Towards Secure Gigabit Passive Optical Networks
Signal Propagation based Key Establishment

Lukas Malina, Petr Munster, Jan Hajny and Tomas Horvath
Department of Telecommunications, Brno University of Technology, Technicka 12, Brno, Czech Republic

Keywords: Communication, Cryptography, Gigabit Passive Optical Networks, Key Establishment, Security.

Abstract: Nowadays, the Passive Optical Networks (PONs) technology is widely deployed in broadband access networks. This paper deals with the security issues of Gigabit PON (GPON) standardized by the International Telecommunications Union (ITU), namely, standard ITU-T G.984 that is widely implemented in Europe these days. We describe and analyze the security of this standard and show its security risks. In spite of that transmitted data are encrypted to provide their confidentiality on a multipoint fibre connection, session secret keys during their establishment can be observed by adversaries. To address this security flaw, we propose a key establishment protocol that securely sets the session secret keys between two communication parties in GPON. Furthermore, we provide the security analysis of the proposed protocol.

1 INTRODUCTION

Passive Optical Network (PON) is the main technology for new and current access networks. In general, passive optical networks are widely used due to the absence of the active elements in Optical Distribution Network (ODN). Internet Services Provider (ISP) does not need to have access to all subscriber networks called the last mile. The subscribers (users) use end units called Optical Network Units (ONUs). On the other hand, the provider manages Optical Line Termination (OLT).

Nowadays, there are many standards of PON. In general, these standards are divided into two parts: the ITU and the Institute of Electrical and Electronics Engineers (IEEE) standards. The standards of IEEE dominate in Chinese and Asian access networks, and the ITU standards dominate in the European access networks. Because the gigabit passive optical network technology is widely implemented in European networks, we deal especially with the security of the GPON technology.

Passive optical networks usually provide standard security methods for data encryption, authentication and key establishment. The encryption of data is voluntary in these networks. Nevertheless, the most notable security threat is that all end units (ONUs) are able to read traffic which is broadcasted in downstream. Before data encryption, ONUs receive the broadcast communication and capture the messages in setup stages. Moreover, secret keys for encryption are sent as plain texts in the ITU-T G.984 standard. Therefore, adversaries are able to decrypt communication if they observed these secret keys.

In this paper, we describe and analyze the security of gigabit passive optical networks. We focus on the ITU-T G.984 standard (ITU, 2014). We outline the security threats in GPON and the flaws of key establishment employed in this standard. Further, we propose a novel key establishment protocol to address the security flaws of the standard. Our secure key establishment approach protects against eavesdroppers in the upstream and downstream communication. Our solution enhances security in gigabit passive optical networks.

1.1 State of the Art

Since 1995, many standards of passive optical networks have been developed. In GPON, the downstream direction is transfered via broadcast which causes that ONU units are able to read whole traffic. There are many works which deal with general security issues in the passive optical networks, the downstream direction especially.

The authors (Drakulic et al., 2012) explore the detection algorithms for an attacker in the PON networks. They use a Frame Error Rate (FER) parameter for each ONU unit. They do not use any provision system but only detection algorithms. They

Malina L., Munster P., Hajny J. and Horvath T..
Towards Secure Gigabit Passive Optical Networks - Signal Propagation based Key Establishment.
DOI: 10.5220/0005559903490354
In *Proceedings of the 12th International Conference on Security and Cryptography* (SECRYPT-2015), pages 349-354
ISBN: 978-989-758-117-5

firstly described the weakness of transmission data in the downstream direction. The work (Froehlich et al., 2005) employs a patented Optical Tapped Delay Line (OTDL) channelizer. This technology is able to channelize an information-carrying light into many narrow spectral subbands and change a phase of each of them. OTDL can be used in fibre and free-space optical communication transmission systems. They present the option of using these systems for Wavelength-Division Multiplexing (WDM) systems but do not show how the management changes the key for a separate wavelength in real time applications. Further, the paper (Kochman and Wornell, 2012) introduces the key distribution in free-space optical communication. The authors incorporate Pulse-Position Modulation (PPM) over multiple spatial degrees of free spaces. They use the quantum key distribution model to establish a key in a quantum channel and a classical channel. The work (Martinez-Mateo et al., 2014) deals with the quantum key distribution in passive optical networks. The authors present how to implement the quantum cryptography into the standard access optical networks. They present a solution for Time Division Multiplexing (TDM) based PON. For example, in TDM-Based PON with 128 ONUs, a quantum emitter (and a receiver) has to be connected to one port of an optical splitter. In general, current networks are combination of TDM and WDM networks.

