ResearchGate

See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/335923774

Attack-Aware Dynamic Upstream Bandwidth Assignment Scheme for Passive Optical Network

Article *in* Journal of Optical Communications · September 2019

DOI: 10.1515/joc-2019-0142

CITATIONS
4

READS
495

5 authors, including:

Rizwan Aslam Butt
NED University of Engineering and Technology, Karachi
75 PUBLICATIONS **1,336** CITATIONS
SEE PROFILE

Waqar Ashraf Khan
Bahauddin Zakariya University
31 PUBLICATIONS **611** CITATIONS
SEE PROFILE

Basit Raza
COMSATS University Islamabad
80 PUBLICATIONS **2,252** CITATIONS
SEE PROFILE

All content following this page was uploaded by Waqar Ashraf Khan on 02 May 2020.

The user has requested enhancement of the downloaded file.

Rizwan Aslam Butt*, M. Faheem, M. Waqar Ashraf, Attaullah Khawaja and Basit Raza

Attack-Aware Dynamic Upstream Bandwidth Assignment Scheme for Passive Optical Network

https://doi.org/10.1515/joc-2019-0142
Received May 29, 2019; accepted September 03, 2019

Abstract: Network security is an important component of today's networks to combat the security attacks. The passive optical network (PON) works at the medium access layer (MAC). A distributed denial of service (DDOS) attack may be launched from the network and transport layers of an Optical Network unit (ONU). Although there are various security techniques to mitigate its impact, however, these techniques cannot mitigate the impact on the MAC Layer of the PON and can cause an ONU to continuously drain too much bandwidth. This will result in reduced bandwidth availability to other ONUs and, thus, causing an increase in US delays and delay variance. In this work we argue that the impact of a 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). The present DBA schemes do not have the capability to combat a security attack. Thus, this study, uses a machine learning approach to learn the ONU traffic demand patterns and presents a security aware DBA (SA-DBA) scheme that detects a rogue (attacker) ONU from its traffic demand pattern and limits its illegitimate bandwidth demand and only allows it the bandwidth assignment to it as per the agreed service level agreement (SLA). The simulation results show that the SA-DBA scheme results in up to 53%, 55% and 90% reduced US delays and up to 84%, 76% and 95% reduced US delay variance of T2, T3 and T4 traffic classes compared to existing insecure DBA schemes.

***Corresponding author: Rizwan Aslam Butt,** Electronic Engineering Department, NED University of Engineering and Technology, Karachi 75220, Pakistan, E-mail: rizwan.aslam@neduet.edu.pk
https://orcid.org/0000-0002-4784-0918
M. Faheem, Department of Computer Engineering, Abdullah Gul University, Kayseri, Turkey, E-mail: muhammad.faheem@agu.edu.tr
M. Waqar Ashraf, Department of Computer Engineering, Bahauddin Zakariya University, Multan, Pakistan,
E-mail: waqarkhan_118@yahoo.com
Attaullah Khawaja, Electronic Engineering Department,
NED University of Engineering and Technology, Karachi, Sindh, Pakistan, E-mail: atta@neduet.edu.pk
Basit Raza, COMSATS Institute of Information Technology, Park Raod, Islamabad, Islamabad 45550, Pakistan,
E-mail: basit.raza@comsats.edu.pk

Keywords: dynamic bandwidth assignment, bandwidth efficient, passive optical network, XGPON, PON, DBA

1 Introduction

With an exponential increase in ICT infrastructure, the cyberattacks have also been increasing continuously and are expected to increase further in future [1]. There are different kinds of cyberattacks in networks such as Masquerading, Replaying the packets, Modification of messages and Denial of service (DOS) attacks. Each type of attack has its own consequences and are detrimental for the network or network nodes. For example, masquerading may result in hacking of a personal login credentials or a website and the modification of messages may result in malfunctioning of a network device [1]. However, the DoS attack is even more dangerous and may result in crashing of a network node or may lead to a reduced availability of network resources. It has various forms with different impact on the network and a particular network node. For example, in a IP spoofing attack the attacker gets the knowledge of the source IP address of a network node and floods the network with useless packets and leads to increased congestion in the network and may even lead to complete denial of service to other legitimate nodes. Due to this excessive flooding the victim (destination) node may be inaccessible to other network nodes or some web page may not be available [2]. Another variation of such attack is DDOS attack in which multiple compromised nodes flood the resources of a particular host node and is also termed as a reflector attack [3].

The masquerading and modification of messages attacks may be avoided by using message encryption algorithms such as advanced encryption system (AES) and access control schemes such as secure hashing algorithm [4]. However, combating DOS attacks is not easy and straightforward. Several techniques have been presented in literature to combat these network attacks. For example, the IP spoofing DOS attack may be mitigated by marking the IP packets and tracing back their source at the edge routers [5, 6]. Another technique is to filter such spoofed packets in the edge routers on the basis of hop count or time to live [3].

