:

1. Integration of SVM Model: The implementation of a Support Vector Machine (SVM) model in the current Dynamic Bandwidth Assignment (DBA) system enhances network traffic management through effective attack detection and mitigation.
2. Proposed Attack Detection Methodology: A framework is introduced to detect attacks, allowing for the identification of instances when flow disruptions occur due to network security violations.
3. Performance Assessment: The effectiveness of the proposed method is evaluated in terms of latency and frame loss, comparing it with relevant studies.

The paper is structured as follows: Section 2 reviews the pertinent literature, while Section 3 provides a detailed description of the network bandwidth prediction attack methodology. Section 4 presents the outcomes of the proposed model, including statistical validation and analysis of upstream delay and frame loss. Finally, Section 5 concludes the paper.

METHODOLOGY

Support Vector Machine (SVM)

Support vector machine (SVM) is a powerful supervised machine learning algorithm used for both classification and regression tasks. Although SVM is best known for its effectiveness in classification problems, the workings of the SVM algorithm are to optimize decision

hyperplanes in higher-dimensional space, allowing data points to be accurately classified into their respective categories based on features. Hyperplane refers to and is chosen to maximize the margin of the decision boundary to achieve the closest points of different classes. In linear data, SVM draws a linear hyperplane to separate data vectors. In a non-linear data set, SVM uses a kernel to map into a higher-dimensional space where the data points become linearly separable. In the classification problem, a hyperplane separates two distinct classes, as shown in Figure. 1 where the nearest points to the hyper plane called support vectors. The dataset, which consists of *n*-data points as a whole data set has both training and testing data sets, is represented by the following formula.

$$(X_1, Y_1) \dots (X_n, Y_n) \quad (1)$$

Equation (1) which is used in SVM models where y_n is the class label can be 1 or -1, indicates the category of the class of target they belong to while x_n is the input features use for training.

$$W^T x - b = 0 \quad (2)$$

Equation (2) is a key component of SVM $W^T x$ represent the weighted sum of the input features in terms of *x*. where each feature is the corresponding weight (W) multiple. The hyperplane is shifted along the weights' (W) orientation by the expression $(-b)$. It permits the hyperplane's positioning to be changed to best divide into categories in the data set. This vector corresponds to the normal vector in the Hessian normal form, with the distinction w that is not necessarily a unit vector. The component $b/\|w\|$ indicates the offset of the hyperplane from its origin along the standard vector w . In (3), every point on or above the boundary belongs to each class, labeled as 1. Conversely, in (4), all points below the boundary labeled with -1 belong to the other class.

$$W^T x - b = 1 \quad (3)$$

$$W^T x - b = -1 \quad (4)$$

The distance between the two hyperplanes geometrically spans $2/\|w\|$. To increase the distance between the planes, it is imperative to decrease the magnitude of *w*. This magnitude is used to calculate the distance between a point and a plane. For every instance, it sets limitations akin to those in (5) and (6) to guarantee that data points do not fall into the margin.

$$W^T x_i - b \geq 1 \qquad v_i = 1 \quad (5)$$

$$W^T x_i - b < 1 \qquad v_i = -1 \quad (6)$$

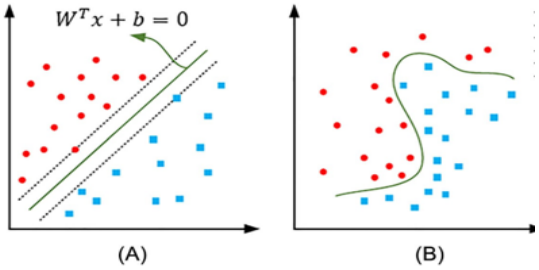

Figure 1.The SVM diagram (A) with linear decision boundary and (B) with nonlinear decision boundary

Furthermore, the following is a summary of the stages involved in implementing the SVM algorithm:

1. To incorporate support vector elements into the HSA-DBA plan.
1. Define the learner for the linear module.
2. To apply the hard margin function.
3. To organize and import all generated attacks.
4. To train the SVM classifier by using 70% data for training purpose of the generated attacks.
5. To assess the classifier's effectiveness by using 30% test data as a created attack.
6. Finally, perform a classification between normal and faulty ONUs.

A common form of network attack is the volumetric attack, originating from the application and transport layers and directed towards a specific ONU, with a focus on targeting the UDP or TCP logical ports. This attack flooded the network with an excessive number of packets, resulting in network congestion and ultimately leading to complete service failure for a specific ONU. In the context of a PON, the term "malicious ONU" refers to a user connected to an ONU who initiates an attack [12, 13, 14].

