Understanding Degradation Attack and TCP Performance in Next Generation Passive Optical Network

F.M. Atan¹²*, N. Zulkifi¹, S.M. Idrus¹, N.A. Ismail¹², A.M. Zin¹²

¹Lightwave Communication Research Group, Universiti Teknologi Malaysia (UTM).
²Fakulti Kejuruteraan Elektrik, Universiti Teknologi MARA (UiTM) Cawangan Johor

Email: fadila2533@uitm.edu.my

Abstract. The next-generation gigabit passive optical network (NG-PON) is a promising solution for network growth and expansion. The NG-PON aims to connect more users as fiber's deployment to the home (FTTH) initiative takes place. The network needs urgent attention to its security establishment, which is currently exposed to a degradation attack. During the attack, already available TCP congestion control is invoked to handle collision. The interconnection of TCP in the transport layer and attack in the MAC layer is investigated. During the attack, a reduction of 63% of total throughput is detected. A variation of the number of ONU also determines the competing nature of TCP, which inherently reduces the maximum throughput of 4%.

1. Introduction

The Passive Optical Network (PON) is the solution for network expansion due to its ability to provide higher transmission speed, a lower overall cost per customer, and guaranteed quality of service (QoS). In a typical time-division multiplex (TDM) PON, traffic from Optical Network Unit (ONU)s and Optical Line Terminal (OLT) is connected through a single optical fiber branched passively through an optical power splitter [1]. Even though only a single fiber is used, communication links between OLT and ONUs used different wavelengths of 1310 nm and 1490 nm, respectively [2]. The downstream traffic works in a broadcast manner and will comply with the Subscriber Line Agreement (SLA). Since PON is a non-cooperative, private network with a passive splitter, any malicious modification made in a MAC layer can results in data availability for every ONU since the traffic flows to all users at the same time. Therefore, to protect the communication link's privacy, PON required a mandatory encryption method on the downstream channel.

However, due to the high directivity of the upstream link, the upstream channel is said to be impenetrable to attack, hence having a more relaxed security system. These flaws lead to the call for stronger security measures in future PON [3-4]. The TDM PON divided all its upstream traffic in a timeslot. During initialization, all ONU is registered and given a timeslot either statically or dynamically. At each transmission time, only single traffic from a specific timeslot is allowed a turn to send. In a normal situation, the dedicated timeslot will ensure all traffic is able to be sent fairly and without loss. An attack in the upstream channel would interrupt the pre-assigned timeslot allocation and caused a collision between the traffic. The throughput of the attacked ONUs will be reduced since the Transmission Control Protocol (TCP) react to those collisions. The attack would further reduce the QoS for the network by having a high frame error loss (FER) rate and slower transmission speed.

The above mention attack is known as a degradation attack [5]. A degradation attack is a security breach that harmed the throughput fairness mechanism among ONUs. The attacker basically exploits two XGPON features by sending upstream signals out of its given slots and caused other ONUs to
experience packet loss. The ONU sends their upstream traffic via allocated timeslot while the malicious ONU obtained legitimate timeslot and sends additional unlawful traffic mixed with other packets.

![Figure 1. Degradation attack](image)

TCP is one of the oldest protocols on the internet that enable users to have congestion-free and reliable communication links [6]. TCP's challenge is to manage a reasonable sending rate using a congestion control mechanism, so the throughput performance between the sender and receiver can be justified at any time during the data transmission. However, as one of the oldest protocols on the internet, the TCP is closed-loop in nature. It sometimes creates synchronizing issues with other networking technologies. The TCP collects information on the acknowledgment feedback to determine data transfer speed in the transport layer. In contrast, XGPON itself determines the bandwidth and data transfer in the MAC layer during its bandwidth allocation scheme [7]. The problems mentioned as asymmetric technologies and high-speed large bandwidth network as XGPON would result in severe QoS reduction.

This paper presented a degradation attack scenario in XG-PON and TCP throughput behavior while the network is under attack. The next section of the paper will discuss the TCP throughput and delay balance. Lastly, the results of TCP throughput variation during the attack are discussed.