The papers (Hajduczenia et al., 2007), (Mendonca et al., 2012) and (Xu et al., 2010) introduce the security issues in passive optical networks and the encryption method of next generation PON systems. In the paper (Hajduczenia et al., 2007), the security issues of Ethernet PON (EPON) are discussed. On the other hand, the article describes security issues and attacks in EPON networks: eavesdropping, denial-of-Service, masquerading and theft-of-service. The paper (Mendonca et al., 2012) introduces security issues which address reflection. In general, the authors describe dividing the signal in the optical splitter and the measurement of reflection in a PON physical medium. The knowledge of the frame structure and a sensitive detector are required for the detection of transmitted data.

The authors (Eun and Kwon, 2006) analyze the design of key security in EPON. They use a pseudo random function for generating keys. The output of the function is a 160 bit random. Their solution needs some requests of ONU and OLT to change a key. In EPON and all others PON networks, downstream is transferred as broadcast, which means that all nodes receive the whole signal. Only ONU with the same ONU-ID can decode the frame. On the other hand, the EPON networks use the well-known structure of the frame. Optical traffic analyzer enables to read the parameters of the network (source and destination addresses, lengths, types, timestamps, data etc.).

The article (Xu et al., 2010) deals with high speed encryption methods for next generation PON systems. The designed method is divided into 3 parts: key generation, key synchronization and key exchange. Secret encryption keys are sent from ONUs to OLT to prevent other ONUs from eavesdropping these keys. Nevertheless, the authors do not describe the first communication states between OLT and ONU units. In these states, the first key establishment is realized. Further, the possibility of upstream eavesdropping has not been considered in the paper.

In GPON networks, the frames have the complicated structure, i.e., many encapsulations with variable lengths of parts. Nevertheless, ONUs are able to listen the downstream communication in PONs and GPONs. Further, we assume the presence of an adversary who is able to listen both directions and read data from ONUs, including keys that are sent in upstream like in (Xu et al., 2010). Due to this fact, we deal with more robust key establishment. The goal of this paper is to provide secure GPON systems by a proposed secure key establishment protocol and data encryption.

1.2 Our Contributions

The contributions of this paper are summarized in the following text:

1. We analyze security in gigabit passive optical networks and emphasize some security flaws of the ITU-T G.984 standard (ITU, 2014) that occur during the establishment of the session secret keys.
2. We propose a novel key establishment protocol which is based on secure assumptions and uses the signal propagation measurement to establish a common value between two communication nodes. The propagation value between certain ONU and OLT serves as a weak password and an identifier and protects against impersonating attacks. Our key establishment protocol protects against passive adversaries.

2 SECURITY IN GIGABIT PASSIVE OPTICAL NETWORKS

The communication units (OLT and ONU) need to be synchronized in the downstream direction (from an OLT view). The synchronization process starts in the first state called Initial state (O1). ONU asserts LOS

(Loss of Signal) and LOF (Loss of Frame) with 1 for both parameters. Once downstream traffic is received, the parameters LOS and LOF are set to 0. The OLT unit needs to calculate a fibre distance for each connecting ONU. We can calculate the fibre distance by the following equation (ITU, 2014):

$$FD_i = (RTD_i - RT_i) \cdot 102, \quad (1)$$

where FD_i represents the fibre distance between OLT and ONU, RTD_i means the round-trip delay in μs measured by OLT, RT_i is the response time of the ONU unit, and constant value 102 m/μs represents the refractive indices for G.652 fibers.

