A Novel Unique Parameter for Increasing of Security in GPON Networks

Tomas Horvath, Petr Munster, and Miloslav Filka

Original scientific paper

***Abstract*—Passive optical networks are widely used because of their sufficient bandwidth and low price of individual elements. Based on the European Commission, The Czech Republic ISPs have to ensure 30 Mbit/s (in existing networks) and 100 Mbit/s (in new constructed networks) for each customer in selected areas till 2020. Nowadays, the GPON standard is dominating in the Europe due to its low price and maturity. In general, the passive optical networks are based on P2MP (Point to Multipoint) physical topology. Therefore each end unit receives data meant for all units. To mitigate this, the standard defines an encryption method (authentication and key exchange phase) but the key exchange phase relies only on a single unique parameter (serial number of an end unit). A new unique parameter for the key exchange phase is proposed. No modification of the transmission convergence layer in GPON is considered. A measuring scheme for determining of accuracy of our new unique parameter, called T_{prop}, is also proposed.**

***Index Terms*—GPON, propagation time, security, measurement.**

I. Introduction

The amount of transmitted data in access and metro networks is increasing by 20 to 30 % every year [1]. This relentless growth of Internet traffic might be solved by the development of advanced technologies, such as EON (Elastic Optical Networks), WDM (Wavelength Division Multiplex), or by traffic grooming in backbone networks, etc. [2],[3]. Also, the European Union established contracts for member states which define the minimum bandwidth for current and new customers in selected areas (areas with low bandwidth).

Although the bandwidth is probably the most important parameter in access networks from the customer's point of view, security is even more important, though not always fully appreciated by the end users. In general, we consider that an ISP (Internet Service Provider) will choose the GPON (Gigabit Passive Optical Network) standard due to its maturity and relatively low price of elements (active elements). Furthermore, migration from the GPON to the XG-PON (Next Generation PON) is possible because both standards use the same ODN (Optical Distribution Network).

Note that the active elements of GPON can use the same ODN but cannot transfer data at transmission speeds of the XG-PON and so must be replaced when updating network. On the other hand, when the ISPs develop high quality ODN (if they respect attenuation class, split ratio, etc.), they can easily increase the bandwidth for each end-user because of installation of optical fiber to customers home. In other words, we consider that the ISPs use two level of the signal splitting. First splitter is connected to OLT (Optical Line Termination) port (typically 1:2) and the second splitting is in the ODN near to the customer's premises (split ratio typically higher than 1:4, it depends on a number of customers in the building) which is called FTTB (Fiber To The Building) method when a different kind of transmission media is used from the second splitter onwards, or FTTH (Fiber To The Home) if optical fiber is used exclusively. The above mentioned methods are dominating in the European Union [4].

The main contribution of this paper is the proposal of usage of a propagation time as a per ONU unique parameter for encryption key establishment in GPON networks. This change has no impact on currrent frame structure, but requires substantial changes transmission convergence layer processes O5.

The rest of this paper is structured as follows. In the next section we get an overview of the related works. Section 3 presents the authentication process in GPON networks. Section 4 describes the proposed improvement of authentication process and the measurement results with the discussion of implementability into real GPON networks. Section 5 concludes the paper.

II. Related Works

In the last few years, many works related to GPON technology have been published. Works published up to date focus on physical and transmission layers of the GPON technology, especially on reach extended networks, end-to-end QoS (Quality of Services), framing in GPON and security in GPON.

The authors in [5] and [6] introduced the security enhancements in novel passive optical networks. They used a TDM (Time Division Multiplexing) between OLT and ONU which allowed to create an unique P2P (Point to Point) connection between OLT and each of the ONUs. In general, it is the main aim of the NG-PON2 (Next Generation PON second stage) in TWDM PON technology combination.

The work [7] introduced solution for multimedia pseudo security in case of Triple Play in passive optical networks via techniques of wavelength hopping and alternating the codes used. Only a technique for downstream direction was proposed, what is also insufficient nowadays as the attacker is

Manuscript received February 14, 2016; revised June 8, 2016.

Research described in this paper was financed by the National Sustainability Program under grant LO1401, and SIX CZ.1.05/2.1.00/03.0072. For the research, infrastructure of the SIX Center was used.

Authors are with Department of Telecommunications, Brno University of Technology, Brno, Czech Republic (E-mails: {horvath, munster, filka}@feec.vutbr.cz).

also able to capture upstream in case of physical access to the fibre.

