Security Challenges and Solutions for Telemedicine over EPON

Ying Yan and Lars Dittmann
Department of Photonics Engineering, Technical University of Denmark
Kgs. Lyngby, Denmark
{yiya, ladit}@fotonik.dtu.dk

Abstract— **Keeping data integrity and privacy is a major design concern for telemedicine applications, where sensitive and personal information are collected and disseminated over telecommunication system. For this reason, this study discusses the network characteristics and security issues in the Ethernet Passive Optical Network (EPON), which is responsible for conveying traffic between the hospital or healthcare centers and patients. Subsequently, different types of security challenges are classified and a survey of solutions is presented. The purpose of this research is to highlight the security issues in EPON system as a transmission method of telemedicine services and any person will be aware of the potential attacks during data transmission.**

Keywords-security challenges; EPON; telemedicine.

I. INTRODUCTION

Security issue is a primary concern for the telemedicine application, where confidential data are exchanged between healthcare providers and patients. A telemedicine communication system consists of three principal divisions: a hospital service/data center, a transmission and distribution system, and patient home environment. The hospital service/data center provides medical instructions and assignments to individual patient, meanwhile it stores patient personal information and medical records/documents in the data center. The transmission and distribution system connects the hospital and the patient at home and exchanges data (such as messages, files, videos, and so on). Telemedicine applications and devices are used by patients at their homes, so that they can remotely communicate with doctors and get correct and necessary medical advices. This work studies the usage of optical access network for the telemedicine communication system for data transmitting and distributing.

Delivering data over optical fiber links becomes the most prominent way in the access networks. Presently, the Fiber to the Home (FTTH) are being deployed to the subscriber by a strong worldwide push: in United States, the annual growth rate was 112% during September 2006 to September 2007 and in Denmark, the FTTH subscribers increased 90% in year 2008 [1] [2]. The cost effective Ethernet Passive Optical Networks (EPON) with point-to-multipoint architecture is the prevalent solution to FTTH. The typical EPON system is a tree structure consisting of an Optical Line Terminal (OLT) located at a central office, a *1:N* splitter, and multiple Optical Network Units (ONUs) at the end users' premises.

The telemedicine communication system relies primarily on health information security and confidentiality. Many countries have legislations with appropriate confidentiality policies, individual identification procedures and practices, so that information access is strictly limited to authorized person with the consent of the patient [3]. In order to design a completely secure telemedicine system, security must be integrated into every node and each element is responsible for ensuring information security. This dictates that data security is related to the entire communication system.

Currently, various research projects begin to investigate the potential security risks on different aspects in the telemedicine system in order to minimize the consequential impacts on the privacy of the whole system and patient personal information. The telemedicine communication system contains different kinds of hardware equipments, software applications and transmission mediums. Therefore, the security and privacy issues are identified and discussed from different aspects. At the software level, Baker and Wallace [4] explore the risks of hacking in software and computer systems and tempering user database, where data can be stolen or altered. At the network level, two network technologies, Ethernet and mobile network, have been studied and discussed regarding to the security aspect, respectively Kiravuo et al. in [5] and Boukerche and Ren [6]. In [7], besides the manmade events, Carvalho and De Souza worked on network resilience and path protection in order to reduce the risks caused by natural effects or earthquake.

This paper focuses on the security issues in the stage of data transmission and distribution. On the basis of EPON, it is vitally important to ensure that any data transmitted over optical channel, for example, medical history of a patient, cannot be leaked out and used to identify a person.

The rest of this paper is organized as follows. In section II, we first describe the basic architecture and operation processes of EPON. We present the security challenges in EPON and give a survey on proposed solutions in section III and section IV, respectively.

II. EPON SYSTEM

In an EPON system, one OLT is functionalized as an administrator connecting multiple ONUs in the subscribers' locations. IEEE 802.3ah Task Force [8] specifies the physical layer and MAC layer characteristics of EPON.

As shown in Figure 1, we consider an EPON system consisting of *K* ONUs that connect to a central control station, OLT, via the optical link. In the downstream direction from the OLT to the associated ONUs, data are broadcasted to each ONU in a point-to-multipoint architecture. On the other hand, it is a multipoint-to-point architecture in the upstream direction from the ONUs to the OLT.