Equation (7) is used to characterize the mean waiting distance when the poison traffic rate (M/G/1 queueing model) is taken into consideration. Here, λ denotes the frequency of ONU arrivals, x^2 is the average time taken to serve an ONU, and ρ is a measure of the PON's workload [11]. (8) is used to find this factor, which is dependent on the speed at which ONUs are served. (9) and (10) are to express the average upstream delay, D_{us} and downstream delay, D_{DS}, respectively. These delays deteriorate the overall upstream link performance and negatively affect another ONU's ability to use upstream bandwidth. As a result of the attack, one ONU experiences an increase in arrival rate (λ), which lowers another ONU's service rate (μ). This is a result of the malicious ONU using a lot of bandwidth, which raises both upstream and downstream latency in the study [10].

$$W = \frac{\lambda x^2}{2(1-\rho)} \quad (7)$$

$$\rho = {}^{\lambda}/_{\mu} \quad (8)$$

$$D_{DS} = W_{DS} + \frac{RTT}{2} \quad (9)$$

$$D_{US} = W_{US} + \frac{RTT}{2} + \frac{SI}{2} \quad (10)$$

The proposed conceptual framework of the model implementation is depicted in Figure 2. Various studies have been carried out where different ML models being used for implementing prediction of attack detection and mitigation [15,16,17,18,19,20,21]. Our study is primarily concerned with data collection from PON traffic. We perform preprocessing procedures to eliminate all null or duplicate entries from our data set to guarantee its integrity. After that, we continue with getting the dataset ready to be divided into both testing and training subsets. Thirty percent of the dataset is set aside for testing, while seventy percent is used for training. Our goal is to anticipate network traffic patterns by using supervised ML models, notably SVM. With this method, our system may use predictive surveillance and mitigation techniques to recognize and deal with both malicious and lawful ONUs.

System Model and Performance Evaluation

A PON comprising 64 ONUs and one OLT with a fiber distance of 40 km in the ODN, as shown in Figure 3, was developed using the OMNET++ simulation environment. Figure 4 illustrates the generation of data set by simulation. The parameters used for the proposed method are detailed in Table 1, while Table 2 illustrates the key simulation parameters. A synthetic dataset was created to train a classifier to detect malicious ONUs in a PON, based on their bandwidth usage patterns. This dataset includes bandwidth demand profiles from ONUs recorded under normal conditions and during simulated attacks.

Table 1. SVM Parameter Description

Parameter	Description
w	Vector
b	scalar
$y(x)$	Hyperplane function
$x_1, x_2 \ldots, xN$,	Training vectors
$\sum$	Sum of values

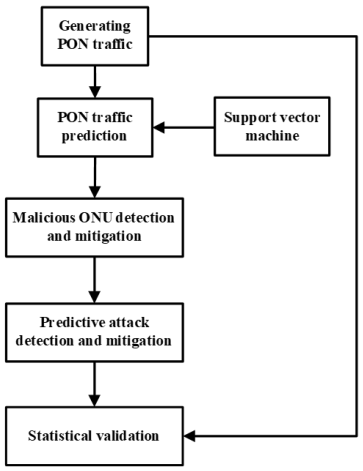

Figure 2. Conceptual framework

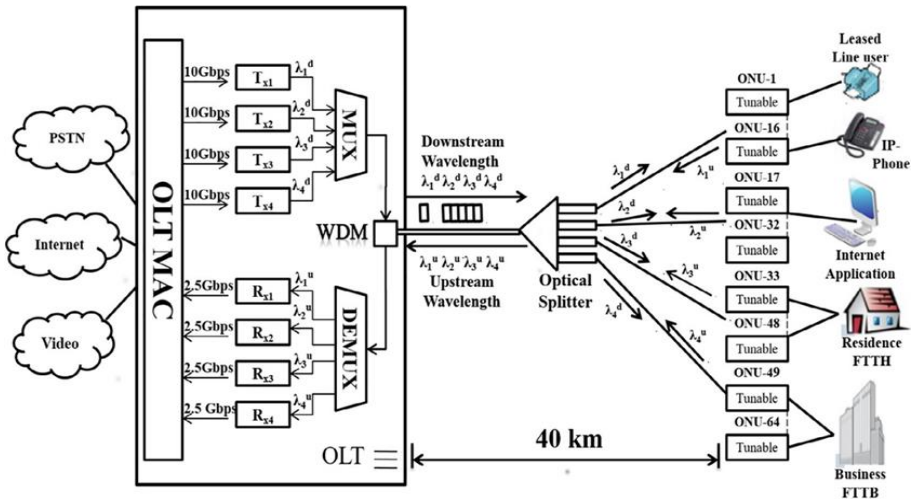

Figure 3. Typical TWDM PON Architecture [10]