Synchronization frames (3 messages with the Psync part) are received by ONU, and then ONU moves to the Standby state (O2). ONU waits for the global parameters (a delimiter value, a power level mode and a pre-assigned delay). The description of these parameters is out of the scope of this article. When ONU gets from OLT the global parameters and then ONU moves to the Serial Number state (O3). The O3 state is the most important for the ONU unit because the unit receives the unique identifier ONU-ID with the Assign ONU-ID message. Then, the ONU unit changes the state to the Ranging state (O4). In this state, ONU still cannot send the user data to the network because it must be synchronized with the GTC (GPON Transmission Convergence) frame. It is necessary to change a pre-assigned delay with an equalization delay. The equalization delay is measured from the first entering into this state. The control unit (OLT) can calculate the time of the equalization delay by the following equation (ITU, 2014):

$$\begin{aligned} Teqd &= T_{1490,i} + RspTime_i + EqD_i + T_{1310,i} \\ &= T_{1490,i}\frac{n_{1310}+n_{1490}}{n_{1490}} + RspTime_i + EqD_i, \end{aligned} \quad (2)$$

where $RspTime_i$ is the response time (μs), EqD_i is an estimation of the equalization delay for fibre distance from the previous formula, n_{1310} represents the group velocity refractive index for 1310 nm in ODN (Optical Distribution Network), n_{1490} represents the group velocity refractive index for 1490 nm in the ODN. The fraction with group velocities can be called as the index correction factor. It can be expressed as:

$$T_{1490,i} = (Teqd - RspTime_i - EqD_i)\frac{n_{1490}}{n_{1310}+n_{1490}}. \quad (3)$$

By substituting the expression for the receive instance of the GTC frame N, we obtain:

$$Trecv_{N,i} = Tsend_{N,i} + T_{1490,i}. \quad (4)$$

The final formula is:

$$\begin{aligned} Trecv_{N,i} &= Tsend_N + Teqd\left[\frac{n_{1490}}{n_{1310}+n_{1490}}\right]_{OLT} \\ &-(EqD_i + RspTime_i)\left[\frac{n_{1490}}{n_{1310}+n_{1490}}\right]_{ONU}. \end{aligned} \quad (5)$$

ONU knows the propagation delay values and moves to the Operation state (O5). The O5 state is the final state for ONU which wants to communicate with OLT and transmits user data. On the other hand, the OLT unit can offer encryption in the O5 state. In default setting, data encryption is disabled but ISP can allow the encryption. Data encryption between OLT and ONU units requires a key exchange protocol.

OLT must send the key change request to end unit/s (ONU/s). After ONU receives the key change request, ONU confirms the request and generates the key. The generated key is transmitted back to the OLT unit in the Physical Layer Operations, Administrations, and Maintenance (PLOAM) messages. The length of the PLOAM message is limited. That is the reason why the generated key is sent to OLT in two messages in the GTC frame. These two messages are sent three times in the PLOAM part. OLT must receive each copy of the key in the PLOAM message. If OLT does not receive all copies, it generates a new key change request. After receiving the new key, OLT starts the key exchange (replacing the old key with the new one). After replacing the old key, OLT notifies ONU with the command which contains the frame number and the new key. This command is sent three times. ONU needs to receive each copy of the command for the using this new key. The complete process of this key exchange is depicted in Figure 1.

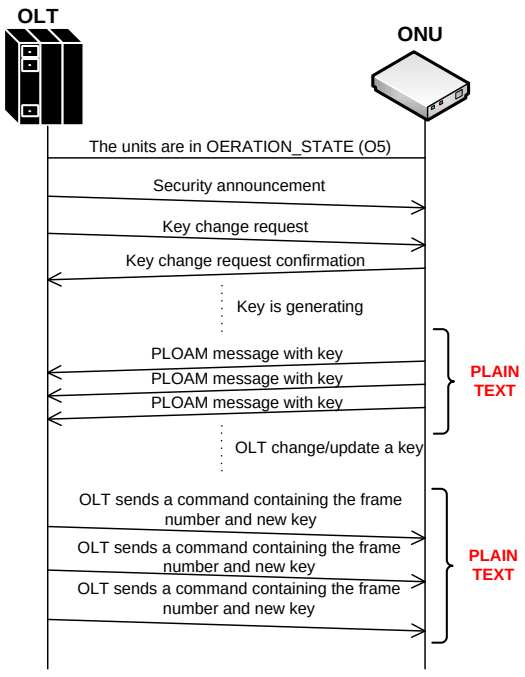

Figure 1: The messages between OLT and ONU during the key exchange process.