ISBN: 978-1-61208-327-8

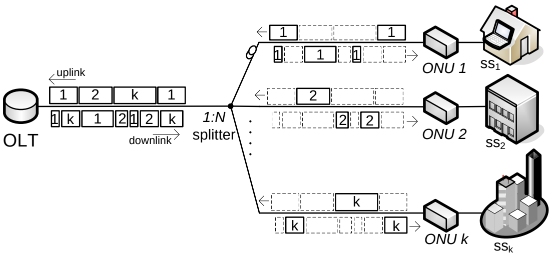

Figure 1. EPON system: upstream (multi-point to point) and downstream (point to multi-point) transmission.

Multiple ONUs share the optical bandwidth with Time Division Multiplexing (TDM) technique [1]. The OLT allocates upstream bandwidth among the ONUs and each ONU transmits packets in dedicated time slots in order to avoid collision. Two processes are performed: the auto-discovery process and the normal process.

- During the discovery process, the OLT searches for ONUs, authenticates and registers attached ONUs, and calculates the Round Trip Time (RTT). After discovering and registering the connected ONUs, the OLT sets up an entry table, which contains the ONU Logic Link Identification (LLID) and RTT values.
- A key perspective of the normal process is the ability to assign bandwidth and schedule transmission for all registered ONUs in a manner of fairness and without conflict. The OLT polls registered ONUs and assigns time slots either statically or dynamically based on the resource requirement negotiation.

III. Security Challenge in EPON

In a communication system for telemedicine applications, security management is applied for keeping the data integrity without being tampered, patient privacy and confidentiality without being released or retrieved, and access control without being unauthorized accessed. In this paper, EPON is used for data transmission for telemedicine service and we study communications security challenges in EPON. EPON have security threats and vulnerabilities that are experienced in the general network. Meanwhile, there are special attacks due to transmission characteristics in EPON, for example, network topology, control protocol, communication equipments as well as network access ports [9][10].

A. Potential Security Risk with EPON Topology

Security depends highly on the configuration of network architecture. Unlike a peer-to-peer network, where a trust between a server and a user is normally existed, EPON system with a point-to-multipoint structure is vulnerable to intruders. In EPON, downstream traffic is broadcasted and upstream bandwidth resources are shared by multiple users. Besides, we cannot assume a fixed topology, because the registration of ONUs is dynamic and an ONU may leave or join the network at any time. The potential threats, eavesdropping and Denial of Service (DoS), are possible occurred due to the point-to-multipoint topology.

- *Eavesdropping*: ONUs can receive all downstream traffic by simply disabling the address/ID filter and freely receiving data destined to other ONUs. Since it is difficult to detect such an attack at OLT, a malicious ONU can eavesdrop traffic without being noticed and interrupted for 24 hours per day.
- *Denial of Service (DoS)*: the upstream bandwidth is distributed among several users. Each ONU needs to transmit in upstream direction by complying with the assigned timeslots. If a misbehaved ONU on purpose transmits outside the schedule, it can consequently cause collision with the ongoing transmission from a legitimate ONU, and even worse, it can block the channel with large amounts of traffic.
- *Theft of Service (ToS)*: ToS is threat that is common to all networks. One malicious subscriber attempts to impersonate another legitimate ONU, by forging all useful ONU information including LLID, MAC address, and so on. Since the LLID is the identity assigned during the registration process and used as a digital signature during the normal process, the malicious subscriber obtains bandwidth without any access cost by a forged LLID.

B. Potential Security Risk with Control Protocol

The Multi-Point Control Protocol (MPCP) as the control and signaling protocol is defined in EPON standard. After the registration process, the OLT communicates and schedules transmission timeslots to ONUs based on their assigned identifications, LLIDs. During the registration process, a potential threat is called *impersonation*.

The malicious user has opportunity to collect information about the target ONU such as its LLID and MAC address and masquerade as a legitimate ONU to use network resources with free charge. Even worse, the attacker can seriously invade other's privacy by forging wrong information and transmitting on behalf of another ONU.

IV. Survey of Solutions for EPON Security

EPON system has unsurpassed advantages in comparison to the data transmission over copper wires or air interfaces. However, protecting the patient's privacy and secure the transmission system becomes an important concern due to its topology. With properly designed security management can reduce the risk of security attacks even though they may not be eliminated. Based on the potential threats and security challenges in EPON, various solutions are proposed to answer specific security requirements.

A. Data Cryptography

Cryptography is the process of hiding the original data in a serial of meaningless scrambled code during transmission. At the receiver node, data is deciphered and converted back into the original information. Due to the point-to-multipoint network topology, eavesdropping is possible in the downstream direction by simply changing a registered ONU configuration into the promiscuous mode. Thus, the downstream data need to be encrypted to safeguard the information.