The papers [8]–[10] deal with the security in PON networks. They identify and classify requirements for the attacks but the authors in [8] consider an addition of an active element into the topology for defense purposes. The question arises whether an ODN with an additional active elements should still be called passive.

Aleksic et al. [11] presented a quantum key distribution scheme over optical access networks. In general, the security is improved by the quantum cryptography but the most crucial argument in favor of optical access networks is the price. If we consider implementation of quantum key cryptography into PONs, the prices will be enormously high but also the security will be very strong. Though the price of active elements for PONs is decreasing, it is not same for quantum cryptography equipment.

In papers [12]–[14] we have provided simulations of the transmission convergence layer and analyzed several security issues in GPON. In [14] we have simulated an equalization delay and influence of the refractive index on the timing. Further, the paper [13] deals with the security issues in GPON networks such as: eavesdropping attack, replay attack, interception (tampering) attack, impersonation attack, DoS (Denial of Service), and ToS (Theft of Service). Both papers [12] and [13] contain novel security methods for GPON while not touching the transmission converge layer. No modification or additional messages are considered.

III. Authentication and Key Exchange Process

The following text deals with security issues and the authentication process in GPON networks. Note that the authentication process is defined as part of the Operational State O5 of each ONU. States description is beyond the scope of this paper, details should be found in [15]). As mentioned, ONU needs to reach the Operational State (O5), which means the unit is able to transfer data bidirectionally, to start the authentication process. More precisely, data are transmited by OLT in time slots. Each ONU has own time slots which can be used for transmission of data. The most important property is that the data are not encrypted in any way. The attacker is able to read the frames in the downstream direction because data are broadcasted, he/she only needs physical access to the fibre or a splitter. The frame structure is defined by [16]. Such a splitter is often located in the building's basement or similar publicly accessible place. If we consider the upstream direction, data are transferred by unicast. In general, the attacker can tap the fibre just before the splitter, as shown in Fig. 1. The GPON standard contains more security issues (see in [12] and [13]) but we mentioned only the general methods how the attacker can receive upstream and downstream communication.

Authentication process, as described in Fig. 2 (left), is optional in ODN, specifically a part of O5. By default it is disabled and therefore data are sent without any encryption. The authentication process is designed as follows. First of all the OLT initializes a random instance register for an ONU, a 3 octet value, this fact is then signalled to ONU using a PLOAM

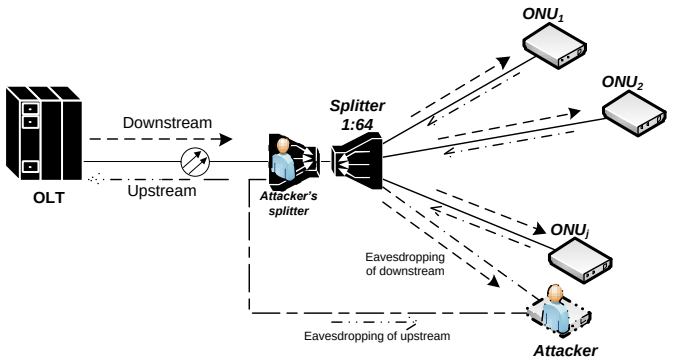

Fig. 1. Basic scheme describing how the attacker can listen upstream and downstream.

message. The ONU enters the challenge pending state and waits for a PLOAM message containing the random instance number. Note that the ONU has own pre-configured values for authentication process, which are compared during the pending state. The ONU has to respond to the OLT during the period of 3 seconds (TO1 timer). If the OLT does not receive any message from ONU in pending state the authentication process finishes with an error and must be restarted. Otherwise the authentication process is done, OLT and ONU have been authenticated. Then the OLT can start a key exchange phase, shown in Fig. 2 (right), with the authenticated ONU. The key exchange phase is initiated by the OLT and the ONU acts on a request-response basis. In general, the OLT is a master in communication and ONUs are slaves. The OLT sends a security announcement and PLOAM message no. 11 (Request_key) to ONU. ONU receives the PLOAM message and computes the encryption key from unique information such as the unit's serial number. The key is then sent to the OLT in a PLOAM message no. 5 (Encryption_key). However, the PLOAM message has a space of only 8 octets for the key, so the ONU should use fragmentation and divide the key into multiple messages. If multiple messages are used, the third header octet contains the fragment sequence number, known as "order of key", and the fourth octet is used as fragmentation indicator. In general, it is not important how many messages were sent, the whole key has to be repeated three times. Next the OLT receives the key which is exactly the same in all cases, it is stored and sent back to ONU with a command containing the frame number and new key. The ONU compares the received key with the generated and if they match, the new encryption key is used. If the key is to be renewed afterwards, the same process is repeated.