2. Literature Review

As more end users are supported over a shared physical medium in optical networks, access network security should be a greater importance as a single attack can affect a great number of users that may involve nearly hundreds of Gbps transmission [3]. GPON does offer security features such as data encryption, authentication, and key establishment. However, since GPON has strong reliance on the assumption that all the GPON elements will be physically protected, its security mechanism is largely relaxed [8]. Both authentications of ONUs and encryption of downstream traffic are optional while upstream traffic is not encrypted assuming high directionality of PON where other ONUs cannot sniff traffic sent by an ONU to OLT.

Research in [5] explains this attack well, although it is simulated in an Ethernet PON (EPON) environment with static bandwidth allocation. The degradation attack manipulates the TCP congestion algorithm embedded in the network transport layer. Another researcher also ventures on the issue of TCP performance in XG-PON, such as [7]. The author in [7] explains the issues of asymmetric and its effect on bandwidth assignment schemes. The study made it clear about TDMA operation and fragmentation on quality metrics like transfer times. However, the study is done in a single traffic type and simplified GPON environment.

The researcher in [9] discusses the effect of TCP on the fairness of interlayer network connection. The research portrayed competing for multiple TCP flows and how TCP controls the bandwidth allocation in the EPON. Due to the MAC layer's shared nature, the conventional bandwidth allocation scheme cannot fairly share the bandwidth during bottleneck situations. However, the system is done in EPON, which inherently different from XGPON architecture. A more recent paper is published by [10] examines the possible outcome of malicious ONU disrespect of the network's assigned timeslot.
However, a disruptive attack can be detected by the physical alarm but cannot be located by the system. The writer suggests a modified end unit of ONU to combat the attack. The modification of physical equipment is not our focus in securing the network as it will increase the cost per user and equipment complexity.

Henceforth, by referring to other published research, a degradation attack is a real threat to the XGPON MAC layer. The attack manipulates the upper layer's behavior that causes a reduced both speed and overall throughput of attacked ONU while at the same time due to dynamic bandwidth allocation in XGPON favors malicious ONU. In this work, we present the effect of degradation attack on the network and the conduct of TCP, contributing to the reduction of throughput. We also discussed the throughput delay tradeoff while examining the effect of multiple TCP flows inside the network.

3. Methodology

A degradation attack destroys the sequence of upstream traffic transmission by manipulating the principle of TCP. Although TCP is the traditional upper-layer protocol that operates on XGPON in the MAC layer, the compromise between TCP throughput and delay is undeniable. Hence it is another discussion we wish to present.

3.1. Attack Formulation

In normal conditions, the scheduled timeslot is obeyed by all ONU. Nonetheless, when a degradation attack is launched, the schedule is no longer followed. Since the XGPON is a passive network, there is no monitoring of whether all party involved is abode by the schedule. The nature of private in XGPON also means the lawful ONU did not aware of the attack. The attack also did not intend to attack a specific user per se but degrade the entire network's QoS. The simulation is written with Python software, and for attack simulation, a random disturbing signal switch is placed inside all ONU. Thus, ONU could be made to be malicious or lawful at a given time. Hence the attack is at a random time and with a random ONU. However, at any given time, only a single attack would occur throughout a simulation time. The attack launched caused the error rate of the lawful ONUs to be increased. Therefore, the attacker is identified as the ONU with the lowest error rate in the network. The table below explains the parameter used in the simulation.

| Table 1. Simulation Parameter |
|------------------------------|
| Parameter                   | Values          |
| Traffic arrival             | Pareto distribution |
| TCP flavour                 | New Reno        |
| Guard band period for uplink connection | 26ns        |
| Sliding windows size        | 7054 bytes      |
| RTT                         | 230msec         |

3.2. TCP behavior under Attack

TCP working principle to ensure reliable communication link is a 3-way handshake. Hence every time a packet arrived, the handshake procedure will send an acknowledgment (ACK) ACK message to the sender notifying the sender that the packet is received, and the next packet can be transferred now. During the normal condition, packet transfer between sender and receiver is numbered in sequence. Retransmission occurs when the packet number sequence received is out of order. A timeout is issued when the ACK message is not received at all after stipulated duration or in the event of duplicated ACKs.