The data encryption for 1G-EPON is undefined in original 802.3ah-2004 standard [8]. Later in 2008, the YD/T 1771-2008 Technical Requirements for Access Networks - Interoperability of EPON Systems uses the triple churning algorithm [11]. When evolving into 10G-EPON, an advanced encryption method, Galois Counter Mode (GCM) is adopted as described in the IEEE MAC security (MACsec) standard, 802.1AE [12]. GCM provides high security by using 128 bits Advanced Encryption Standard (AES) in counter mode and supports high speed data transmission due to the pipeline architecture of AES [13]. An alternative solution is the multi-byte churning encryption algorithm, which increases the key length in order to improve the security level and can be implemented at fast transmission speed [14].

In order to analyze the alternative encryption algorithms proposed for EPON system, we compare the single / triple churning algorithm and the AES algorithm in terms of speed, complexity and security strength (shown in Table 1). The churning algorithm is used to protect data confidentiality by scrambling function. The single churning algorithm uses a 24-bit key code. The implementation is simple and high speed. Triple churning algorithm is expanded on the basis of single churning algorithm in order to increase the security level. The key length is increased to 48 bits. AES is a symmetric-key encryption algorithm, where the same key is used for both encryption at the transmitter and decryption at the receiver. In EPON standard, GCM uses the AES with a key length of 128 bits. Designed as a pipelined architecture, AES is suitable for high-speed hardware implementation and meets the operation requirement in the10G EPON systems.

TABLE I. COMPARISON OF ENCRYPTION ALGORITHMS IN EPON

	Single Churning	*Triple Churning*	*GCM with AES*
Speed	Fast	Fast	Fast
Security level	Low (14 bits key)	Low (48 bits key)	High (128 bits key)
Implementation Complexity	Low	Low	high

B. Authentication Protocols

An authentication protocol is used to verify an identification of a node as a valid member in the network. Same as date encryption, node authentication is also a main defense again attack. EPON topology is open and dynamic. In the upstream direction, an authorization and authentication mechanism is required to ensure the communication reliability and to avoid the impersonation from illegal masquerading users. A new ONU must be mutually authenticated during the auto-discovery process.

Given various authentication protocols have been proposed [10], ONU authentication and secure provisioning are presented in the latest IEEE 1904.1-2013 standard for Service Interoperability in EPON (SIEPON) [15] [16]. To deal with both legacy 1G-EPON and the next generation 10G-EPON, IEEE 802.1X-2004 and IEEE 802.1X-2010 are defined as ONU authentication mechanisms, respectively. Both two generations are based on Extensible Authentication Protocol (EAP) methods:

- *IEEE 802.1X-2004 and EAP-MD5*: The EAP-MD5, defined in RFC 2284, is known as simple with very light and fast processing. The principle is in a challenge-response principle. The OLT as an authenticator sends an EAP request. The ONU as a supplicant replies with its identification in a response message, which is relayed to an authentication server. The OLT then sends an EAP challenge packet of type MD5 challenge to the ONU. After calculating a MD5 hash based on the challenge, the ONU returns a response containing the hash value. On the server side, the same hash computation is performed and two values are compared. The authentication is success if two hash values are identical, otherwise, the authentication fails.
- *IEEE 802.1X-2010 and EAP-GPSK*: the authentication scheme, EAP Generalized Pre-Shared Key (EAP-GPSK), is an advanced technique to obtain mutual authentication and key agreement between the authenticator and supplicant *[17]*. For the authentication in the 10G-EPON, an OLT starts with an EAP request message containing its identification ID_olt. The applicant ONU responses with its own identification, ID_onu. The OLT sends ID_olt, a random number RAND_server, and a list of supported ciphersuites, CSuite_List. The ONU then requests with ID_onu, a random number, RAND_onu, a repeat of received parameters of the OLT, the selected ciphersuite and a Message Authentication Code (MAC_onu) that is computed based on all the transmitted parameters. The OLT verifies the received MAC_onu code and the consistency of parameters. In case of successful verification, the EAP server computes a MAC_olt over the session parameter and returns it to the peer. The peer verifies the received MAC_olt code, and consistency of parameters. If the verification is successful, ONU replies with a message that can optionally contain the peer's protected data parameters. Then, the OLT sends an EAP Success message to indicate the successful outcome of the authentication. The keys used to compute MAC at the OLT and ONU are both derived from a Key Derivation Function (KDF), which based on a long-term pre-shared key. Both the server OLT and the peer ONU are authenticated by using the MAC key code.