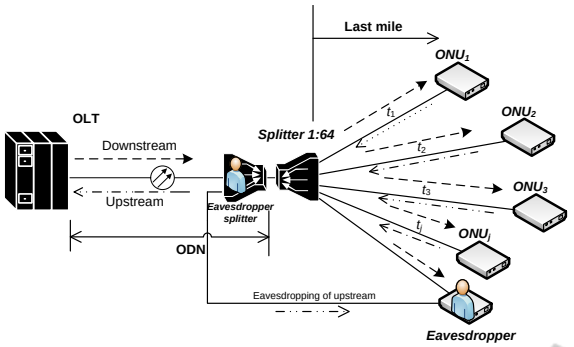

Figure 2: GPON scheme with eavesdropper.

In general, the final version of the ITU-T standard (ITU, 2014) presents that a new key is sent as a plain text in the PLOAM message due to the upstream direction is not easy to capture. Nowadays, adversaries are able to connect the splitter of the upstream channel to split the signal from ONU. OLT detects that the line is down for a certain time and decreases the optical power for ONU that is under the attack. This scenario is not easy to realize in practice but we have to assume that an adversary is able to do it. On the other hand, the scenario is different for the downstream direction. The downstream data are transmitted via broadcast. In other words, each ONU is able to read the downstream direction. Thus, an adversary can analyze commands and PLOAM messages and can try to decrypt data because OLT sends the command in the final state with the number of the frame and the secret key three times in the plain text. The standard ITU-T G.984 (ITU, 2014) too much relies on the character of passive optical networks where eavesdropping is hard to realize. The main security risk of PON is the presence of the splitter. If the attacker is able to connect on a free port of the splitter then he/she can capture transmitted data. In worse case, the attacker is able to connect another splitter and gets the upstream transmission. Upstream eavesdropping is studied in the paper (Gutierrez et al., 2007). The scenario of GPON with an eavesdropper is shown in Figure 2. Due to using the splitter, the attacker can read both direction and get the keys that are sent in plain texts. Therefore, this security flaw must be addressed and more secure key establishment approach must be employed into current passive optical networks.

3 OUR NOVEL KEY ESTABLISHMENT PROTOCOL

In this section, we describe our novel key establishment approach in gigabit passive optical networks. Our proposed protocol runs after the authentication protocol in the Operation state (O5) and substitutes the current and insecure key exchange described in ITU-T G.984 (ITU, 2014).

The proposed protocol is based on the Diffie-Hellman key establishment protocol that is modified to a SPEKE (Simple Password Exponential Key Exchange) approach (Hao and Shahandashti, 2014). Nevertheless, we do not use a generator g that is created from a hash of a password like in the IEEE P1363.2 and the ISO/IEC 11770-4 standards. The common unique value T_{prop} between two communication sides is based on a propagation value which is measured between ONU$_i$ and OLT nodes before the key establishment protocol. The signal propagation value is measured by ONU$_i$ and OLT on the transmission convergence (TC) layer. There is a small probability that the T_{prop} might be a little different on both sides (ONU$_i$ and OLT). Therefore, the measurement is confirmed by ONU$_i$ that sends the HMAC value of T_{prop}, an actual time and the authentication credential of ONU$_i$ to prevent a guessing attack. The measurement of T_{prop} can be repeated to get the equal value on both sides. In our protocol, the T_{prop} value protects against the impersonating attack due to that the value is unique only for the certain pair of ONU$_i$ and OLT. The protocol is depicted in Figure 3. The key establishment protocol runs between the ONU$_i$ unit and the OLT unit in two rounds (two messages) and is described in the following text:

