Optica Applicata, Vol. XLVI, No. 3, 2016
DOI: 10.5277/oa160309

Novel rogue optical network unit detection algorithm for gigabit passive optical networks

Tomas HORVATH[1*], Petr MUNSTER[1], Lubos DUBRAVEC[2], Miloslav FILKA[1]

[1] Brno University of Technology, Faculty of Electrical Engineering and Communication,
Department of Telecommunications, Technicka 12, 616 00, Brno, Czech Republic

[2] Orange Slovensko, a.s., Metodova 8, 821 08 Bratislava-Ružinov, Slovakia

Passive optical networks are widely used as a promising solution for future access networks. Currently, the bandwidth is still increasing which means the current copper networks are not able to transfer new services such as 4K video, live streaming, *etc*. In other words, they reached their capacity limit. The passive optical networks rely on point-to-multipoint technology. That means each customer uses a share medium by time slots. Each time slot exactly specifies who and when is able to transfer data. In general, this control mechanism is implemented in the optical network unit by worst transmission convergence layer. On the other hand, there are cases when the optical network unit (it is called rogue optical network unit) does not follow instructions provided by the optical line termination, for example, if an attacker modifies a firmware of the end unit and/or when the control protocol is not loaded properly inside optical network unit. In worst case, the optical network unit transmits data in a continual mode (other optical network units cannot send data). The standard defines finding of the rogue optical network unit but it does not specify how the rogue optical network unit should be allocated because the frames of the rogue optical network unit do not contain the proper parameters. We realized a measurement in a real network with the rogue optical network unit and then we analyzed the captured data. A new algorithm for the rogue optical network unit allocation is presented. We do not consider any modification of the transmission convergence layer in gigabit passive optical networks.

Keywords: gigabit passive optical network (GPON), rogue optical network unit (ONU), data analysis, detection algorithm.

1. Introduction

Passive optical networks (PONs) was a widely discussed topic, and many operators have come to the conclusion that it is feasible solution for access networks due to the simplicity of the deployment, maintenance, and extension. From another point of view, current copper media are not able to provide a sufficient bandwidth, especially for longer distances between a head-office and customers.

An international conference called FTTX Council (FTTX – fiber to the X) annually deals with the development and appointment of the PON [1]. Lithuania was presented which has 14% of a market share with fiber to the home (FTTH) and 21% of a market share with fiber to the building (FTTB) technology. For example, in the Czech Republic FTTH/FTTB had about 14% of a market share as reported by Czech Telecommunication Office (CTO) in 2014. On the other hand, the European Union approved the broadband access for everyone at least with 30 Mbit/s (current customers) or 100 Mbit/s (new customers). The current Internet services providers (ISPs) develop a new infrastructure based on FTTH or FTTB because they are the technologies of most provision, from customers (bandwidth opportunities) and providers (bandwidth controling in optical domain) point of the view.

There are two standards groups of the PON, based on Institute of Electrical and Electronics Engineers (IEEE) or International Telecommunication Union (ITU). The first ones are based on Ethernet frames and the second ones use different encapsulation methods. In general, these standards spread around the world, the IEEE standards dominate in Asian access networks and the ITU solutions prevail in Europe networks [2]. Nowadays, the major part of access optical networks uses ITU standards. More precisely, the ITU defines the following standards: APON (ATM PON), BPON (broadband PON), GPON (gigabit PON), XG-PON (next generation PON), and NGPON2 (next generation stage 2 PON). First generation (APON and BPON) used asynchronous transfer mode (ATM) cells for data transmission. The main disadvantage was a static bandwidth allocation for each optical network unit (ONU). The GPON technology is currently used because the technology is mature and active elements are relatively cheap. XG-PON, in comparison with the GPON technology, is available only in laboratory or pilot appointment in the United States of America. The last one is still in development and only the physical layer specifications are done.

The main contribution of this article is a detection of the rogue ONU in real networks with GPON Xpert and concept of an algorithm for the optical line termination (OLT) which can detect the rogue ONU in the network in the real time without OLT disconnection.

The rest of this paper is structured as follows. Next section presents a description of the related works. Section 3 introduces the GPON technology and communication principles in GPON networks. Sections 4 and 5 deal with the measurement on the real network and an evaluation of the results. Section 6 proposes our algorithm for detection of rogue ONU in the real networks and Section 7 concludes our work.