As the timeslot is violated during the attack, the malicious ONU transmits disturbing signals into another lawful ONUs legitimate timeslot. Since the splitter in the XG-PON is passive, the two signals will be mixed and transferred to OLT. At OLT, it is found that the packet mixed signals are considered incorrect and erroneous, yet OLT is unable to distinguish the real signal from its disturb signal. This packet is known as an error packet, and there is no ACK message produce as the result of the error. The TCP congestion control applied the scheme of TCP timeout and consider this as congestion in the
network. To secure the link again, TCP needs to clear the congestion. An algorithm of a slow start and congestion avoidance will be invoked. This will clear the congestion but at the same time speed of packet transfer is compromised, and as a result client, i.e., lawful ONUs will experience a decrease in throughput. The TCP throughput is calculated as function of several variables such as RTT, Maximum Segment Size (MSS) and loss probability. The original mathematical model given by [11]. Taking consideration of area under saw-tooth graph.

\[
\text{TCP Throughput} = \frac{\text{Window size}}{\text{RTT}} = \frac{\text{MSS} \times \frac{2W^2}{\text{RTT} \times W}}{2}
\]

\[\text{C} = \frac{3}{2}\]  \hspace{1cm} (3)

Collecting the constant term as (3), the equation finalized as:

\[
\text{TCP Throughput} = \frac{\text{MSS} \times \text{C}}{\text{RTT} \times \sqrt{\rho}}
\]

Where window size is the amount of biggest unfragmented data received in bytes and \(\rho\) is the packet loss probability. From (4), it is apparent that packet loss probability interferes with the throughput as it is inversely proportional to overall throughput.

### 3.3. Throughput delay tradeoff

The XG-PON experiences this tradeoff in the waiting time in the scheduling queue and during the upstream delay. During the experiment, if a single ONU is attached to OLT, using a large MSS to be served by DBA, the throughput of the receiver is high since the large MSS means fewer packets can be put inside a single upstream frame. A low-size MSS would require many more packets (hence increasing burst overhead per packet) to fit inside a single upstream frame. However, if multiple ONUs is connected to the OLT with the same DBA scheme scheduling algorithm, having a larger MSS is actually reducing the throughput of the receiver. A higher MSS value between multiple ONUs means a longer scheduling delay between upstream transmission. This is due to the standard upstream cycle duration of 125 µs, which might segmentize big-sized data into multiple packets. The packet is then sent into two consecutive upstream transmissions instead of single transmission, consequently reaching the throughput delay tradeoff. An increased sliding window size with timestamp evaluation is used to counter this issue (TCP extension of RFC 1323). When the size of the sliding window is increased, the amount of data being able to be packed inside a single packet is increased hence increased throughput. However, this is a TCP size rescaling features that are not available widely, and manual reconfiguration is needed.

### 4. Results and Discussion

The throughput of malicious ONU, in this case, is determined by the minimum value of the congestion window and advertised window. The maximum throughput that any ONU can achieve is 250Mbps. The number of total TCP to be sent is 1024 bytes. During the initial attack, as in Figure 3, malicious ONU (ONU 4) is getting all the bandwidth as it attacks the network, while lawful ONUs suffers. For all ONU, the maximum throughput allowable is 250Mbps. However, based on the result shown, only malicious ONU is able to maintain maximum throughput during the attack. This is due to the non-violation of its timeslot. Other ONUs are experiencing timeslot violation; hence error probability is increased, which results in the reduced throughput due to the TCP congestion control algorithm. Throughput calculation is given by:
The total throughput reduction on the attacked ONU is as high as 66\% during the attack. However, the malicious ONU throughput is maintained without reduction as its timeslots were never violated. The bandwidth assignment would favor the malicious ONU since the link is deemed reliable. Figure 4 showed the behavior of TCP when the number of ONU is varied. As the ONU number increased, TCP flow competes to be served by the upstream channel is also increased. However, handling multiple TCP requests with large MSS has proven to increase the network scheduling algorithm's delay. A packet is made to stay in the scheduling queue for a bit longer if competing TCP flow increases. Hence the more ONU in the network, the maximum throughput is reduced by about 4\%. The network is set to have 100\% capacity at the time of the experiment. The hypothesis is as the number of user increase, the degradation attack launched at the network would impact the TCP behavior and the way the MAC layer granting the timeslot request. The amount of maximum throughput reduction might be small now, but the later revised XGPON aims to serve up to 256 users per single connection to OLT.