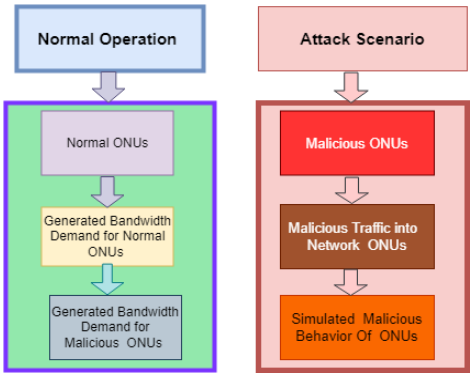

Figure 4. Normal and Malicious ONUs

Table 2. Simulation Parameters

Parameter	Values/Details
US/DS Line rates	40Gbps/10bps
US/DS Traffic Load	0.1 to 1
ONU to OLT Line rate	200 Mbps
Average traffic frame size F_{avg}	Follows the Broadcom CATV distribution as in
Bandwidth Assignment for T2	ABmin=AB sur=7812 with SImax=SImin=5
Bandwidth Assignment for T3	ABmin=AB sur=7812 with SImax=SImin=10
Bandwidth Assignment for T4	ABsur=15,624 and SI max=10(100 Mbps)

The network performance is analyzed using a traffic generator based on a Poisson distribution [11]. Traffic is produced by computing the inter-arrival time, *IIT* using an exponential function that aligns with the designated traffic load. The traffic generator determines the arrival rate of traffic per ONU. F_{avg} signifies the average size of packet frames in the generated traffic, while '*N*' indicates the total count of active optical network units. The traffic load is described as the proportion of the total traffic bytes sent by all optical network units to the link rate. The system model diagram is explained in Figure 3. The volumetric attack is simulated by modeling 64 ONUs with their traffic load varying from 0.01 to 1. The simulation was conducted for a duration of one minute in each run.

Hybrid Security Aware DBA (HSA-DBA)

The hybrid security aware DBA (HSA-DBA) consists of two key steps, firstly the identification of malicious ONU and secondly the implementation of defensive measures against attacks. These two steps are explained in the following two sections.

Step 1: Malicious ONU Detection Algorithm

Each ONU exhibits a distinct trend in bandwidth utilization and requires the application of a deep learning model. However, classification between a regular ONU and an ONU affected by an attack is achieved through a SVM model. For this HSA-DBA scheme, the buffer occupancy reports from traffic classes T2, T3, and T4 for each ONU are calculated as a vector variable load (i) during the service interval (SI). A SVM model is used in the prediction of bandwidth demand for all ONUs. The malicious ONU requires more bandwidth as compared to all normal ONUs. Their bandwidth demand significantly exceeds that of all other ONUs, resulting in consistently positive and notably high error rates ranging from 30% to 80%. The detailed workings of the proposed algorithm are observed in algorithm 1.

ALGORITHM1: MALICIOUS ONU DETECTION

1: Start x [64] using input features
2: Start y [64] by corresponding output (Load ONU)
3: Adjust learning Rate = 0.00001
4: Set epochs = 1000
5: Set weight = 0.0
6: Set bias = 0.0
7: Iterate over epochs from 1 to epochs
8: Compute total Error = 0.0
9: Loop over data points:
10: $Compute\ prediction = weight * x[i] + bias$
11: Find error = abs(y[i] - prediction)
12: Sum both error and total Error
13: we Modify weights and bias of inputs using gradient descent
if $x[i]$ is not equal to 0
14: Show output: Epoch, epoch, Total Error, total Error.
15: Show "Predictions and malicious ONUs:"
16: Loop over samples:
17: Compute prediction = weight * x[i] + bias
18: Find error1 = y[i] - prediction
19: Output "x = ", x[i], " Load ONU = ", y[i], " Bandwidth Demand = ", prediction, " Error = ", error1
20: Determine, malicious ONUs:
21: **If** abs (error1) > 1000 then
22: Output "ONU = ", i, "is a malicious ONU"
23: **Else**
24: Output "ONU = ", i, "is a Normal ONU"
25: Output

Step 2: Mitigation Of Attack Algorithm

The most important task is to protect the DBA from attacking again with the same type. Due to this attack, as a result more and more bandwidth draining out. For this purpose, we limit the bandwidth assignment to such ONUs and also all other ONUs having the same service level agreement (SLA) in both guaranteed phase allocation (GPA) and surplus phase allocation (SPA). To achieve this, we proposed the modified EBU scheme. The bandwidth assignment process uses the following algorithm first to separate the normal and malicious ONU [22]. A list of malicious ONU is created. Bandwidth assignment is stopped to ONU, which are all malicious, and assigned to all normal ONU as per schedule [23]. The algorithm does not assign the surplus bandwidth to malicious ONUs. Restrictions are set higher to assign the bandwidth to malicious ONU.