2. Related works

In recent years, many works related to GPON technology have been published. Works published up to date deal with increasing split ratio, dynamic bandwidth allocation (DBA), security, and transmission convergence layer. Increasing split ratio is very important from the Internet services provider (ISP) point of view but it is necessary to deal also with the attenuation budget and timing relationship between active elements in real networks. However, a higher split ratio may respect the attenuation budget with the time relationship not be kept (the OLT has only 125 μs periods and the ONU has its own time slots with defined duration).

HAJDUCZENIA *et al*. [3] proposed the fault discovery protocol for PON. The main contribution of the article is an independent protocol for PON. In other words, they proposed the protocol for Ethernet PON (EPON) and GPON. Nowadays the rogue ONU should arise from the modified ONU with the attackers request.

BYUNGCHUL and CHOI [4] dealt with detection of failed ONUs in time division multiplexing PON (TDM-PON) using code division multiple access (CDMA) coding scheme. The authors focused on the upstream direction which is enough because the rogue ONU destroys the upstream direction. In general, the model needs to use CDMA coding scheme which is not satisfied because there is a necessity to make some changes in a frame.

Further, the paper [5] introduced the failed ONU detection technique applicable to commercially available PON by logical link identifier (LLID). Note that the authors dealt only with the EPON (Ethernet PON) because the EPON is dominating in the Asian access networks. The proposed algorithm should not be used in the PON according to the ITU standards because the LLID does not exist in these networks.

OISHI *et al*. [6] dealt with ONU tester for diagnosis of TDMA-PON (TDMA – time division multiple access) using multipoint control protocol messages. The product is able to detect the rogue ONU but the tester has to replace the OLT.

The paper [7] introduced the bandwidth analysis of multimode fiber based PONs. They compared three architectures of the multimode PON numerically and experimentally. Note that the main role in the bandwidth dividing has the splitter for the higher split ratio when the bandwidth is decreasing and *vice versa*.

JONGWOOK JANG and PARK [8] proposed the comparison of the DBA algorithms for PON. They dealt with the first standard of passive optical networks: APON with FIFO (first in, first out) queue and multiple FIFO. Note that the APON used only static DBA that means if the ONU did not have data, the time slot is still allocated for the same ONU.

In our previous paper [9] we provided the simulation of the transmission convergence layer in the XG-PONs. We dealt with the influence of an equalization delay and the refractive index on the timing.

Further, the papers [10–12] dealt with the security issues in the PONs, especially in GPON and EPON networks. We proposed the security solution in [10] and the novel authentication scheme in [11]. Paper [12] focused on EPON security issues which are relatively similar but in the EPON it is not difficult so understand the frame structures (EPON uses the Ethernet frame but GPON uses the ITU structures for data which contain the Ethernet frame).

3. GPON technology

As was mentioned before, the GPON technology is dominating in the Europe access networks because we deal only with this standard. The following text introduces GPON from the physical layer point of view. The basic characteristic contains: 1.244/2.488 Gbit/s bandwidth for downstream, 0.155/0.622/1.1244/2.488 Gbit/s for up-

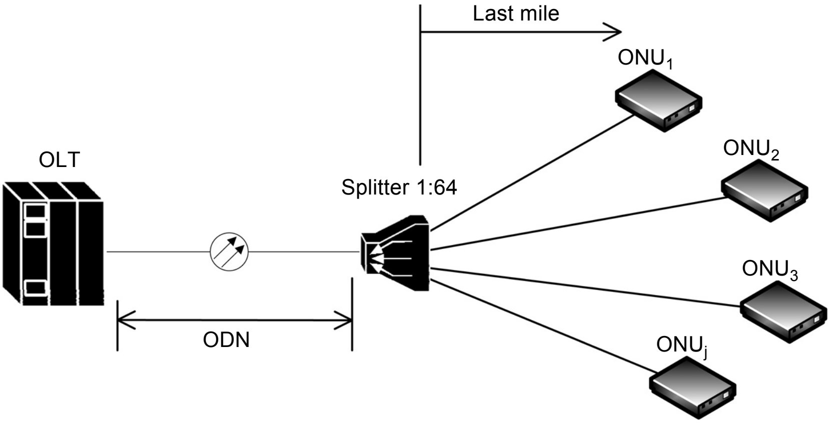

Fig. 1. The general scheme of GPON. OLT – optical line termination, ONU – optical network unit, ODN – optical distribution network.

stream, split ratio up to 1:64 (the standard advises up to 1:128), four attenuation classes N1, N2, E1, and E2 (nominal and extended), different wavelengths for each direction, and bit error rate (BER) either with forward error correction (FEC) 1×10^{-4} or without FEC 1×10^{-9} [13]. The basic topology for GPON is shown in Fig. 1.