IV. Proposal of an Additional Key Establishment Parameter

In previous section we dealt with the authentication process and key exchange phase as defined by the specification. Especially the fact that the key exchange phase relies on a single unique parameter (serial number). If we consider that attacker is able to find an algorithm corresponding to an assignment function he/she is able to find the secret key of ONUs. Nowadays, the authors [17] deal with security issue

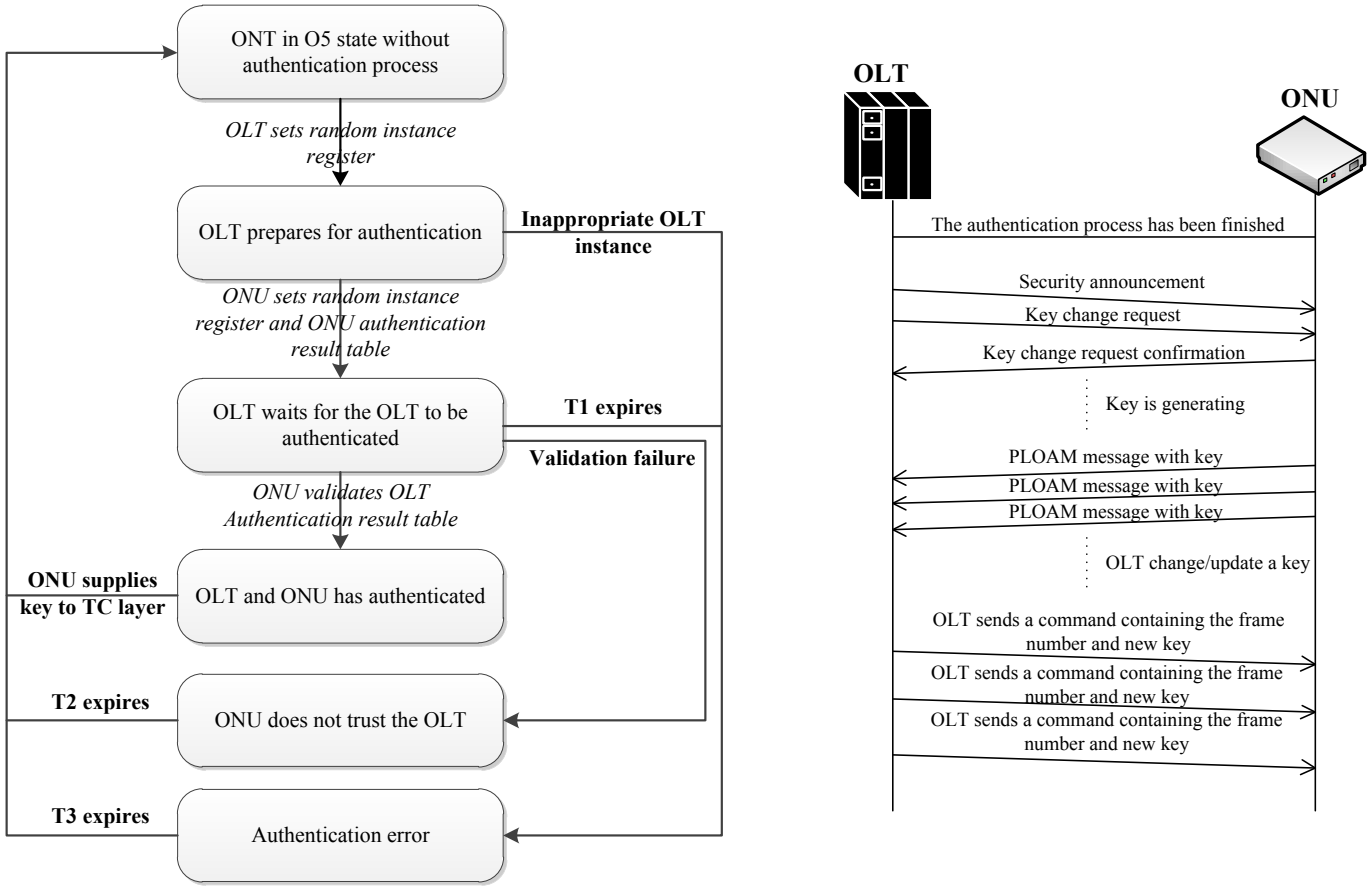

Fig. 2. The authentication (on the left side) and key exchange phases (on the right side) in GPON networks.

in NG-PON with FPGA (Field Programmable Array) in real time. When we consider that the FPGA are used for real time traffic analysis (more than 40 Gb/s) the assignment function should be found in short time because the first three octets identify a producer of active elements (brand).