Brought to you by | provisional account
Unauthenticated
Download Date | 1/12/20 7:04 PM

The PON is an optical fiber-based emerging access network topology that offers very high bandwidth. It works in a point – to – multipoint tree topology access to users, where the root of the tree is the OLT. The simple optical splitter (OS), connected to root via optical fiber, splits the optical signal from single fiber into many fiber points to connect to ONUs and vice versa [7]. Transmission of data could take place in both directions i. e. Upstream (US) – from ONUs to the OLT and Downstream (DS) – from OLT to ONUs. Generally, PONs utilize Time Division Multiple Access to allow US channel sharing between ONUs. Simply, all US traffic is partitioned into transmitting time slots and each ONU is allocated a specific amount of non-overlapping time slots either statically or dynamically by the OLT to ensure collision free transmissions. Use of a DBA mechanism for the US bandwidth management offers an efficient and as per need bandwidth utilization of the US link.

The PON network is considered very secure due to its passive nature and difficult for an attacker to get access to the optical signal. However, the recent study in [8] shows that now the attackers have devised several methods such as splitting attack and bending attack to get unauthorized access to a PON network. as it is not easy to tap in uses non – cooperative, confidential users with a broadcast DS channel which can be ultimately accessible to any malicious group willing to take advantage of changing the normal behavior of the ONU on the MAC layer. Then malicious ONUs may collect sensitive information intended for some other ONUs and may even result in traffic collision [9]. PON standards consequently enforce the use of cryptography to safeguard user information [10]. However, at the other side, US transmission channel is generally not susceptible to eavesdropping attacks owing to the characteristics of the OS, which allows US traffic accessible only to OLT and not to the ONUs. However, US channel is susceptible to attacks that control and manipulate the channel's shared nature.

Since PON is an access network technology and works at the MAC, a DOS attack at the Network and transport layer will also result in a massive increase in traffic frames in DS and US link of PON. Specially, the ONU under attack will have in increased bandwidth demand in the US shared link. Its excessive bandwidth demand will result in reduced share of bandwidth for the other normal ONUs. A normal DBA scheme used for US bandwidth management will not be able to handle this situation. This problem is studied in this work and a machine learning based detection mechanism for the ONUs under attack (Rogue ONUs) is presented. A secure DBA scheme is also presented to restrict the assignment to a rogue ONU, the ONU under DDOS attack.

Rest of the paper, Section 2 presents the literature review, Section 3 explains the DDOS attack scenario on in PON, Section 4 presents the security aware DBA (SA-DBA) scheme, the simulation setup and the results are discussed in Section 5. The study is concluded in Section 6 with a future outlook.

2 Related work

Four types of security attacks are possible in PON. The first is the eavesdropping, DOS attack, masquerading and service theft (ToS). The PON standards have an option of using encryption algorithm which can provide effective defense against eavesdropping and, thus, block the path toward a masquerading as well as the TOS attack [11]. The PON standard supports the AES encryption algorithm using a symmetric key mechanism [12]. However, the exchange of key is not encrypted which may be compromised. The study in [13] proposed an improved mechanism with secure key exchange using Diffie–Hellman key exchange protocol. Another work in [10, 14] stressed on the use of the quantum cryptography in PON networks with fiber Bragg grating implementation for a robust secure mechanism for PON networks. They presented a secure key establishment protocol with both way encryption and mutual authentication in GPON. The cryptographic specifications are transferred via PLOAM messages. In addition, this approach employs the characteristics of signal propagation that define the relation between OLT and ONU pairs. Although the DOS attack is possible from within the PON network itself [15, 16] in addition to a network layer attack. However, a DDOS attack is purely from the network and transport layer, therefore, the mitigation methods presented in literature such as packet marking [6], IP source tracing [5] and cloud based mechanism [17] also work at the network and transport layers.

A detailed description of these PON related security issues were initially investigated in [18] and then in a recent study [19] in a very comprehensive and detailed manner. Different types of security attacks on PON are explained in these studies such as simple eavesdropping monitoring, DoS, masquerading and service theft (ToS). Although there are specific DoS attacks on PON from the physical layer through a light signal injection from the remote node (Splitter/Combiner) which can only be mitigated through physical layer protection mechanisms [15, 16]. However, these are very targeted and specific attacks and their probability of occurrence is very low. In fact, the impact of a DDOS attack on a MAC layer of PON needs investigation and has not been earlier studied. Such an

Brought to you by | provisional account
Unauthenticated
Download Date | 1/12/20 7:04 PM

attack will result in a flooding of packets toward a particular ONU which will increase the DS and US bandwidth requirement of the ONU under attack.

In this work we study the impact of a DDOS attack on the US performance. Since, the US bandwidth is managed dynamically through a DBA scheme, therefore, a secure DBA scheme is presented in this work that mitigates the impact of a DDOS attack on PON without violating the SLA. Although the DBA schemes for PON [20–22] have been widely studied but they are not designed keeping in view the security requirements in PON. For the Rogue ONU detection, machine learning-based algorithm is used as machine learning has been shown to be very useful in data and traffic analysis of the optical access networks [23].