Figure 1 shows basic components of the optical distribution network: OLT which is located in the central office in the provider part of the network, optical distribution network (ODN), which refers to each component (such as optical fiber, connectors, splitters, *etc*.) between OLT and ONU which is located in the customer part of the network. The term "last mile" defines the method of FTTX techniques; in most cases providers use FTTB or FTTH.

The following section deals with the communication principle in the downstream and upstream direction in GPON networks.

3.1. Communication in GPON network

GPON network is able to transfer data in the upstream and downstream direction but there is a difference between them. On the one hand, the downstream direction is centralized to the OLT which means that only OLT provides data, encapsulation, data formatting, frame formatting, *etc*., for each ONU. As was mentioned above, ODN contains the splitter which divides the optical signal into each ONU. How the ONU recognizes its own frame will be described later. On the other hand, the upstream direction is distributed in unicast because ONUs in the customer part of the networks have different data to transmit.

3.2. Downstream overview

The downstream traffic is centralized to the OLT. The OLT multiplexes GEM (GPON encapsulation method) frames into the transmission medium using GEM Port-ID. The Port-ID identifiers separated ONU, which means that in one frame should be data for many ONUs. We can imagine it like identifiers for the logical connection between OLT and ONU separate. Due to the fact that the downstream direction uses the broadcast, each ONU receives each frame. However, the frame with the exactly same Port-ID is processed and the rest is discarded.

3.3. Upstream overview

Upstream direction uses different schemes for the communication, in comparison with the downstream. In general, the OLT sends the frames to ONU with the exact specification of transmission parameters, or upstream bandwidth allocation, to the traffic-bearing entities within the matching ONUs [14]. The traffic-bearing entities are identified by their allocation IDs (Alloc-IDs). An allocation identifier is a 12 bit number that the OLT assigns to an ONU to identify a traffic-bearing entity. In other words, the traffic-bearing is the same such as transmission container (T-CONT) or optical network unit management and control channel (OMCC). Note that the ONU has to have at least one Alloc-ID which is the same with the ONU-ID that is something like the unique media access control (MAC) address and it is valid until the ONU is powered off. A traditional scheme of the GPON network contains the splitter with the huge split ratio (up to 1:128). In other words, each subscriber is in a different length from the OLT so the propagation time of the frames should be various (see Fig. 2).

Figure 2 shows the relation between times in GPON networks. First of all, the OLT prepares the frame with the following parts: PCBd (physical control block downstream), PSync (physical synchronization), BWMap (bandwidth map), and downstream frame payload (data). The frame is then transferred via the ODN to each ONU. Note that the propagation delay reflects various distances between OLT and ONU. ONU receives the header (PCBd) with the PSync and since then knows the time when the frame starts

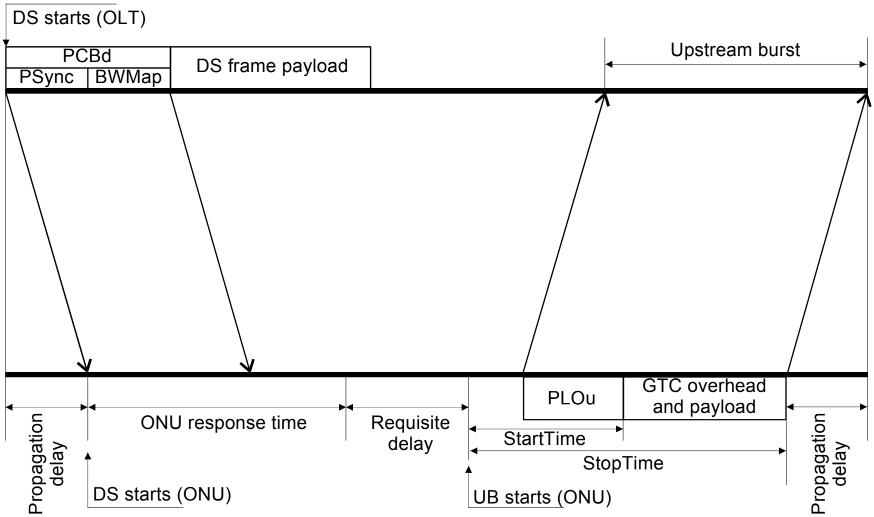

Fig. 2. Time relations between OLT and ONU in GPON [14]; see text for explanation.