ALGORITHM 2: MITIGATION OF ATTACK

1: **Input**: R_p, Avg Tp, VBp [k], F_bytes
2: **Output**: Bandwidth TCONTs
3: n=64, i = 0, j=16, p =2,3,4
4: **For** (l= i to j)
5: K (l % n)
6: **If** (F_Bytes > 0)
{
7: **If** (VBp [k]>0
8: ON_uno = Search (M_ONUs.begin(), M-ONUs. End (), K);
9: **If** (ON_uno 1 = M_ONUs.end ())
10: Grant = min (VBp [k], Avg Tp,F_Bytes);
11: Rp = 0;
11: **Else**
12: Grant = min {VBp[k], Rp, F_Bytes};
13: Rp= Rp_Grant
14: **Endif**
15: F_Bytes = F_Bytes_Grant
16: **Endif**
17: **Endif**
18: **Start ++;**
19: **End++;**
20: **End for**

Step 3: Surplus Bandwidth Assignment Algorithm

The third step involves allocating surplus bandwidth in the excess bandwidth assignment stage. This is accomplished by refraining from granting surplus bandwidth to a malicious ONU. Limiting the bandwidth available to malicious ONUs results in increased bandwidth allocation for the remaining ONUs.

ALGORITHM 3: SURPLUS BANDWIDTH ASSIGNMENT

1: **Inputs**: F_Bytes, M_ONUs;
2: **Output**; S_Grant_T CONTs
3: **If** (F_Bytes>0)
4: Raw = F_Bytes;
5: M_size = M_ONUs.size();
6: Ex_Bytes= Raw/ (n-M_size);
7: **For** (i:0 to n)
8: ONUno = Find (M_ONUs.begin(), M_ONUs.end(),K);
9: **If** (ONUno!= R_ONUs.end()_
10: S_Grant= Ex_Bytes
11: Else
12: S_Grant=0

Figure 5 explains all three steps involved in the implementation of HSA-DBA. The first step is the implementation of the malicious ONUs detection algorithm. The second step is the implementation of mitigation of attacks. The third step is the implementation of surplus band width assignment algorithm.

RESULTS AND DISCUSSION

The HSA-DBA scheme's performance is compared to a recent non-secure DBA, known as the EBU algorithm [20, 21, 22, 23, 25, 26, 27]. Figure 5 shows in detail all the implementation steps of HSA-DBA.