3 DDOS attack in PON

The DDOS attack is a very common type of network attack that is launched from the application layer from different sources toward a specific ONU, typically, on some UDP or TCP logical port. The attacker flood the network with too many packets, which may lead to very high network congestion and may even lead to complete service failure for that ONU.

The PON frame works at the MAC layer and thus any attack at the higher layer will be reflected in PON at the MAC layer. The attack will be from some user connected to an ONU that we term as rogue ONU throughout this paper. Assuming a Poisson traffic arrival rate the mean delay of an ONU can be given by eq. (1), where λ is the traffic arrival rate of the ONU, $\bar{X}^2$ is the second moment of the service time and the ρ is the service utilization ratio of the PON link and it depends upon the ONU service rate and is defined in eq. (2). Thus, the average US delay (D_{US}) and the DS delay can be expressed by eq. (3) and eq. (4). degrade the US bandwidth availability to other ONUs and may significantly degrade the US link performance. Figure 1 shows a DDOS attack scenario on an ONU. It can be seen that this attack scenario leads to an increased traffic λ of the ONU which will lead to reduced μ of the other ONUs due to heavy bandwidth utilization by the rogue ONU. Thus, the D_{US} and the D_{DS} will increase.

$$W = \frac{\lambda \bar{X}^2}{2(1-\rho)} \tag{1}$$

$$\rho = \frac{\lambda}{\mu} \tag{2}$$

$$D_{DS} = W_{DS} + \frac{RTT}{2} \tag{3}$$

$$D_{US} = W_{US} + \frac{RTT}{2} + \frac{SI}{2} \tag{4}$$

4 Security aware DBA

The SA-DBA scheme comprises of two stages; the Rogue ONU detection and the attack defense stages which are described in the following sub sections.

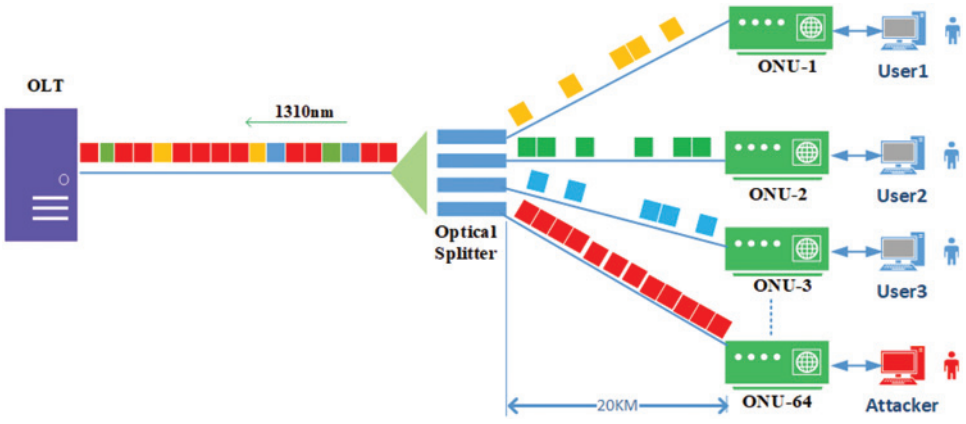

Figure 1: DOS Attack scenario in PON.

Brought to you by | provisional account
Unauthenticated
Download Date | 1/12/20 7:04 PM

4.1 Rogue ONU detection

Although each ONU user has a specific bandwidth utilization trend which requires deep and complicated learning model. However, differentiating between a normal ONU and an ONU suffering from a DOS attack can be achieved with a simple regression model-based learning. For this purpose the SA-DBA scheme accumulates the buffer occupancy reports of the T2, T3 and T4 traffic classes of each ONU in a vector variable $Load(i)$ during a service interval (SI). At the end of SI, the regression model comprising of eq. (5) to eq. (7) is used to compute the predicted values of the ONU bandwidth demand ($D_p(i)$) for all ONU "N". Where m_{ONU} is the slope of regression line and C_{ONU} is the y-axis intercept for the regression line. Then the is used to look for the presence of Rogue ONUs. The algorithm first computes the predicted load values using the regression model and then computes the error vector $Err[i]$ by taking the difference of the $D_p(i)$ and the $Load(i)$. The regression model is based on the eq. (5) and eq. (6) which are used to compute the m_{ONU} and C_{ONU} from the recorded traffic load (i) of each ONU during a SI. Figures 2 and 3 show the recorded average ONU bandwidth demand trend of the ONUs from simulation and the corresponding trend line predicted by the regression model using , during a SI for low and high traffic load conditions. It is evident from these results that the ONUs suffering from DOS attack, ONU numbers 3 and 12, have very high bandwidth demand compared to all other ONUs which causes their error values to be always positive and very high in the range of 50 % to 90 %. Therefore, we set the threshold for a rogue ONU detection to 50 % in Algorithm 1.