but the most important is the BWMap because it specifies when and how many data should be transferred to the OLT. ONU has only a limited time to prepare an upstream response. A value of the ONU response time is 35 ± 1 μs. We need to consider the second parameter, a requisite delay. This delay has the most important role because it compensates various distances between OLT and ONU, various processing delays of individual ONUs, and the last one is to avoid or reduce collisions between upstream transmissions. The requisite delay value corresponds with the equalization delay specified by the OLT during the ranging state (more details about each state should be found in [15]).

4. Measurement setup

In the previous section the downstream and upstream communications were introduced. The principle of the upstream communication is to divide the bandwidth by time slots and each ONU gets its own slot by the downstream frame with the BWMap part. That is the reason why we cannot measure at one of the output ports of a splitter (1:64) because we do not receive each upstream burst. We connected another splitter in front of the last one for dividing the upstream direction. Note that GPON Xpert machine was used for our measurements with a post processing of data. The GPON Xpert uses the field programmable gate array (FPGA) for storing data for post processing and report generating. Figure 3 shows our measuring topology in GPON. In general, an additional splitter 1:2 is used, which means that the attenuation of the ODN is increased but ISPs have a reserve in used attenuation class and the attenuation of this splitter is around 3 dB. Due to the next splitter, the upstream communications are captured and stored in the GPON Xpert for post processing.

5. Measurement results

We proposed two simulation scenarios. The first one was in the real network with usual traffic, which means that the ONU respects its own time slots for transmission data

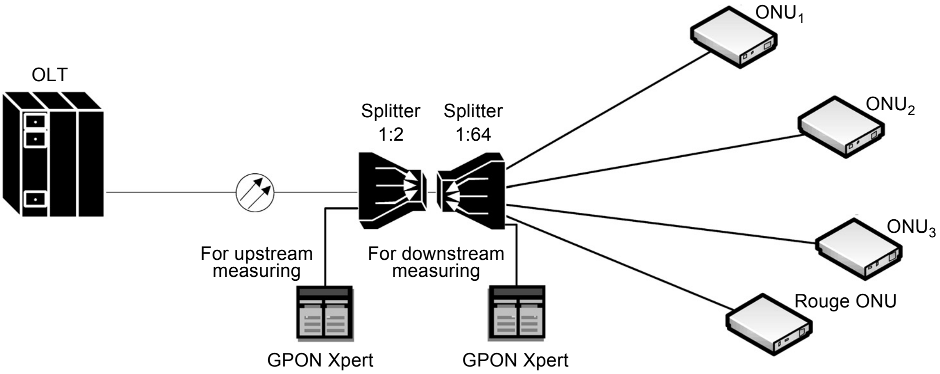

Fig. 3. The GPON networks with rogue ONU.

T a b l e 1. The details of the new ONU connected into the ODN in the registration process (the output is omitted).