The passive optical networks use splitters for affiliation of end-users. The first section dealt with methods of termination of optical fiber. From the future point of view the better solution is FTTH because there are ”no transmission” limits thanks to connection of each user by optical fiber. We propose new unique parameter for the key encryption phase (we note this parameter as T_{prop}). The parameter specifies the time for transferring data between OLT an ONU. When we consider the basic topology of the passive optical networks (see Fig. 3) in real network each ONU has different distance from the OLT. That is the reason why our parameter T_{prop} is unique for each customer's ONU. For example, the ISP tries to find a housing scheme with a lot of customers in the same building or complex but each building has many floors and hence fiber distances between customers in the first and the last floor are completely different. More precisely, the parameter T_{prop} will have different value between OLT and ONU for each customer.

The standard encryption model uses only the single secret (saved by producer). Note that the OLT should send a request for the key changing but it will use again random numbers and stored secret. Our model is unique in another point of view.

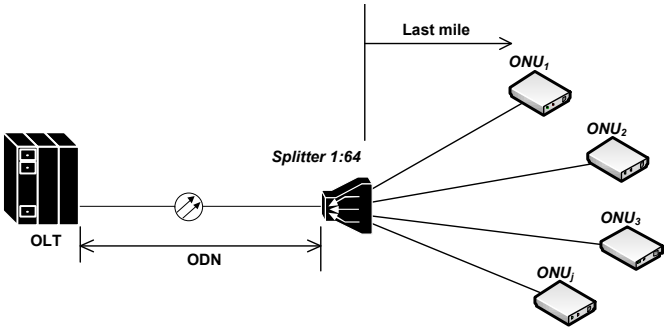

Fig. 3. The general scheme of GPON networks.

The ONU has different T_{prop} delay. It is not necessary to send any message with T_{prop} value by ODN. In other words, the OLT and ONU know the same value because each of them knows the time of sending and receiving frame. If it is necessary, the OLT can specify the specific value (by PLOAM message 11 in downstream – Request_Key – which will be added for the T_{prop}.

A. Experimental setup

We wanted to verify the updated scheme in a real network, however, manufactures of GPON elements do not provide any API (Application Programming Interface). In general, if we

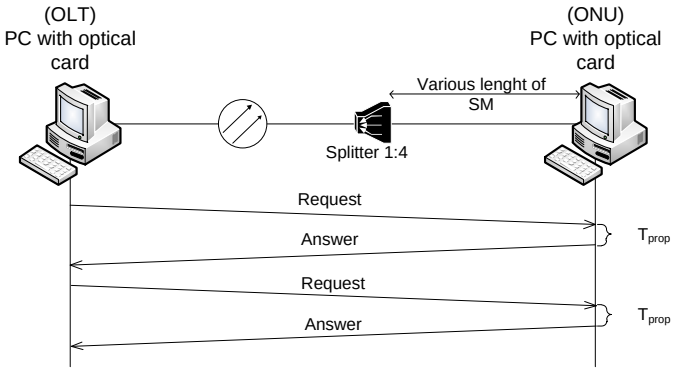

Fig. 4. Alternate scheme to GPON network with T_{prop} measuring.

consider that OLT and ONU use the ODN for data transfer we do not need exactly GPON active elements (ONU and OLT) because they transfer only Ethernet frames encapsulated into GTC (GPON Transmission Convergence) frames [16]. An alternate scheme was proposed for our verification, see Fig. 4.

The real network contains the SM (Single mode) fibers, splitters, and active elements. In our scheme we used two PC (Personal Computer) with optical cards (Broadcom NetXtreme II BCM57711) having SFP (Small Form-factor Pluggable) slots, SFPs (Finisar FTLX1671D3BC), splitter with lowest splitting ratio, and various length of the SM placed after 1:4 splitter. In comparison with real network we used splitter with lower split ratio due to using of longer lengths of fibers, and since the splitter is a passive element without any time influence – only divides the upstream or downstream directions.