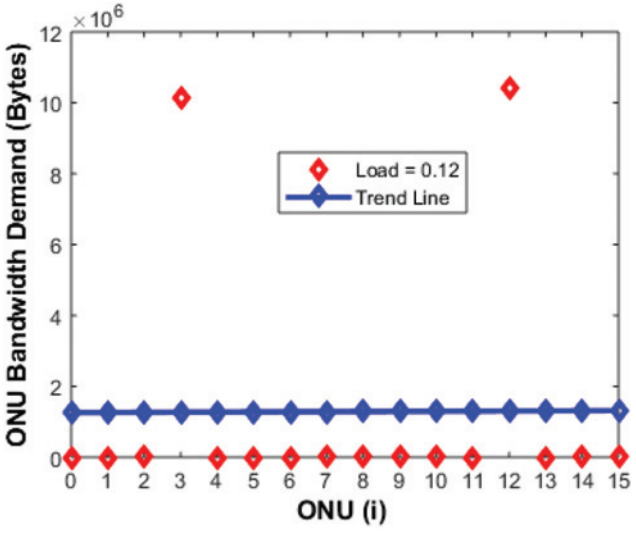

Figure 2: ONU Bandwidth demand in an SI at a Traffic Load of 0.12.

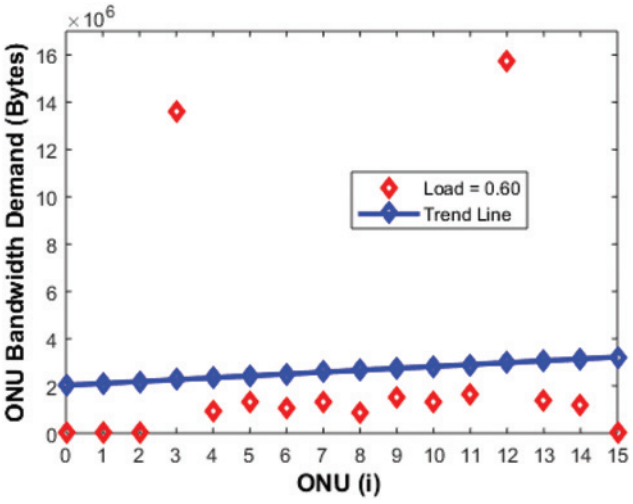

Figure 3: ONU Bandwidth demand in an SI at a Traffic Load of 0.60.

Algorithm 1: Rogue ONU detection.

Input: $ONU(i)$, $Load[i]$
Output: *RogueONU* List

1 ***If*** $(Flag_{SW} = 1)$
3 ***For*** $(i = 0\ to\ N)$
4 $MeanX+ = ONU[i]$
5 ***End For***
6 $MeanX = \frac{MeanX}{N}$
7 ***End If***
8 ***For*** $(i = 0\ to\ N)$
9 $MeanY + = Load[i]$
10 ***End For***
11 $MeanY = \frac{MeanY}{N}$
12 ***For*** $(i = 0\ to\ N)$
13 $VarX = ONU(i) - MeanX$
14 $VarY = ONU(i) - MeanY$
15 $SqVarX[i] = (x[i] - meanX)^2$
16 $Num+ = varX[i] * varY[i]$
17 $Dnum+ = SqVarX[i]$
18 ***End For***
19 $m_{ONU} = Num/Dnum$
20 $C_{ONU} = MeanY - m_{ONU} * MeanX$
21 ***For*** $(i = 0\ to\ N)$
22 $\text{Load}_p[i] = (m_{ONU} * (i + 1) + C_{ONU})$
23 $\text{Err}[i] = (y[i] - \text{yPredicted}[i])/y[i] * 100$
24 ***End For***
25 ***If*** $(\text{Err}[i] > 50)$
26 ***Push*** $ONU(i) \rightarrow RogueONU$
27 ***End If***

$$m_\lambda = \frac{\sum_{i=1}^{M}\left(\left(D_p - \frac{\sum_i^N Load(i)}{N}\right) * \left(ONU(i) - \frac{\sum_{i=1}^{N} ONU(i)}{N}\right)\right)}{\sum_{i=1}^{M}\left(ONU(i) - \frac{\sum_i^M ONU(i)}{N}\right)^2} \quad (5)$$

Brought to you by | provisional account
Unauthenticated
Download Date | 1/12/20 7:04 PM

$$C_\lambda = \left(L(i) - \frac{\sum_i^N Load(i)}{N} \right) - m_\lambda \star \left(ONU(i) - \frac{\sum_{i=1}^M \lambda(i)}{N} \right) \quad (6)$$