Line	Message	Time	ONU ID	Message type	Message source	Direction
1	2	00:00:11.806177	Unassigned ONU ID	Serial number ONU	PLOAM message	Upstream
2	9	00:00:12.005427	Unassigned ONU ID	Serial number ONU	PLOAM message	Upstream
3	14	00:00:12.198677	Unassigned ONU ID	Serial number ONU	PLOAM message	Upstream
4	16	00:00:12.398927	Unassigned ONU ID	Serial number ONU	PLOAM message	Upstream
5	40	00:00:56.698166	Unassigned ONU ID	Serial number ONU	PLOAM message	Upstream
6	42	00:00:57.091666	Unassigned ONU ID	Serial number ONU	PLOAM message	Upstream
7	44	00:00:57.290916	Unassigned ONU ID	Serial number ONU	PLOAM message	Upstream
8	363	00:00:57.539500	Broadcast message	Assign ONU-ID	PLOAM message	Downstream
9	364	00:00:57.539625	Broadcast message	Assign ONU-ID	PLOAM message	Downstream
10	365	00:00:57.539750	Broadcast message	Assign ONU-ID	PLOAM message	Downstream
11	369	00:00:57.740125	2	Ranging request	BWMap event	Downstream
12	1	00:00:57.740161	2	Serial number ONU	PLOAM message	Upstream
13	370	00:00:57.741500	2	Ranging time	PLOAM message	Downstream
14	371	00:00:57.741625	2	Ranging time	PLOAM message	Downstream
15	372	00:00:57.741750	2	Ranging time	PLOAM message	Downstream
16	374	00:00:57.777750	2	Configure Port-ID	PLOAM message	Downstream
17	375	00:00:57.777875	2	Configure Port-ID	PLOAM message	Downstream
18	376	00:00:57.778000	2	Configure Port-ID	PLOAM message	Downstream

Table 2. The data communications between ONU and OLT (the output is omitted).

Line	Packet	Time (start of capture)	Source port	Destination port	Length	Direction
1	1	00:00:11.806177	DHCPv6 client (546)	DHCPv6 server (547)	103	Upstream
2	1	00:00:12.005427	DHCPv6 server (547)	DHCPv6 client (546)	151	Downstream
3	2	00:00:12.198677	39272	DNS (53)	46	Upstream
4	3	00:00:12.398927	39272	DNS (53)	46	Upstream
5	2	00:00:56.698166	DNS (53)	39272	74	Downstream
6	3	00:00:57.778000	DNS (53)	39272	85	Downstream

Table 3. The details of the rogue ONU traffic in the real network (N.A. – not available).

Line	Packet no.	Timestamp	PLOAM ONU-ID	PLOAM message type	BWMap	TCONT-ID	GEM payload type	DBRu mode	Frame	Slot	Direction	Raw data
1	1	00:01:08.140930	N.A.	N.A.	N.A.	253	N.A.	0	545125	3364	Upstream	0xAEAB59831E0418
2	2	00:01:08.144119	N.A.	N.A.	N.A.	253	N.A.	0	545150	13270	Upstream	0xAEAB59831E0418
3	3	00:01:08.146184	N.A.	N.A.	N.A.	253	N.A.	0	545167	3999	Upstream	0xAEAB5983008418
4	4	00:01:08.146934	N.A.	N.A.	N.A.	253	N.A.	0	545173	3999	Upstream	0xAEAB5983018418
5	5	00:01:08.150727	N.A.	N.A.	N.A.	253	N.A.	0	545203	10730	Upstream	0x02AB5983018A78
6	6	00:01:08.152684	N.A.	N.A.	N.A.	253	N.A.	0	545219	3999	Upstream	0xAEAB5983018418
7	7	00:01:08.156434	N.A.	N.A.	N.A.	253	N.A.	0	545249	3999	Upstream	0xAEAB5983018418
8	8	00:01:08.158219	N.A.	N.A.	N.A.	253	N.A.	0	545263	9460	Upstream	0xAEAB59831E0418

without rogue ONU. The second scenario was with the usual traffic and rogue ONU. Note that in our measurement by rogue ONU we mean the ONU with the modified firmware because it does not respect the time slot. In general, we can say that the rogue ONU laser transmits in CW (continuous wave) mode. For example, in the first scenario we connected the new ONU into the network and captured the traffic between OLT and ONU as can be seen in Tables 1 and 2. The ONU needs to pass the whole registration process (the details about registration process were presented in [15]) and data communication. The outputs are omitted. The GPON Xpert is able to analyze signaling, OMCI channel, Ethernet, IPv4 (Internet protocol), IPv6, and UDP (user datagram protocol) communications. We choose only the signaling and UDP communication as an example. The second scenario dealt with measuring the rogue ONU in the real network. Then after the traffic was captured and post processed, we analyzed data from the GPON Xpert. As should be expected, the rogue ONU did not follow the time slots in the network and did not provide any information about itself. On the other hand, it is necessary to find the solution how to discover the rogue ONU in the network as soon as possible. As was mentioned before, the ONU has its own time slots and unique parameters which may be used for the detection of the rogue ONU.