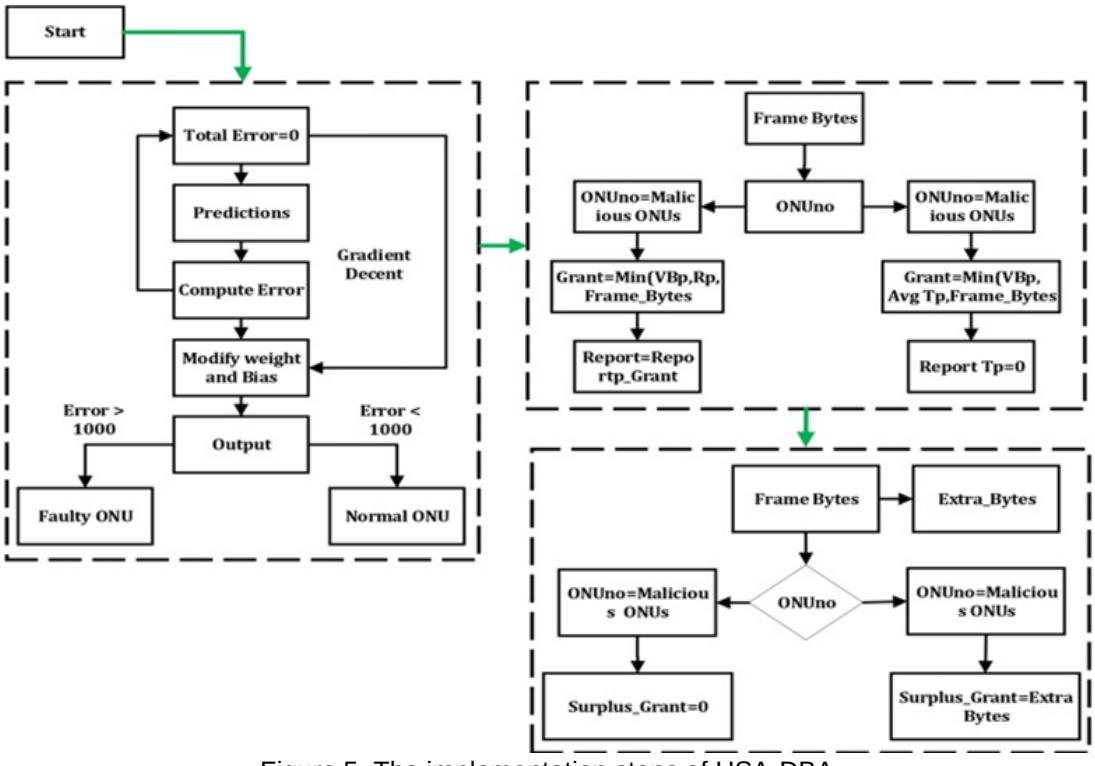

Figure 5. The implementation steps of HSA-DBA

Figure 6 to 9 showcase the average delays of traffic classes T2, T3, and T4, along with the frame loss results. In order to exclusively examine how the volumetric attack affected other ONUs and how the HSA-DBA scheme improved performance, all of the results are documented for the normal ONUs and not for the malicious ONUs. The delay results make it clear that the EBU DBA lacks the ability to distinguish between a regular ONU and a malicious ONU and, hence, is unable to counter the volumetric attack on an ONU, causing the malicious ONUs to use a lot of bandwidth.

This leads to a decrease in the availability of bandwidth for the remaining ONUs. The influence of the volumetric attack intensifies under heavier traffic conditions, as the excessive bandwidth is heavily utilized by malicious ONUs, thereby leaving minimal surplus bandwidth for the regular Onus. Conversely, the HSA-DBA restricts the allocation of guaranteed and excess bandwidth to malicious ONUs, aligning it with the mean bandwidth requirement of another optical network unit under the same service level agreement [25][26].

This leads to increase bandwidth availability for another ONUs compared to the EBU scheme. In figure 6 at lower traffic load (0 to 0.2), the mean upstream delay for both methods are quite low and similar. As the load increases beyond 0.2, the EBU scheme's mean delay rises more rapidly than that of the HSA-DBA scheme. At the highest traffic load (1.0) the mean upstream delay for the EBU scheme is significantly higher than that for the HSA-DBA scheme.

The HSA-DBA scheme appears to be more efficient in handling higher traffic loads with lower mean upstream delays compared to the EBU scheme. Figure 7 shows that the HSA-DBA scheme consistently outperforms the EBU scheme in term of maintaining a lower mean upstream delay across all traffic loads.

The EBU method shows significant fluctuations in mean upstream delay, especially peaking at traffic load of around 0.6, which indicates potential instability under varying traffic conditions. Figure 8 shows that HSA-DBA scheme consistently outperforms the EBU scheme by maintaining a lower mean upstream delay across all traffic loads. Overall, the HSA-DBA scheme appears more efficient and stable, providing lower delays under increasing traffic loads compared to the EBU scheme.