B. Measuring of T_{prop}

As was mentioned, we have designed an alternate scheme that is in principle relatively same in comparison with a real network. The second step was a proposal of methodology how to measure T_{prop} parameter. For example, when we consider networks based on the Ethernet we can use ping command in CMD (Command Line) but it uses ICMP (Internet Control Message Protocol) at the third layer of the ISO/OSI (International Organization for Standardization/Open Systems Interconnection) model but GPON networks use only the first two layers of ISO/OSI model. In general, ARP (Address Resolution Protocol) works at the second layer in Ethernet networks. We used *arping* request with known physical addresses of the cards but values were measured in ms units. That is the reason why we needed to use Wireshark application in both PCs and thanks to that we were able to store time stamp of each frame (Wireshark uses μs unit). The measurement of each request was repeated nine times and for post-processing we considered same order of frames. In other words, we used the second, third, and fourth frames for our post-processing (evaluating T_{prop} parameter from request and response time).

C. Experimental results

We proposed three measurement scenarios in our ODN using 1, 20, and 40 km lengths of optical fibers. The real network has an ODN limit length of 20 km due to attenuation and time synchronization but we used also 40 km length for verification of T_{prop}. For double length of ODN we expected that T_{prop} will be two times higher. The results of all measurements are shown in Table I.

TABLE I
RESULTS OF THE TPROP MEASURING.

ODN length [km]	T_{prop} A→B [μs]	T_{prop} B→A [μs]
1	278	278
20	435	435
40	594	594

From Table I is obvious that we obtained the same values in the considered frame sequence. It is a proof that our proposed measurement works in alternate network environment and also will work in real networks, because for different lengths the values of propagation delay (with ping command) were different and the measurement error was around $1 \cdot 10^{-5}$. From the results we can deduce accuracy in the range of several meters for each ONU. In general, the measured propagation delay in 20 km of SM fibre is approximately $\approx$158 μs, $\approx$317 μs in 40 km respectively. For one kilometre long optical fibre the measured T_{prop} is $\approx$8 μs (includes propagation delay in optical fibre and processing time). Based on this knowledge we can infer that in our measurement for 1 km long ODN the value 270 μs from the total result 278 μs represents the processing time. Finally, we can solve for the accuracy, which is 126 m. This resolution means the customers on the first and the last floors will have different T_{prop}. Finally, in combination with the serial number this parameter could be used in the key exchange phase for improved security in GPON networks.

The most important part of our solution is a unit of measurement. When it is able to measure in "ns" unit, then it can eliminate the same T_{prop} value for two customers. On the other hand, each ONU has unique secret (provided by producer which is used for the generating the security key among others).

V. CONCLUSION

Nowadays the passive optical networks are widely used in access networks and this should continue in the near future due to the maturity of the technology and low price of the elements. Further, a new services such as 4K video streaming, or high volume background data transfer are becoming more common and this will cause even the GPON networks to be insufficient. On the other hand the access networks should not only offer high bandwidth, but also provide security of the payload. Threat of a high customer churn rate due to reputation of not providing enough information security is very real for the ISPs. The current PON encryption scheme depends on only one unique parameter (for example serial number) and the practice of detecting fibre tapping is not very advanced among the ISPs.

We proposed a new parameter for improvement of the passive optical networks encryption key establishment scheme. In general, it is an unique parameter for each ONU with different distances between nodes. The attacker is not able

to estimate this parameter because he/she does not know the real distance between OLT and ONU. That is one of the most important aims of our work. The second main aim was to design the unique parameter without any modification in the transmission convergence layer of the PON. This was bounded by PLOAM messages but we also considered a simple model request/response. We proposed solution with 126 m accuracy which means time stamp unit in (μs).

The future research will continue with implementation of our model into a real optical network and improvement of time resolution into the (ns) range.

REFERENCES

[1] Cisco: *The Zettabyte Era: Trends and Analysis*, 2015.

[2] Tibor Cinkler. Traffic and grooming, *IEEE Network*, vol. 17, issue 2, pp. 16–21, 2003.

[3] Bijoy Chand Chatterjee, and Eiji Oki. Performance evaluation of spectrum allocation policies for elastic optical networks, *2015 17th International Conference on Transparent Optical Networks (ICTON)*, no. 1, pp. 1–4, 2015.

[4] Mark Jackson. UK Ultrafast FTTH Fibre Optic Broadband Lines Slow to Grow – Global Ranking, FTTH Council, no. 1, 2014.

[5] Alan Harris, Andres Sierra, Stamatios V. Kartalopoulos, and James J. Sluss Jr. Security Enhancements in Novel Passive Optical Networks, *2007 IEEE International Conference on Communications*, no. 1, pp. 1399–1403, 2007.