Tables 1 and 2 contains the worst case for the ONU because in the real network we modified the ONU, which means that the laser does not follow the instruction for "on" and "off" time. In other words, the ONU has CW laser. In [16] two scenarios how the ONU should become the rogue ONU were defined. No scenario defines the modified firmware by an attacker which is so important from the security point of view. The standard defines only two possibilities for the rogue ONU: MAC and transceiver errors. More precisely, the MAC error should be caused by the incorrect loading of the program in FPGA, which means that the behavior of the ONU is undefined; the transceiver error is very probable with only a handful of transistors between a Tx-enable pin and laser [16].

Table 3 shows the data from the GPON Xpert after post processing. As can be seen from Table 3, the rogue ONU does not contain ONU-ID, BWMap, and TCONT-ID. If we consider that the rogue ONU still uses exactly the same ONU-ID and Alloc-ID, these parameters should be used for the rogue ONU detection. On the other hand, Table 3 shows that the parameters are not used because we measured the worst case of the rogue ONU (continual transmitting). We will deal with the detection of the rogue ONU in the following Section.

6. Algorithm for rogue ONU detection

In the previous Section we have shown the measurement results from the worst case of the rogue ONU behavior. It is defined by the rogue ONU which transmitted data all-time without respecting the time slots provided by OLT. The worst scenario is a unique case in real networks and can be realized by CW laser placed in one of the output ports of a splitter (1:64). As it was mentioned above, in [16] two scenarios of ONU failure (MAC and transceiver errors) have been shown. When we consider that the attacker can modify the firmware of ONU, then it is necessary to provide an algorithm which is able to detect these ONUs as soon as possible. The main purpose of this article is the algorithm for rogue ONU detection which is shown in Fig. 4.

Our algorithm starts with an identifiers inspection. In general, the traffic in the ODN has to have the unique identifiers (ONU-ID, Alloc-ID, T-CONT ID, *etc.*) which are unique for each ONU. If the identifiers are right, the traffic in the network is correct. If they are not, the OLT checks attenuation in the ODN by a power level of each ONU. In case the attenuation is not exactly the same, then OLT sends a report message to control the centre (central office). In opposite case, it continues with the next phase

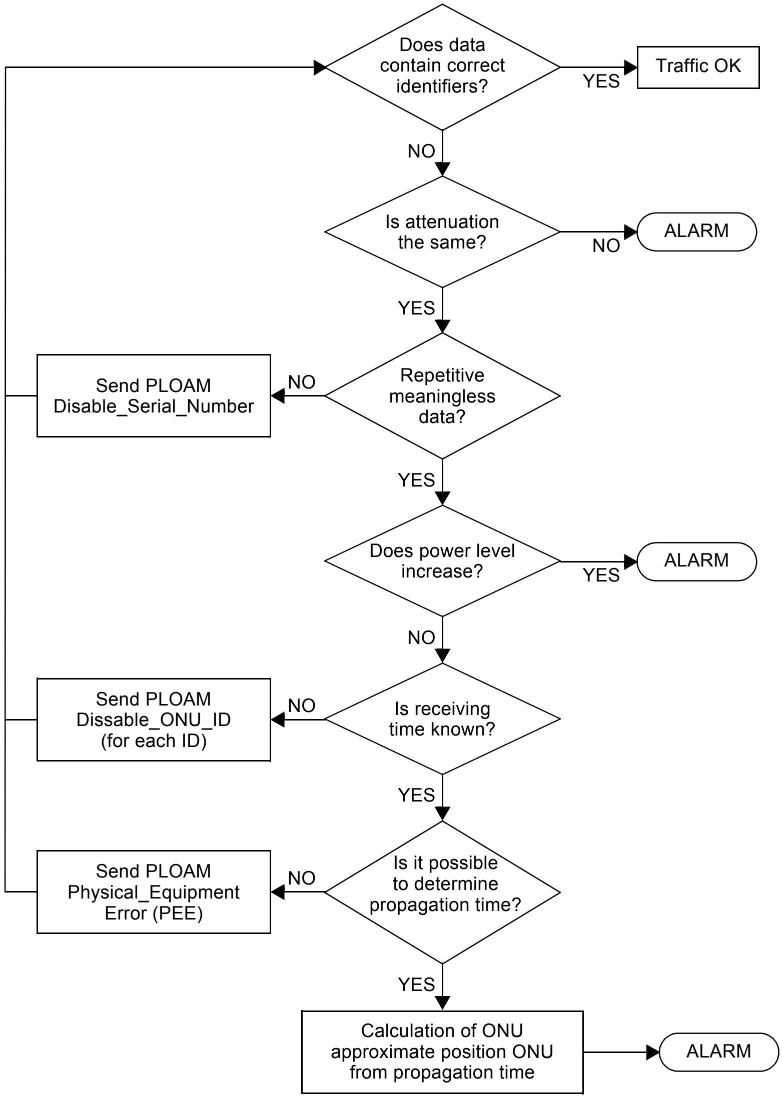
Does data contain correct identifiers?
YES
Traffic OK
NO
Is attenuation the same?
NO
ALARM
YES
Repetitive meaningless data?
NO
Send PLOAM Disable_Serial_Number
YES
Does power level increase?
YES
ALARM
NO
Is receiving time known?
NO
Send PLOAM Dissable_ONU_ID (for each ID)
YES
Is it possible to determine propagation time?
NO
Send PLOAM Physical_Equipment Error (PEE)
YES
Calculation of ONU approximate position ONU from propagation time
ALARM