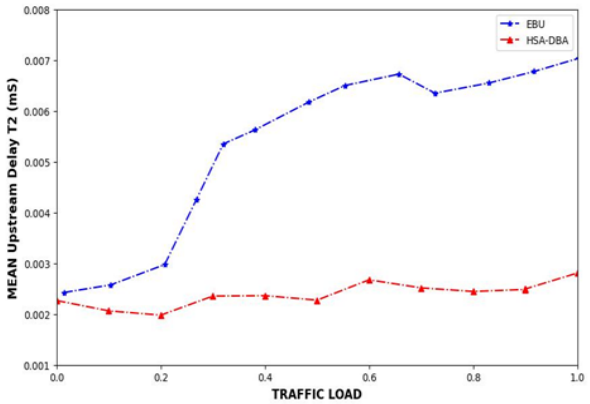

Figure 6. Mean upstream delay vs load for TCONT2 traffic

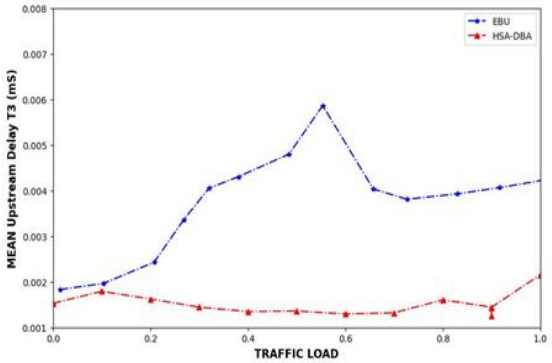

Figure 7. Mean upstream delay vs load for TCONT3 traffic

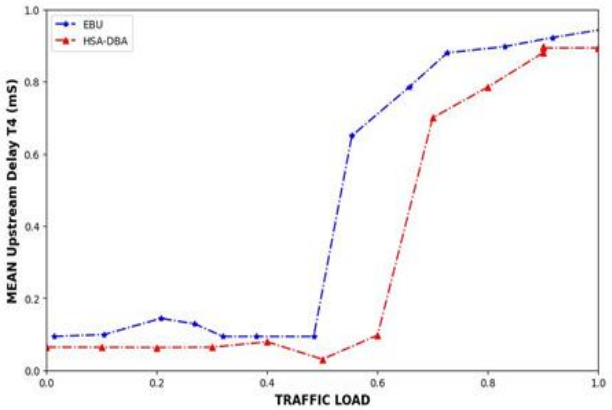

Figure 8. Mean upstream delay vs load for TCONT4 traffic

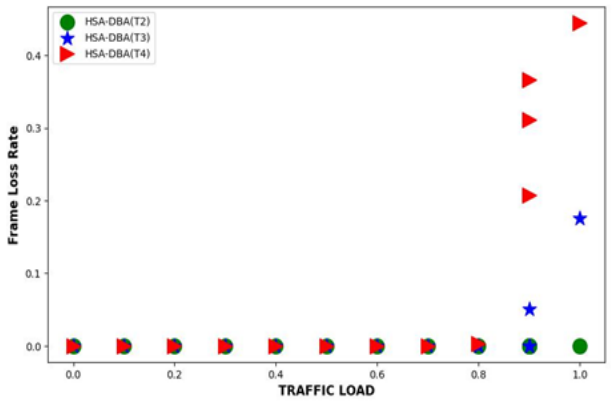

Figure 9. Frame loss rate vs traffic load

Figure 9 shows that implementation of HSA-DBA also reduces frame loss rate of the normal ONUs as compared to the EBU scheme due to higher bandwidth availability. Thus, under HSA-DBA, the delays for T2, T3, and T4 are reduced by 63%, 65%, and 95%, respectively, compared to the EBU scheme. All the excellent results shown in the presented work indicate that the delays for T2, T3, and T4 are due to the implementation of SVM as a classifier. Its excellent performance gives excellent results.

The SVM model achieves superior classification accuracy in distinguishing between normal and malicious ONUs. In earlier work, the DBA scheme lacked integrated security measures, resulting in higher delay outcomes. The study in [28] applied SVM for multiclass classification due to its robust performance, while [29] demonstrated SVM's effectiveness in enhancing fault detection accuracy in passive optical neural networks. Additionally, researchers in [30] and [31] employed ML-SVM for threat detection in optical networks, achieving notable improvements in detection accuracy.

In its entirety, the HSA-DBA system demonstrates its efficacy as a secure Dynamic Bandwidth Allocation (DBA) solution for passive optical networks (PONs) [20, 22, 24] by adeptly safeguarding against volumetric attacks targeting any ONU. This is accomplished through the strategic constraint of the bandwidth demands of the affected ONU, ensuring that the allocation of bandwidth to another ONUs remains unaffected. The standard allocation of bandwidth to the unauthorized ONUs not only adheres to the SLA but also constrains the traffic burden imposed by the malicious ONU. ML improves classification and detection by optimizing signal processing, resource use, and network management. It boosts data transmission efficiency, enhances error correction, and supports adaptive system development [32][33].

CONCLUSION

In this investigation, we introduce a new volumetric attack-resistant DBA scheme tailored for TWDM-PON. This enhanced DBA incorporates advanced detection and mitigation techniques, serving as a robust defense mechanism against potential attacks. The proposed scheme has the capability to identify malicious ONUs during the DBA process by employing a support vector

machine learning algorithm that learns the traffic demand patterns of all ONUs. Thus, it mitigates volumetric attacks while adhering to the service level agreement agreed upon with the user. This work significantly contributes to improving network security in PON. The effectiveness of the suggested scheme is assessed using a simulation testbed for PON implemented in OMNET++. The results validate our claim and the success of the new scheme.

REFERENCES

[1] R. Bonk, “The Future of Passive Optical Networks,” in *25th International Conference on Optical Network Design and Modelling, ONDM 2021*, Institute of Electrical and Electronics Engineers Inc., Jun. 2021.doi: 10.23919/ONDM51796.2021.9492398.

[2] R. Singh and M. Kumar, “A comprehensive analysis for the Performance of Next Generation Passive Optical Network,” in *2021 International Conference on Smart Generation Computing, Communication and Networking*, Smart Gencon 2021, Institute of Electrical and Electronics Engineers Inc., 2021, doi: 10.1109/smartgencon51891. 2021.9645886.

[3] V. Clupek, T. Horvath, P. Munster, and V. Oujezsky, “New security improvements in next-generation passive optical networks stage 2,” *Applied Sciences*, vol. 9, no. 20, pp. 1–16, 2019, doi: 10.3390/app9204430.