[6] Alan Harris, David R. Jones, Keith H. Horbatuck, and Andres Sierra. A Novel Wavelength Hopping Passive Optical Network (WH-PON) for Provision of Enhanced Physical Security, *Journal of Optical Communications and Networking*, vol. 4, issue 3, pp. 289–295, 2012.

[7] Walid Shawbaki. Multimedia Security in Passive Optical Networks via Wavelength Hopping and codes cycling technique, *Advanced Intl Conference on Telecommunications and Intl Conference on Internet and Web Applications and Services (AICT-ICIW06)*, no. 1, pp. 51–51, 2006.

[8] Y. Yan, S. Yamashita, S.-H. Yen, P.T. Afshar, V. Gudla, L.G. Kazovsky, and S.-W. Wong. Invited Paper: Challenges in next-generation optical access networks, *IET Optoelectronics*, vol. 5, issue 4, pp. 133–143, 2011-08-01.

[9] A. Teixeira, A. Vieira, J. Andrade, A. Quinta, M. Lima, R. Nogueira, P. Andre, and G. Tosi Beleffi. Security issues in optical networks physical layer, *2008 10th Anniversary International Conference on Transparent Optical Networks*, no. 1, pp. 123–126, 2008.

[10] Walid Shawbaki, and Ahmed Kamal. Security for FTTx Optical Access Networks, Proceedings. *2006 31st IEEE Conference on Local Computer Networks*, no. 1, pp. 221–228, 2006.

[11] Slavisa Aleksic, Dominic Winkler, Gerald Franzl, Andreas Poppe, Bernhard Schrenk, and Florian Hipp. Quantum key distribution over optical access networks, *Proceedings of the 2013 18th European Conference on Network and Optical Communications*, no. 1, pp. 11–18, 2013.

[12] Tomas Horvath, Lukas Malina, and Petr Munster. On security in gigabit passive optical networks, *2015 International Workshop on Fiber Optics in Access Network (FOAN)*, no. 1, pp. 51–55, 2015.

[13] Lukas Malina, Petr Munster, Jan Hajny, and Tomas Horvath. Towards Secure Gigabit Passive Optical Networks, *International Conference on Security and Cryptography*, no. 1, pp. 349–354, 2015.

[14] Lukas Koci, Tomas Horvath, Petr Munster, Michal Jurcik, and Miloslav Filka. Transmission Convergence Layer in XG-PON, *2015 38th International Conference on Telecommunications and Signal Processing (TSP)*, no. 1, 2015.

[15] Tomas Horvath, Petr Munster, Michal Jurcik, Lukas Koci, and Miloslav Filka. Timing measurement and simulation of the activation process in gigabit passive optical networks, *Optica Applicata*, vol. 45, no. 4, pp. 459–471, 2015.

[16] International Telecommunication Union. *G.984.3 : Gigabit-capable passive optical networks (G-PON): Transmission convergence layer specification*. 2014. 2015-08-23.

[17] Xiaoling Xu, Guochu Shou, Zhigang Guo, and Yihong Hu. Encryption method of next generation PON system, *2010 3rd IEEE International Conference on Broadband Network and Multimedia Technology (IC-BNMT)*, no. 1, pp. 384–387, 2010.

Tomas Horvath (MSc) was born in Havirov, Czech Republic on March 7, 1989. He received his MSc. degrees in Telecommunications from the Brno University of Technology, Brno, in 2013. His research interests include passive optical networks (xPON), optoelectronics, and BitTorrent protocol. Currently, he has been actually post graduate student at Brno University of Technology, Department of Telecommunications and his topic of dissertation thesis is Optimization services in FTTx optical access networks.

Petr Munster (MSc, Ph.D.) was born in 1984, in Zlin (Czech Republic). He received his PhD at the Brno University of Technology, Department of Telecommunications in 2014 on the thesis entitled Parameters of the FTTx networks. His current research themes focus on fiber-optic sensors, especially distributed fiber-optic sensors, and also on fiber-optic telecommunications. He has about 50 scientific publications in journals and conferences in last 5 years.

Miloslav Filka (prof.) was born in 1946 in Brno, Czech Republic. Since 2010 he is a professor at the Department of Telecommunications at Brno University of Technology. Hi is a leader of the optical group OptoLab and also head of the Laboratory of transmission media and optical networks. He is a member of a several institutes (e.g. Institute of Electrical & Electronics Engineeres) and is also committee of many conferences (International Conference Telecommunications and Signal Processing, International Conference New Information and Multimedia Technologies). His current research themes focus on fiber-optic telecommunications, especially FTTx technologies.