\[
\text{throughput}_{\text{max}} = \frac{\text{total bytes sent}}{\text{RTT}} = \frac{1024 \times 7 \times 8}{230 \times 10^{-3}} = 250 \times 10^3 \text{bps}
\]

Figure 2. TCP Throughput vs Time

5. Conclusion

The paper discussed the degradation attack in the XG-PON. During the attack, the already available TCP congestion control algorithm reacts to the attack hence slowing the network in an effort to solve the congestion. The competing TCP flows are also an issue that increases the delay in the connection. A more thorough analysis is needed to create an algorithm to stop and defend the network against the degradation attack since its severity only increases with the additional user.
Acknowledgement

The authors acknowledge the Ministry of Higher Education Malaysia (MOHE) and the research management center of Universiti Teknologi Malaysia (UTM) for the project financial support through Fundamental Research Grant Scheme with reference no. FRGS/1/2018/ICT03/UTM/02/8 (UTM vote no. 5F086) and Transdisciplinary Research Grant (TDR) program with vote no. 05G60.

References

[1] FSAN, “10-Gigabit-capable passive optical networks(XG-PON): Transmission convergence (TC) layer specification,” ITU-T G.987.3 Recomm., 2010.

[2] E. Wong, “Next-generation broadband access networks and technologies,” J. Light. Technol., vol. 30, no. 4, pp. 597–608, 2012, doi: 10.1109/JLT.2011.2177960.

[3] L. Malina, J. Hajny, R. Fujdiak, and J. Hosek, “On perspective of security and privacy-preserving solutions in the internet of things,” Comput. Networks, vol. 102, pp. 83–95, Jun. 2016, doi: 10.1016/J.COMNET.2016.03.011.

[4] F. M. Atan, A. Zin, N. A. Ismail, N. Zulkifli, and S. M. Idrus, “An Overview on Security Issues in The Optical Access Network,” in 2018 IEEE 7th International Conference on Photonics (ICP), 2018, pp. 1–3, doi: 10.1109/ICP.2018.8533171.

[5] S. Drakulic, M. Tornatore, and G. Verticale, “Degradation attacks on Passive Optical Networks,” 2012 16th Int. Conf. Opt. Netw. Des. Model. ONDM 2012, 2012, doi: 10.1109/ONDM.2012.6210184.

[6] T. Lukaseder, L. Bradatsch, B. Erb, R. W. Van Der Heijden, and F. Kargl, “A Comparison of TCP Congestion Control Algorithms in 10G Networks,” Proc. - Conf. Local Comput. Networks, LCN, pp. 706–714, 2016, doi: 10.1109/LCN.2016.121.

[7] J. Orozco and D. Ros, “TCP Performance over Gigabit-Capable Passive Optical Networks,” in AccessNets, vol. 6, 2009, pp. 264–279.

[8] N. Ansari and J. Zhang, Media Access Control and Resource Allocation. New York, NY: Springer New York, 2013.

[9] H. Nishiyama, Z. M. Fadlullah, and N. Kato, “Inter-layer fairness problem in TCP bandwidth sharing in 10G-EPON,” IEEE Syst. J., vol. 4, no. 4, pp. 432–439, 2010, doi: 10.1109/JSYST.2010.2082230.

[10] T. Horvath et al., “GPON Network with Simulated Rogue ONU,” in 2019 International Conference on Software, Telecommunications and Computer Networks (SoftCOM), 2019, pp. 1–5, doi: 10.23919/SOFTCOM.2019.8903811.

[11] M. Mathis, J. Semke, J. Mahdavi, and T. Ott, “The macroscopic behavior of the TCP congestion avoidance algorithm,” Comput. Commun. Rev., vol. 27, no. 3, pp. 67–82, 1997, doi: 10.1145/263932.264023.