$$D_p(i) = m_{ONU} \star \lambda(i) + C_{ONU} \quad (7)$$

4.2 Security aware DBA algorithm

The main challenge in DBA assignment in this study was how to defend the DDOS attack by the Rogue ONU after it has been detected. We cannot simply stop assigning bandwidth to such an ONU as the user of that ONU has signed an SLA with the service provider which needs to be abided. Therefore, we limit the bandwidth assignment to such an ONU to the average bandwidth demand of all the other ONUs having the same SLA in both the guaranteed phase allocation (GPA) to T2 and T3 and in surplus allocation phase (SPA) to T3 and T4. For this purpose we modified the EBU scheme [24, 25] as it an improved form of earlier presented IACG [26] and GIANT [27] DBA schemes. The bandwidth assignment process uses Algorithm 2 to look first for an ONU to be a Rogue ONU or a normal ONU by checking the *RogueONUs* list. If the ONU is found to be in the list then it is only assigned the bandwidth as per the average bandwidth demand $AvgT_p$ for its traffic class T_p that is computed from queue reports received in the last SI. The queue report Report_p is set to zero to stop any further assignment to T_p during the current SI. If ONU is not found in the list then the normal bandwidth assignment process is followed. Since, the EBU scheme also divides the excess bandwidth uniformly to all the ONUs. In SA-DBA scheme, the modified algorithm (Algorithm 3) is used to distribute the surplus bandwidth in the excess bandwidth assignment phase. This algorithm do not assign surplus bandwidth grant (*Suplus_Grant*) to a **RogueONU**. Where Frame_Bytes is the total US bytes for XGPON and RAW is the remaining unassigned bandwidth left after the GPA and SPA phases. The restriction of bandwidth for the **RogueONUs** leads to higher bandwidth assignment to the other ONUs.

Algorithm 2: DBA assignment algorithm for T2, T3 and T4 TCONTs.

Input: Report_p, $AvgT_p$, $VB_p[k]$, *Frame_Bytes*
Output: *Bandwidth Grant for TCONTs*

$N = 16$, $Start = 0$, $End = 16$, $p = 2, 3, 4$

```
1   For(i = Start to End)
3   k = (i % N)
4   If(Fram_Bytes > 0)
5   {
6   If(VB_p[k] > 0)
7   ONUno = Find(RogueONUs.begin(), RogueONUs.end(), k);
8   if(ONUno! = RogueONUs.end())
9   Grant = Min(VB_p[k], AvgT_p, Frame_Bytes);
10  Report_p = 0;
11  Else
12  Grant = Min(VB_p[k], Report_p, Fram_Bytes);
13  Report_p = Report_p – Grant
14  End If
15  Frame_Bytes = Frame_Bytes – Grant
16  End If
17  End If
18  Start + + ;
19  End + + ;
20  End For
```

Algorithm 3: Surplus bandwidth assignment algorithm for T2, T3 and T4 TCONTs.

Input: *Frame_Bytes*,*RogueONUs List*
Output: *Surplus Bandwidth Grant for TCONTs*

```
1   If(Frame_Bytes > 0
3   RAW = Frame_Bytes;
4   RogueSize = RogueONUs.size();
5   Extra_Bytes = RAW /(N-RogueSize);
6   For(i = 0 to N)
8   ONUno = Find(RogueONUs.begin(), RogueONUs.end(), k);
9   If(ONUno! = RogueONUs.end())
10  Suplus_Grant = Extra_Bytes
11  Else
12  Suplus_Grant = 0
17  End If
18  End For
19  End If
```

5 Simulation setup

A PON network with comprising of 16 ONUs was designed using OMNET++ simulation environment. The main simulations parameters are shown in Table 1. The network performance is studied with a Poisson distribution based traffic generator. The traffic is generated by computing the inter-arrival time (I.I.T) using an exponential function according to the desired traffic load. The traffic generator computes the traffic arrival rate R per ONU using eq. (8), where the *Link_Capacity* is 38,880 bytes for US link of the XGPON. Then the I.I.T is computed by

Brought to you by | provisional account
Unauthenticated
Download Date | 1/12/20 7:04 PM

Table 1: Simulations parameters.

Parameter	Values/Details
US/DS Line rates	10 Gbps/2.5 Gbps
US/DSTrafficLoad	Varied from 0.1 to 1
ONU to OLT Line rate	200 Mbps
Average traffic frame size F_{avg}	Follows the Broadcom CATV distribution as in [28, 29]
Bandwidth Assignment for T2	AB_{min} = 7812 bytes with SI_{max} = 5 (100 Mbps)
Bandwidth Assignment for T3	AB_{min} = AB_{sur} = 7812 with SI_{max} = SI_{min} = 10 (50 Mbps Assured and Non-assured portions).
Bandwidth Assignment for T4	AB_{sur} = 15,624 and SI_{max} = 10. (100 Mbps)

eq. (9). The F_{avg} is the average packet size of the generated traffic frames and the 'N' is the total number of active ONUs. The *Traffic_Load* is the ratio of total traffic bytes sent by all the ONUs and the *Link_Rate*. The DDOS attack is modeled on two ONUs by increasing their traffic load five times of their actual load value.

$$R = \frac{Traffic\_Load^{*}Link\_Capacity}{N^{*}F_{avg}} \tag{8}$$

$$I.I.T = Exponential\left(\frac{1}{\lambda}\right) \tag{9}$$

6 Results and discussion

The performance of SA-DBA scheme is compared with normal DBA which cannot detect a rogue and assigns bandwidth equally to all ONUs. We choose EBU DBA scheme for comparison as it is an improved version of earlier IACG [26] and GIANT [27] DBA schemes and its unused bandwidth assignment algorithm was further improved in our earlier work in [30]. The US link performance results including average US delays of T2, T3 and T4 traffic classes and the delay variance results are shown in Figures 4 to 6. All the results are recorded for the normal ONUs and not for the Rogue ONUs to only study the impact of the DDOS attack on other ONUs and the improvement contributed by the SA-DBA scheme.