Fig. 4. The novel rogue ONU detection algorithm.

(checking repetitive meaningless data). The OLT contains a database with the records of each ONU (power level, ONU-ID, Alloc-ID, T-CONT ID, *etc*.). We consider that the power level is still the same because the power level is setup in the registration phase by OLT and when the attenuation of the ODN is increased. In other words, in comparison with the current records, the OLT sends PLOAM (physical layer operation admission and maintenance) message *Disable_Serial_Number*. In second case the data are still the same (data contain a meaningless format).

The OLT checks if the power level is increasing. For an increased power level, the OLT sends a report message to the control centre (central office). Otherwise, the OLT moves to the next phase in algorithm where the OLT verifies if it is able to read the receiving time from GTC frames. For example, Table 3 shows the meaningless data from the rogue ONU where the OLT is able to read the receiving time. Alternatively, the OLT sends PLOAM message *Disable_ONU-ID* (for each ONU-ID from a database). The following phase deals with determining the propagation delay time for rogue ONU. In other words, if there are frames with a receiving time, the OLT may calculate the propagation time if not the OLT sends PLOAM message *Physical_Equipment_Error* (PEE). The last phase calculates an approximate position of ONU by the propagation time parameter. In [14] a coefficient 100 m/μs for single mode fibers G.652 is defined. Then the OLT sends a report message to the control centre (central office).

Note that the PLOAM message *Disable_Serial_Number* causes that the ONU moves to the emergency stop state. In other words, the ONU stops to transmit data in the upstream direction, it cannot respond to the upstream bandwidth allocation. The PLOAM message disable ONU-ID makes the ONU turn off the laser and the ONU-ID, Port-ID, and Alloc-ID are discarded. More precisely, the ONU is in the standby state. The PLOAM message *Physical_Equipment_Error* (PEE) causes that the ONU activates its own alarm and moves to the *standby* state (forced state). The most important part of the rogue ONU is that only the upstream direction is affected but the ONU is able to receive the downstream control message.

7. Conclusion

The first mention about the passive optical network in a research field was proposed in 1989 [17]. The researchers used the asynchronous transfer mode (ATM) cell format. The current state in optical access networks is to transfer users data to many subscribers in the real network with a bandwidth as high as possible. Nowadays, new services are still being developed such as real-time streaming, 4K video, *etc*. That is the main reason why the optical fibers are popular in access networks especially when their price is decreasing.

The ONU and OLT use the same implementation of the TC layer. The ONU has a transceiver and FPGA part. In general, the ONU has to respect allocation structures provided by OLT. When the attacker is able to modify firmware of ONU and/or the FPGA application is not loaded properly, it causes that the ONU does not follow allocation structure. In other words, the ONU transmits data in a continual mode and other ONUs is/are not able to transmit data. The current standard defines fundamental information how to avoid the rogue ONU in network.