- We assume that the DH public parameters (g, p, q) are securely shared among ONU$_i$ and OLT. Further, the unique value T_{prop} is equal at both sides (ONU$_i$, OLT) that establish a session key (K_s).
- ONU$_i$ generates a random secret value $x \in (1,\ q-1)$ and computes public DH parameter $M = g^x$. Then, the identity of ONU$_i$ (ID_ONU_i) and M are sent to OLT.
- OLT receives ID_ONU_i and M. OLT firstly checks if ID_ONU_i is in a list of ONUs. If ID_ONU_i is found, then stored parameter T_{prop} is loaded. OLT generates a random secret value $y \in (1,\ q-1)$ and computes public DH parameter $N = g^y$. Then, OLT computes the session key K_s = H(ID_ONU_i, min (N,M), max(N,M), M^y, T_{prop}) where H is a secure hash function (e.g. SHA2). The session key is securely stored in OLT. Moreover, OLT computes a key confirmation value KC = HMAC(K_s,'check session key'$||T_{prop}||$ ID_ONU_i). OLT sends ID_ONU_i, N and KC to ONUs in broadcast channel.
- ONU$_i$ receives ID_ONU_i, N and KC by broadcast. ONU$_i$ firstly checks if ID_ONU_i is its

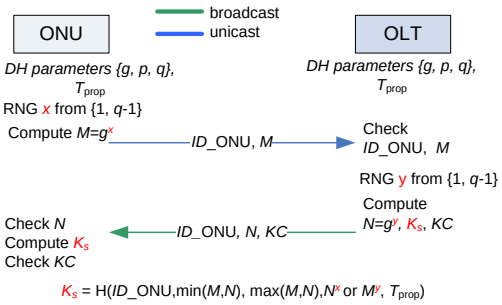

Figure 3: Proposed key establishment protocol.

own. Then, ONU$_i$ computes the session key K_s = H(ID_ONU$_i$, min (N,M), max(N,M), N^x, T_{prop}) and checks incoming KC by recomputing the HMAC(K_s,'check session key'$||T_{prop}||$$ID$_ONU$_i$) where HMAC is a secure keyed-hash message authentication code function (e.g. HMAC-SHA256). If recomputed KC is equal then ONU$_i$ and OLT can start encrypted communication using the established session key K_s. Otherwise, the secret key is discarded.

4 SECURITY ANALYSIS

In this short paper, we provide the informal security analysis of our key establishment protocol. We assume that an attacker has access to the communication and is able to eavesdrop messages in both directions (upstream and downstream). Furthermore, we assume that attackers do not have computational power which allows them to break current cryptographic assumptions that are considered to be secure. Due to the optical network environment and high communication speeds, we assume that attackers are not able to realize man in the middle attacks on the physical layer. Then, we assume that attackers do not have physical access to ONUs and OLT. The goal of the attacker is get the secret key and then decrypt transmitted data. Also, we consider malicious ONU which wants to impersonate another ONU to get its data. This adversary is able to resend, modify and create new messages. In the following subsections, we describe how our protocol protects against possible attacks and adversaries.

4.1 Protocol Protects against Eavesdroppers

An attacker, who eavesdrops on the communication between ONU and OLT during our protocol, is not able to get the secret key. The attacker needs to know secret x or y and T_{prop} in order to compute the valid secret key. The attacker has to solve the Diffie-Hellman problem and must know a valid T_{prop} value to get the secret key. Further, the attacker is not able to get the secret key from cipher texts while he/she is eavesdropping on the encrypted communication. The security of the secret key is based on the security of a symmetric cipher used (e.g. AES).

4.2 Protocol Protects against Impersonating ONU

An attacker (e.g. malicious ONU$_x$) who tries to impersonate another ONU$_i$ with ID_ONU$_i$ has to know the valid signal propagation value T_{prop} of ID_ONU$_i$ to compute the secret session key. Nevertheless, we assume that this value is unique and secret for each pair of ONU$_i$ and OLT. The value is measured and stored after valid authentication of ONU and before every key establishment. The attacker without T_{prop} is not able to compute the same secret key K_s such as OLT. Further, the attacker who gets T_{prop} is not able to compute the previous secret keys of ONU$_i$ and read ONU$_i$'s data because the attacker does not have the secret DH parameter (x) that is needed for the computation of the secret key.

4.3 Protocol Protects against Replay Attack

If an attacker captures the protocol message which is sent from ONU$_i$ to OLT then he/she can try to replay this message to get the secret key. OLT responses with the protocol message that contains new and different parameters, the DH parameter N' and the KC' parameter. The attacker is not able to compute the secret key with these parameters and without the knowledge of x and T_{prop}.