From the delay results it is evident that the EBU DBA cannot differentiate between a normal ONU and a Rogue ONU and, thus, cannot combat with the DDOS attack on an ONU which leads to very high bandwidth utilization by the rogue ONUs. This results in reduced bandwidth availability for the other ONUs. Thus the US link performance is severely degraded, resulting in higher delays of all T2, T3 and T4 traffic of all the other ONUs. The impact of the DDOS attack increases at lower traffic loads due to very high utilization of the excess bandwidth by the rogue ONUs, leaving only little excess bandwidth for the normal ONUs. On the other hand the SA-DBA limits the guaranteed and surplus bandwidth assignment to the rogue ONUs to the average bandwidth demand of the other ONUs with the same SLA which results in higher bandwidth availability

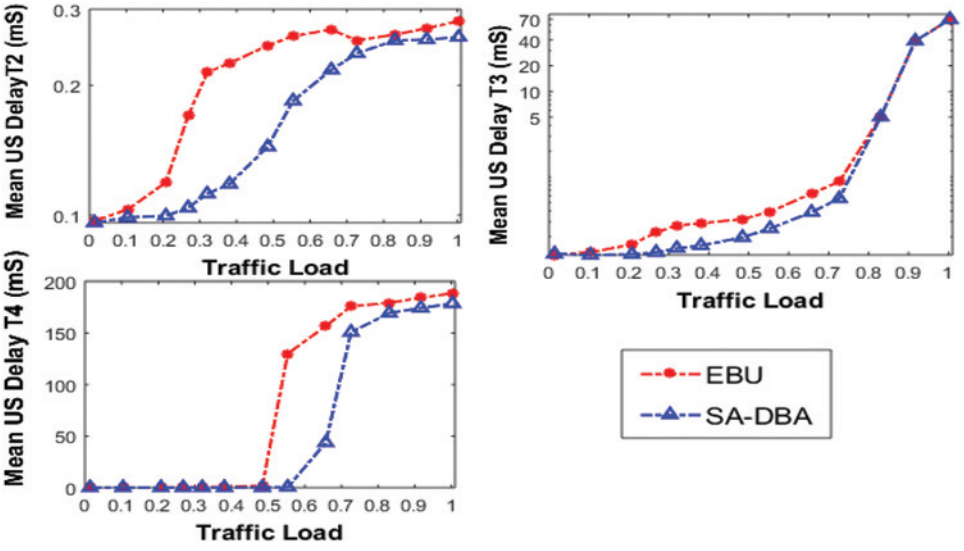

Figure 4: US Delays of T2, T3 and T4 traffic excluding Rogue ONUs.

Brought to you by | provisional account
Unauthenticated
Download Date | 1/12/20 7:04 PM

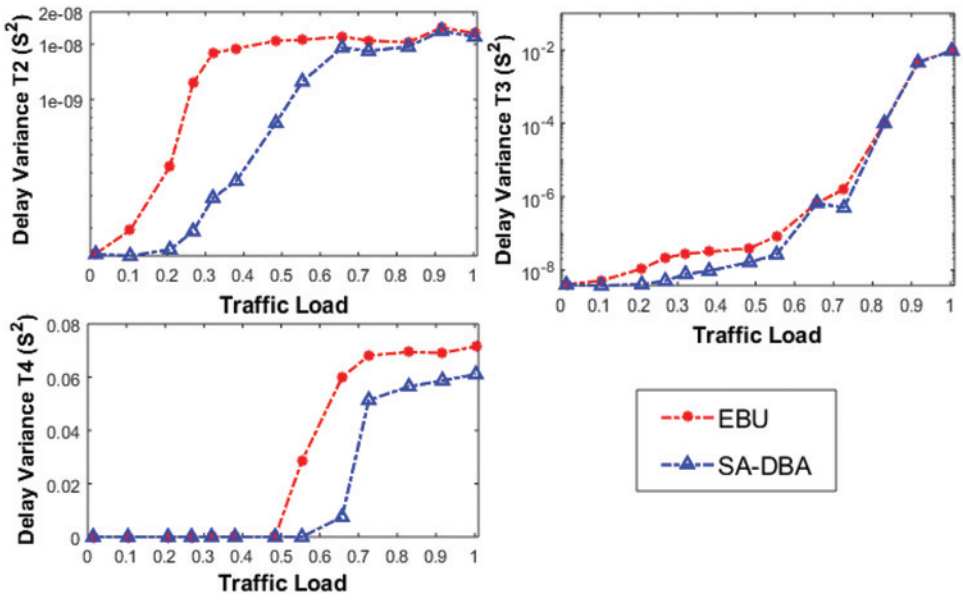

Figure 5: US Delay Variance of T2, T3 and T4 traffic excluding Rogue ONUs.

