Optik 127 (2016) 6715–6725

Contents lists available at ScienceDirect

Optik

journal homepage: www.elsevier.de/ijleo

Original research article

Security solution with signal propagation measurement for Gigabit Passive Optical Networks

Lukas Malina*, Tomas Horvath, Petr Munster, Jan Hajny

Department of Telecommunications, Brno University of Technology, Technicka 12, Brno 61600, Czech Republic

ARTICLE INFO

Article history:
Received 2 December 2015
Received in revised form 12 April 2016
Accepted 16 April 2016

Keywords:
Authentication
Communication
Cryptography
Gigabit Passive Optical Networks
Key establishment
Security

ABSTRACT

The paper deals with the security of Gigabit Passive Optical Networks (GPON) and presents a novel robust security solution. The solution provides secure mutual authentication and key establishment between the Optical Line Termination (OLT) unit and end units (ONUs) in Optical Distribution Network (ODN) defined by the ITU-T G.984 standard series. The authentication and key establishment are based on modern cryptographic methods. The cryptographic parameters are transported by the PLOAM (Physical Layer Operations, Administration and Maintenance) messages to get better integration into the ITU-T G.984 standard. Moreover, the solution uses signal propagation values that characterize the connection between the pairs of OLT and ONU. The signal propagation values provide more secure mutual authentication. Our solution is implemented and tested to get performance results that show its efficiency.

1. Introduction

Nowadays, Gigabit Passive Optical Networks (GPONs) are widely used for the access networks in Europe. GPON is the first of the Passive Optical Network (PON) specification that provides the bidirectional communication speed above 1 Gb/s. GPON is defined by the ITU-T G.984 standard series. GPON basic working principle and its limitations are described in [1,2]. Because PONs do not require active elements, this technology is widely used in Optical Distribution Network (ODN). PONs usually consists of OLT (Optical Line Termination), ONUs (Optical Network Units or Optical Network Terminals denoted as ONTs) and ODN (Optical Distribution Network). OLT that is located at the provider's side of the access network is responsible for the setup of all parameters such as power level, frame duration and so on. The end unit (ONU) located at the customer's side provides the conversion from optical to electrical signal and the conversion from GTC frames to Ethernet frames. Generally, Internet Service Providers (ISPs) with OLT do not need to have access to subscriber networks called the last mile. Hence, the subscribers (users) use only ONUs and ISP manages only Optical Line Termination (OLT) nodes. The distribution network employs one or more splitters (POS – Passive Optical Splitter). For example, one splitter divides an optical signal at the provider's part and other splitters are used at the customer's part. The signal is carried into all ports of the splitter and the end unit with the same parameters as in the frame is able to read data. This may lead to serious security threats [2–4].

GPON offers security features such as data encryption, authentication and key establishment. Nevertheless, data encryption is optional. If the data encryption property is not applied then all end units (ONUs) are able to read traffic which is broadcasted in downstream. Further, more serious threat is that ONUs receive broadcast communication and can capture

* Corresponding author. Tel.: +420 541146926.
E-mail address: malina@feec.vutbr.cz (L. Malina).

http://dx.doi.org/10.1016/j.ijleo.2016.04.069
0030-4026/

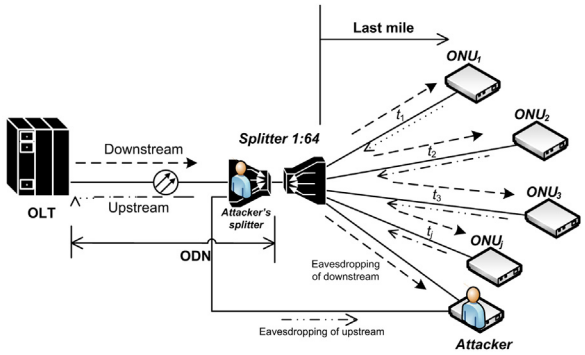

Fig. 1. Scenario with an attacker in GPON.

the messages used in setup stages when secret session keys are established. In the ITU-T G.984 standard, the secret session keys are sent as plain texts in the PLOAM (Physical Layer Operations, Administration and Maintenance) messages. Therefore, adversaries are able to decrypt data communication if they observed these keys. Fig. 1 presents the scenario with an attacker who is able to eavesdrop on communication in both directions due to the splitter and insufficient security protection provided in GPON defined by ITU-T G.984.

In this paper, we propose a novel robust security solution for GPONs defined under the ITU-T G.984 standard [5]. The solution provides the mutual authentication of GPON's parties (ONUs and OLT), secure key establishment and secure data communication in both directions. The goal of our work is to enhance the security level of Gigabit Passive Optical Networks.

The paper is structured as follows: Section 2 discusses the related work in passive optical networks and the contribution of this work. Section 3 describes theory background and cryptography used in our security solution. Section 4 outlines our proposed solution and the main phases. Section 5 includes the security analysis of the solution and Section 6 presents the performance evaluation and the results. The last section presents our conclusions.

2. Related work

There are several papers that deal with the security of passive optical networks (PONs), Ethernet PON but only few papers deal with the security of GPON and 10 G-EPON.

The security of PONs is investigated by Drakulic et al. [6]. They use the detection algorithms that work with a Frame Error Rate (FER) parameter for each ONU unit in order to reveal an attacker. They mentioned the weakness of transmission data in the downstream direction. Other papers [3,7–9] describe more security issues in passive optical networks and the encryption method of next generation PON systems. For example, the work [7] describes the security issues of Ethernet PON (EPON) such as: eavesdropping, denial-of-Service, masquerading and theft-of-service. The work [8] 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. Further, the work [10] describes the ONU and user authentication process in EPON (Ethernet PON). The EPON standard is defined by IEEE (Institute of Electrical and Electronics Engineers), e.g. IEEE 802.3ah, and the EPONs dominate especially in Asia. Nevertheless in our work, we deal with the security in GPONs which are defined by the family of recommendations ITU-T G.984.

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. 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 [9]. The paper [9] 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 session 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.

Some papers offer security solutions for various types of passive optical networks. Kazovsky et al. [4] present the possibilities of attacks: eavesdropping, DOS (Denial of Service), masquerade (spoofing attacks) and replay attacks and propose a countermeasure with active switching and passive fuse for TDM-PON (Time Division Multiplex PON). The work [11] deals with the quantum key distribution in passive optical networks. The authors present an implementation of the quantum cryptography into the Ethernet access optical networks with FBG (Fiber Bragg Grating) in downstream. Further, the paper [12] employs a patented Optical Tapped Delay Line (OTDL) channelizer. They combine an information-carrying light into many narrow spectral bands. Each band has a different phase in comparison with the previous sample. OTDL can be used in all optical networks (fiber and free space optical communication). On the other hand, they do not present how OLT change key via PLOAM (Physical Layer Operations, Administration and Maintenance) messages.