4.4 Protocol Protects against Forgery and Modification Attacks

If messages in the protocol are tampered by an attacker during their transmission then the key confirmation KC parameter is not equal on ONU$_i$ and OLT sides and ONU$_i$ does not use the established secret key. The modification of KC without the knowledge of x or y and T_{prop} is hard if the used HMAC function is secure.

4.5 Protocol Protects against On-line Dictionary Attack

If an attacker tries to guess T_{prop} by running the key establishment protocol then he/she sends messages and get the responses with *KC*. Nevertheless, *KC* parameters from OLT are computed from the secret keys derived from random secret values (y). Thus, the attacker has only one attempt per one protocol run to try guess T_{prop}.

4.6 Protocol Protects against Off-line Dictionary Attack

If an attacker captures the protocol messages then he/she attempts to guess T_{prop} by recomputing *KC*. Nevertheless, *KC* is computed by using the secret key which is derived from the random secret value (y). The attacker is not able to recompute *KC* without y.

4.7 Protocol Protects against Weak Password Leakage

In case that an attacker knows the value T_{prop} that represents a weak password in the protocol then the attacker is not able to compute the secret keys that are already used without knowing a secret value x or y. To obtain these secrets from messages transmitted in the key establishment protocol, the attacker must be able to break the discrete logarithm problem or perform the man in the middle attack that is hard to realize in GPON.

5 CONCLUSIONS

In this paper, we analyze the security of gigabit passive optical networks. Due to the possibility of eavesdropping in downstream and upstream directions, the more secure key establishment protocols are needed. We propose the key establishment protocol that is based on Diffie-Hellman key exchange and the signal propagation time value. Our protocol provides the secure key establishment between ONUs and OLT. The protocol protects against various attacks and eavesdroppers in GPON.

In future work, we would like to implement our solution into real GPON devices and get experimental results about the performance of the proposed protocol.

ACKNOWLEDGEMENTS

Research described in this paper was financed by the National Sustainability Program under grant LO1401, by the Czech Science Foundation under grant no. 14-25298P and the Technology Agency of the Czech Republic project TA0301081. For the research, infrastructure of the SIX Center was used.

REFERENCES

Drakulic, S., Tornatore, M., and Verticale, G. (2012). Degradation attacks on passive optical networks. *2012 16th International Conference on Optical Network Design and Modelling (ONDM)*, pages 1–6.

Eun, J.-S. and Kwon, Y. (2006). The design of key security in ethernet pon. *2006 8th International Conference Advanced Communication Technology*, vol. 1(1):1026–1030.

Froehlich, F., Price, C., Turpin, T., and Cooke, J. (2005). All-optical encryption for links at 10 gbps and above. *MILCOM 2005 - 2005 IEEE Military Communications Conference*, pages 1–7.

Gutierrez, D., Cho, J., and Kazovsky, L. G. (2007). Tdm-pon security issues: upstream encryption is needed. In *Optical Fiber Communication Conference*, page JWA83. Optical Society of America.

Hajduczenia, M., Inacio, P. M., Silva, H. D., Freire, M., and Monteiro, P. (2007). On epon security issues. *IEEE Communications Surveys*, vol. 9(issue 1):68–83.

Hao, F. and Shahandashti, S. F. (2014). *The SPEKE Protocol Revisited.* Springer.

ITU (2014). G.984.3 : Gigabit-capable passive optical networks (g-pon): Transmission convergence layer specification.

Kochman, Y. and Wornell, G. W. (2012). On high-efficiency optical communication and key distribution. *2012 Information Theory and Applications Workshop*, vol. 1(1):172–179.

Martinez-Mateo, J., Ciurana, A., and Martin, V. (2014). Quantum key distribution based on selective post-processing in passive optical networks. *IEEE Photonics Technology Letters*, vol. 26(issue 9):881–884.

Mendonca, C., Lima, M., and Teixeira, A. (2012). Security issues due to reflection in pon physical medium. *2012 14th International Conference on Transparent Optical Networks (ICTON)*, vol. 1(1):1–4.

Xu, X., Shou, G., Guo, Z., and Hu, Y. (2010). Encryption method of next generation pon system. *2010 3rd IEEE International Conference on Broadband Network and Multimedia Technology (IC-BNMT)*, vol. 1(1):384–387.