to other ONUs compared to EBU scheme. Moreover, the SA-DBA scheme completely stops the excess bandwidth assignment to the rogue ONUs which further boosts the US performance of all the T2, T3 and T4 traffic of the other ONUs not under attack. Thus, it completely fails the DDOS attack and avoids the performance degradation of US link. Thus, the US delays of T2, T3 and T4 in case of SA-DBA are up to 53 %, 55 % and 90 % times lower compared to EBU scheme. The SA-DBA scheme also reduces the delay variance of T2, T3 and T4 traffic classes by 84 %, 76 %, 95 % respectively. The T4 class is most severely hit by the DDOS attack because it works on best effort basis and works only on the unused bandwidth of other traffic classes. The DDOS attack results in exponential increase of bandwidth demand by the rogue ONUs which leads to shortage of unused bandwidth and, thus, the performance of T2 traffic is severely degraded in case of EBU scheme. At traffic loads higher than 0.7, the surplus bandwidth is not available, thus, the performance of both DBA schemes become quite close.

The SA-DBA scheme also reduces the frame loss rate of the normal ONUs compared to EBU scheme due to higher bandwidth availability as evident from Figure 6(b). Since the DDOS attack made by the ONU is on US link only, thus, the performance of DS link remains unaffected and as evident from Figure 6(a).

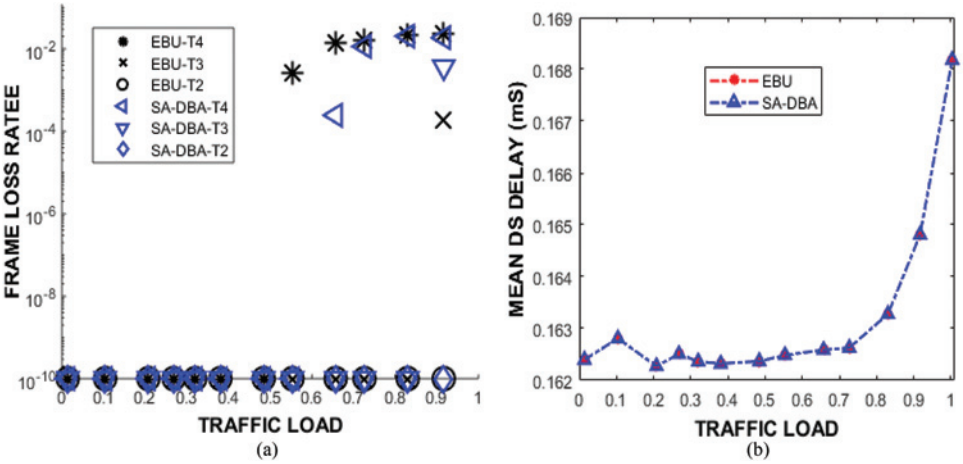

Figure 6: (a) Frame Loss Rate (b) Average DS Delay.

Brought to you by | provisional account
Unauthenticated
Download Date | 1/12/20 7:04 PM

Overall, SA-DBA scheme proves to be a secure DBA for PON by successfully defending the DDOS attack on any ONU by limiting the bandwidth demand of that ONU so that the bandwidth assignment to other ONUs is not disturbed. A normal bandwidth assignment to the Rogue ONUs also ensures compliance to the SLA and also limits the traffic load of the Rogue ONU.

7 Conclusion

In this study, a novel DDOS attack resilient DBA scheme is presented. The presented scheme can detect rogue ONUs in the DBA process by learning the traffic demand pattern of all the ONUs using a machine learning algorithm, similar to the earlier work in [31]. The presented scheme combats the attack by limiting the bandwidth assignment to such ONUs to the average bandwidth demand of other ONUs with the same SLA. Thus it counters the DDoS attack without violating the SLA signed with the user. The proposed scheme is evaluated through an OMNET++ based simulation testbed for PON. The simulation results verify our claim and show the success of the presented DBA scheme.

Acknowledgements: The authors acknowledge the financial support for this work provided by Higher Education Commission (HEC) Pakistan through SRGP Research grant number 1981.