[4] W. C. Lyu, Y. Qiu, J. Han, N. Deng, and J. Xu, “On the security weaknesses of a power splitting- based passive optical network,” *Optik* (Stuttg), vol. 174, pp. 623–629, Dec. 2018, doi: 10.1016/j.ijleo.2018.08.128.

[5] P. Pinho and D. Camacho, “Analysis tool for passive optical access network,” *Journal of Microwaves, Optoelectronics and Electromagnetic Applications*, vol. 20, no. 2, pp. 395–406, Jun. 2021, doi: 10.1590/2179-10742021V20I21185.

[6] Y. Li, Y. Zhao, J. Li, X. Yu, Y. Zhao, and J. Zhang, “DDoS Attack Mitigation Based on Traffic Scheduling in Edge Computing-Enabled TWDM-PON,” *IEEE Access*, vol. 9, pp. 166566–166578, 2021, doi: 10.1109/ACCESS.2021.3134671.

[7] A. Usman, N. Zulkifli, M. R. Salim, K. Khairi, and A. I. Azmi, “Optical link monitoring in fibre-to-the-x passive optical network (FTTx PON): A comprehensive survey,” *Optical Switching and Networking*, vol. 39. Elsevier B.V., Nov. 01, 2020. doi: 10.1016/j.osn.2020.100596.

[8] A. N. Kadhim and S. B. Sadkhan, “Security Threats in Wireless Network Communication-Status, Challenges, and Future Trends,” in *2021 International Conference on Advanced Computer Applications*, ACA 2021, Institute of Electrical and Electronics Engineers Inc., 2021, pp. 176–181. doi: 10.1109/ACA52198.2021. 9626810.

[9] 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. doi: 10.1088/1742-6596/1933/1/012107.

[10] R. Aslam, F. M. Faheem, M. W. Ashraf, K. 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, 2023. doi: 10.1515/joc-2019-0142..

[11] F. M. Atan, N. Zulkifli, S. M. Idrus, N. A. Ismail, A. M. Zin, A. Ramli, and N. Md. Yusoff, "Security enhanced dynamic bandwidth allocation algorithm against degradation attacks in next generation passive optical networks," *Journal of Optical Communications and Networking*, 13, 301-311 2021 doi: 10.1364/JOCN.434739.

[12] V. Sharma, S. Sharma, and A. Kumar, “Passive Optical Network: A New Approach in Optical Network,” *Proc. - 2020 International Conference on Advances in Computing, Communication and Materials (ICACCM) 2020*, pp. 295–300, 2020, doi: 10.1109/ICACCM50413.2020.9213059..

[13] R. Barona and E. Baburaj, “An efficient DDoS attack detection and categorization using adolescent identity search-based weighted SVM model,” *Peer-to-Peer Network Appl.cations*, vol. 16, no. 2, pp. 1227–1241, Mar. 2023, doi: 10.1007/s12083-023-01460-6.

[14] Y. Wang *et al.*, “Dynamic Bandwidth allocation algorithm based on traffic classification with the aid of LSTM and GRU for industrial passive optical networks,” in *2023 21st International Conference on Optical Communications and Networks, ICOCN 2023*, Institute of Electrical and Electronics Engineers Inc., 2023. doi: 10.1109/ICOCN59242.2023.10236158.

[15] L. Yang, Q. Zhang, Z. Huang, and W. Zhang, “Dynamic Bandwidth Allocation (DBA) Algorithm for Passive Optical Networks,” in *2020 30th International Telecommunication*

Networks and Applications Conference, ITNAC 2020, Institute of Electrical and Electronics Engineers Inc., Nov. 2020. doi: 10.1109/ITNAC50341.2020.9315119.

[16] Y. Luo, A. Shen, and F. Effenberger, "Dynamic Bandwidth Assignment with Upstream Crosstalk Control in Passive Optical Network Coexistence," in *Asia Communications and Photonics Conference, ACP*, Optica Publishing Group (formerly OSA), 2022, pp. 1030–1034. doi: 10.1109/ACP55869.2022.10088725.

[17] Y. A. Chen, "A Machine Learning Based Scheme for Indoor/Outdoor Classification in Wireless Communication Networks," in 2023 International Conference on Consumer Electronics - Taiwan, ICCE-Taiwan 2023 - Proceedings, Institute of Electrical and Electronics Engineers Inc., 2023, pp. 745–746. doi: 10.1109/ICCE-Taiwan58799.2023.10226696.

[18] N. Zaeri and R. R. Qasim, "Intelligent Wireless Sensor Network for Gas Classification Using Machine Learning," in *IEEE Systems Journal*, vol. 17, no. 2, pp. 1765-1776, June 2023, doi: 10.1109/JSYST.2023.3238357

[19] M. Bhavsar, K. Roy, J. Kelly, and O. Olusola, "Anomaly-based intrusion detection system for IoT application," *Discoveriy for Internet Things*, vol. 3, no. 1, 2023, doi: 10.1007/s43926-023-00034-5.