We proposed a novel algorithm for the rogue ONU detection. It is based on measurements in the real network with the rogue ONU. Our algorithm contains the following parts: detection of an anomaly in data, checking the attenuation in the ODN, checking correctness data, checking the receiving time of frames, and determining the approximate position. The last phase of the algorithm sends the approximate position of the rogue ONU to the central office. Note that it is the worst case because the ONU (normal and rogue) should have an ability to process downstream messages which are provided by the OLT. For the research, the infrastructure of the Orange Slovakia was used.

The future research will continue with implementation of our model into a real optical network and with verification of our algorithm.

Acknowledgements – Research described in this paper was financed by the National Sustainability Program under grant LO1401.

References

[1] JACKSON M., *UK ultrafast FTTH fiber optic broadband lines slow to grow – global ranking*, FTTH Council, February 18–20, 2014, Stockholm.

[2] PAN H., China Telecom Monthly Newsletter **17**(11), 2010, pp. 1–5.

[3] HAJDUCZENIA M., FONSECA D., DA SILVA H.J.A., MONTEIRO P.P., *Fault discovery protocol (FDP) for passive optical networks (PONs)*, 12th IEEE Symposium on Computers and Communications, July 1–4, 2007, Aveiro, IEEE, pp. 101–106.

[4] BYUNGCHUL CHOI, JAESUNG KIM, EUN-MO YEO, YOUNGIL P., *Detection of failed ONUs in TDM-PON using CDMA coding scheme*, 14th OptoElectronics and Communications Conference, July 13–17, 2009, Hong Kong, IEEE, pp. 1–2.

[5] OISHI M., OHARA K., HORIUCHI Y., *Failed ONU detection technique applicable to commercially available passive optical networks*, 36th European Conference and Exhibition on Optical Communication, September 19–23, 2010, Torino, IEEE, pp. 1–3.

[6] OISHI M., HORIUCHI Y., NISHIMURA K., *ONU tester for diagnosis of TDMA-PON using multi-point control protocol messages*, 10th International Conference on Optical Internet, May 29–31, 2012, Yokohama, Kanagawa, IEEE, pp. 81–82.

[7] STEPNIAK G., MAKSYMIUK L., SIUZDAK J., *Bandwidth analysis of multimode fiber passive optical networks (PONs)*, Optica Applicata **39**(2), 2009, pp. 233–239.

[8] JONGWOOK JANG, PARK E.K., *Dynamic resource allocation for quality of service on a PON with home networks*, IEEE Communications Magazine **38**(6), 2000, pp. 184–190.

[9] KOCI L., HORVATH T., MUNSTER P., JURCIK M., FILKA M., *Transmission convergence layer in XG-PON*, [In] *2015 38th International Conference on Telecommunications and Signal Processing (TSP)*, 2015, pp. 104–108.

[10] HORVATH T., MALINA L., MUNSTER P., *On security in gigabit passive optical networks*, International Workshop on Fiber Optics in Access Network (FOAN), October 6–7, 2015, Brno, Czech Republic, pp. 1–5.

[11] Malina L., Munster P., Hajny J., Horvath T., *Towards secure gigabit passive optical networks*, International Conference on Security and Cryptography, July 20–22, 2015, France, pp. 349–354.

[12] Hajduczenia M., Inacio P.R.M, Da Silva H.J.A., Freire M.M., Monteiro P.P., *On EPON security issue*, IEEE Communications Surveys and Tutorials **9**(1), 2007, pp. 68–83.

[13] *G.984.2: Gigabit-Capable Passive Optical Networks (G-PON): Physical Media Dependent (PMD) Layer Specification*, International Telecommunication Union, 2003, pp. 1–38.

[14] *G.984.3: Gigabit-Capable Passive Optical Networks (G-PON): Transmission Convergence Layer Specification*, International Telecommunication Union, 2003, pp. 1–170.

[15] Horvath T., Munster P., Jurcik M., Koci L., Filka M., *Timing measurement and simulation of the activation process in gigabit passive optical networks*, Optica Applicata **45**(4), 2015, pp. 459–471 .

[16] *G.Sup49 Rogue Optical Network Unit (ONU) Considerations*, International Telecommunication Union, 2011, pp. 1–16.

[17] McGeeney B.M., *Performance of an integrated services ATM protocol over a broadband passive optical network*, 6th United Kingdom Teletraffic Symposium, May 24–26, 1989, Harlow, pp. 12/1–12/8.

Received January 22, 2016
in revised form March 15, 2016