References

1. Wang Q, Dunlap T, Cho Y, Qu G. DoS attacks and countermeasures on network devices. In: 2017 26th Wireless and Optical Communication Conference, WOCC 2017, 2017:1–6.
2. Maraj A, Jakupi G, Rogova E, Grajqevci X. Testing of network security systems through DoS attacks. In: 2017 6th Mediterranean Conference on Embedded Computing. MECO 2017 – Including. ECYPS 2017, Proceedings, 2017:1–6.
3. Sieklik B, MacFarlane R, Buchanan WJ. Evaluation of TFTP DDoS amplification attack. Comput Secur. 2016;57:67–92.
4. Stallings W, Brown L, Bauer MD, Bhattacharjee A. Computer security: principles and practice, 3rd ed. New York, USA: Pearson Education, 2012.
5. Singh K, Singh P, Kumar K. A systematic review of IP traceback schemes for denial of service attacks. Comput Secur. 2016;56:111–39.
6. Patel H, Jinwala DC. LPM: A lightweight authenticated packet marking approach for IP traceback. Comput Netw. 2018;140:41–50.
7. Nesset D. PON Roadmap [Invited]. J Opt Commun Netw. 2017;9:A71–A76.
8. Diaa M, Shalaby M, Mohamed AA, Hassan KM, Mokhtar AM. Undetectable tapping methods for gigabit passive optical network (GPON). In: 2018 14th International Computer Engineering Conference (ICENCO), 2019:52–7.
9. Drakulic S, Tornatore M, Verticale G. Degradation attacks on passive optical networks. In: 2012 16th International Conference on Optical Networking Design and Modelling, ONDM 2012, 2012:1–6.
10. Martinez-Mateo J, Ciurana A, Martin V. Quantum key distribution based on selective post-processing in passive optical networks. IEEE Photonics Technol Lett. 2014;26:881–4.
11. Horvath T, Malina L, Munster P. On security in gigabit passive optical networks. In: 2015 International Workshop on Fiber Optics in Access Network, FOAN 2015, 2015:51–5.
12. 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.
13. Malina L, Horvath T, Munster P, Hajny J. Security solution with signal propagation measurement for gigabit passive optical networks. Opt (Stuttg). 2016;127:6715–25.
14. Fröhlich B, Dynes JF, Lucamarini M, Sharpe AW, Tam SW, Yuan Z, et al. Quantum secured gigabit passive optical networks. In Optical Fiber Communication Conference, Optical Society of America, March 2015: W4F-1.
15. Yeh CH, Chow CW, Wu YF, Shih FY, Chi S. Experimental demonstration of CW light injection effect in upstream traffic TDM-PON. Opt Fiber Technol. 2010;16:178–81.
16. Lyu W, Qiu Y, Han J, Deng N, Xu J. Optik on the security weaknesses of a power splitting-based passive optical network. Opt Int J Light Electron Opt. 2018;174:623–9.
17. Fujinoki H. Cloud-base defense against DRDoS attacks. 2018 IEEE International Conference on Consumer Electronics, 2018:1–2.
18. Ajduczenia M, Freire PR, Monteiro PP. On EPON security issues marek. IEEE Commun Surv Tutorials. 2007;9:68–83.
19. Atan1 SM, MZin3 A, Ismail NA, Zulkifli N. An overview on security issues in the optical access network. In: IEEE 7th International Conference on Photonics (ICP), 2018:1–3.
20. Ashraf MW, Idrus SM, Butt RA, Iqbal F. Post-disaster least loaded lightpath routing in elastic optical networks. Int J Commun Syst. 2019;32:1–19.
21. Butt RA, Waqar Ashraf M, Faheem M, Idrus SM, A survey of dynamic bandwidth assignment schemes for TDM-based passive optical network, 2018.
22. Neaime J, Dhaini AR. Dynamic wavelength and bandwidth allocation in tactile-capable optical cloud distribution networks. In: IEEE International Conference on Communications. vol. 2018. 2018:1–6.
23. Musumeci F, Rottondi C, Nag A, Macaluso I, Zibar D, Ruffini M, et al. An overview on application of machine learning techniques in optical networks. IEEE Communications Surveys & Tutorials 2018;21:1383–1408.
24. Han MS, Yoo H, Lee DS. Development of efficient dynamic bandwidth allocation algorithm for XGPON. Etri J. 2013;35:18–26.
25. Han M-S. Iterative dynamic bandwidth allocation for XGPON. In: 14th International Conference on Advanced Communication Technology (ICACT), 2012:1035–40.
26. Han M-S, Yoo H, Yoon B-Y, Kim B, Koh J-S. Efficient dynamic bandwidth allocation for FSAN-compliant GPON. J Opt Netw. 2008;7:783–95.

Brought to you by | provisional account
Unauthenticated
Download Date | 1/12/20 7:04 PM

27. Leligou HC, Linardakis C, Kanonakis K, Angelopoulos JD, Orphanoudakis T. Efficient medium arbitration of FSAN-compliant GPONs. Int J Commun Syst. 2006;19:603–17.
28. Kramer G, Mukherjee B, Maislos A. Ethernet passive optical network (EPON), 1st ed. New York, USA: McGraw-Hill Education, 2005.
29. Butt RA, Ashraf MW, Anwar MY, Anwar M. Receiver ON Time optimization for watchful sleep mode to enhance energy savings of 10-gigabit passive optical network. Tech J Univ Eng Technol Taxila. 2018;23:72–80.
30. Butt RA, Idrus SM, Rehman S-U, Shah PM, Zulkifli N. Comprehensive polling and scheduling mechanism for long reach gigabit passive optical network. J Opt Commun. 2019;40:1–12.
31. Butt RA, Faheem M, Arfeen A, Ashraf MW, Jawed M. Machine learning based dynamic load balancing DWBA scheme for TWDM PON. Opt Fiber Technol. 2019;52:101964.

Brought to you by | provisional account
Unauthenticated
Download Date | 1/12/20 7:04 PM

View publication stats