[20] Y. Luo, C. Zhang, X. Wang, X. Liang, and K. Qiu, "Robust Key Update With Controllable Accuracy Using Support Vector Machine for Secure OFDMA-PON," *Journal of Lightwave Technology*, vol. 41, no. 14, pp. 4663–4671, Jul. 2023, doi: 10.1109/JLT.2023.3244202.

[21] J. Bhayo, S. A. Shah, S. Hameed, A. Ahmed, J. Nasir, and D. Draheim, "Towards a machine learning-based framework for DDOS attack detection in software-defined IoT (SD-IoT) networks," *Engineering Applications of Artificial Intelligence*, vol. 123, Aug. 2023, doi: 10.1016/j.engappai.2023.106432

[22] A. Usman, N. Zulkifli, M. R. Salim, and K. Khairi, "Fault monitoring in passive optical network through the integration of machine learning and fiber sensors," *International Journal of Communication Systems*, vol. 35, no. 9, Jun. 2022, doi: 10.1002/dac.5134

[23] F. N. Khan, Q. Fan, C. Lu, and A. P. T. Lau, "Machine learning methods for optical communication systems and networks," in *Optical Fiber Telecommunications VII*, Elsevier, 2019, pp. 921–978. doi: 10.1016/B978-0-12-816502-7.00029-4

[24] D. Kaur, G. Gupta, and V. Jha, "A Game Theoretic Bandwidth Allocation Scheme towards Improving the Fairness of XG-PON Systems," *The International Conference on ICT Convergence*, vol. 2021-Octob, pp. 921–926, 2021, doi: 10.1109/ICTC52510.2021.9620757

[25] S. Venkatesh, X. lu, T. Bingjun, and S. Kaushik, "Secure space–time-modulated millimetre-wave wireless links that are resilient to distributed eavesdropper attacks," *Nature Electronics*, vol. 4, pp. 827–836, 2021, doi: 10.1038/s41928-021-00664-z.

[26] C. Su, J. Zhang, and Y. Ji, "Time-aware deterministic bandwidth allocation scheme in TDM-PON for time-sensitive industrial flowsitle," *Journal of Optical Communications and Networking*, vol. 15, no. 5, pp. 255–267, 2023, doi: 10.1364/JOCN. 481996.

[27] H. Uzawa et al., "Dynamic bandwidth allocation scheme for network-slicing-based TDM-PON toward the beyond-5G era," *Journal of Optical Communications and Networking*, vol. 12, no. 2, p. A135, Nov. 2019, doi: 10.1364/jocn.12.00a135

[28] M. Diaa, M. Shalaby, A. A. Mohamed, K. M. M. Hassan, and A. M. Mokhtar, "Undetectable tapping methods for gigabit passive optical network (GPON)," in *ICENCO 2018 - 14th International Computer Engineering Conference: Secure Smart Societies*, Institute of Electrical and Electronics Engineers Inc., Jul. 2018, pp. 52–57.doi: 10.1109/ICENCO.2018.8636110.

[29] V. Ivanova, T. Tashev, and I. Draganov, "DDoS Attacks Classification using SVM," *WSEAS Transactions on Information Science and Applications*, vol. 19, pp. 1–11, 2022, doi: 10.37394/23209.2022.19.1

[30] A. Bachar, N. El Makhfi, and O. EL Bannay, "Machine learning for network intrusion detection based on SVM binary classification model," *Advances in Science, Technology and Engineering Systems*, vol. 5, no. 4, pp. 638–644, 2020, doi: 10.25046/AJ050476.

[31] W. Man, G. Yang, and S. Feng, "Joint Selfattention-SVM DDoS Attack Detection and Defense Mechanism Based on Self-Attention Mechanism and SVM Classification for SDN Networks," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E107.A, no. 6, pp. 881–889, 2024, doi: 10.1587/transfun.2023EAP1057.

[32] T. Dewi et al., “Fuzzy logic-based control for robot-guided strawberry harvesting: visual servoing and image segmentation approach,” *SINERGI (Indonesia)*, vol. 28, no. 3, pp. 661–668, 2024, doi: 10.22441/sinergi.2024.3.021.

[33] A. Irwanto and L. Goeirmanto, “Sentiment Analysis from Twitter about Covid-19 Vaccination in Indonesia using Naïve Bayes and XGboost Classifier Algorithm,” *SINERGI (Indonesia),* vol. 27, no. 2, pp. 145–152, 2023, doi: 10.22441/sinergi. 2023.2.001.