During the authentication process, three types of ONU identification are used: MAC address based, logical ID based and hybrid authentication. The first method uses information provided by ONU during the auto-discovery process. The second method requires a provider defined logical ID, which is manufactured into an ONU device. In the hybrid mode, if the MAC address based authentication fails, the OLT then initiates to the logical ID based authentication [16].

C. Security Enhanced Communication Technologies

PON technology is developed with the aims of increased data rate, increased range, reduced cost and reduced energy consumption. The following technologies improve network performances and profits. Meanwhile they affect the security properties of EPON system in term of involving multiple wavelengths, operating at fast speed, and deploying a different multiplexing method.

- *Wavelength Division Multiplexing (WDM) technology*: The straight way to improve network security is to setup a point-to-point communication between the server and the client. By assigning traffic on links with different wavelengths, the WDM-PON allows the OLT exchange data with each ONU at a unique wavelength.
- *High speed 10G-EPON*: The churning encryption scheme has drawbacks such as short key length and low operation speed. With the upgrading to 10G EPON, GCM is deployed to ensure data security as well as to guarantee the information reliability. By combining Galois field message authentication code (GMAC), the method realizes authentication process and can be used as an incremental MAC [13].
- *Optical Code Division Multiple Access (OCDMA) technology*: While being successfully developed in wireless communication, the OCDMA introduces this concept into fiber optic communication systems, where encoding and decoding operations are performed in optical domain. Advantages of using OCDMA include realizing higher spectral efficiency, providing higher system capacity and enhancing security. In OCDMA-PONs, different users are assigned orthogonal codes, with which each user's data are encoded/decoded with an optical pulse sequence. Thus, this technique provides asynchronous communications and security against unauthorized users [18] [19].

D. Security Enhanced Communication Devices

Using a conventional TDM PON, security enhancement can be introduced to the physical devices, OLT and ONU. In [20], authors demonstrate the physical security enhancement from using a pair of matched tunable lasers in OLT. A unique point-to-point link is created between the OLT and the destination ONU since the tunable laser transmits each frame with a unique identifying code and each ONU is also assigned with a unique wavelength.

E. Security Mechanism in Hybrid Network Topology

A telemedicine communication system is composed of different communication technologies instead of a solo transmission links. EPON is responsible for delivering traffic to the users' premises. The last-mile can be accomplished by using Digital Subscriber Line (DSL) or Wireless Local Area Network (WLAN) technologies. Research about a unified security framework for integrated technologies is ongoing. In [21] [22], authors discuss about the integrated authentication process and data encryption scheme in the combined EPON and wireless networks.

V. Conclusion and Future Work

The major strengths of EPON are its high data rate and low cost. They are also the causes of its prevalence in the access network. Nowadays, security issues for EPON system become a serious concern, particular for transmitting patient medical histories and hospital health records. Concerns are raised about patient privacy and data security due to the broadcast characteristics in EPON. This paper discusses several research efforts, which have been trying to address the security issues in EPON. The challenges are addressed in order to point out the secure weakness caused by EPON structure, protocol and devices. Hence, this work shows that as the transmission channel is vulnerable, potential attacks can be possible to harm the entire telemedicine system. This paper further presents a survey of existing solutions to deal with data confidentiality, authentication, access control and integration with other network technologies. Through our study, we showed different aspects and concerns for a security framework for the telemedicine system over EPON. Future work will consider simulation and result analysis for the discussed solutions.

Acknowledgment

The authors would like to acknowledge the support by the Patient @ Home project - Danish welfare technological research and innovation initiative project [23].

References

[1] M. Maier, "Optical Access-Metro Networks", in "Broadband Access Networks", Springer US, pp. 237-259, 2009. Doi:10.1007/978-0-387-92131-0_11

[2] "Denmark Sees the Light: 90% Increase in the Fibre - to - the - Home Subscribers in the Past Year", Press release, 2009.

[3] B. Fong, A.C. M. Fong, and C.K. Li, "Telemedicine Technologies: Information Technologies in Medicine and telemedicine", Wiley, United Kingdom, pp.137-170, 2011.

[4] W. H. Baker and L. Wallace, "Is Information Security Under Control?: Investigating Quality in Information Security Management", IEEE Security & Privacy, vol 5, iss. 1, pp. 36 – 44, Feb 2007.

[5] T. Kiravuo, M. Sarela, and J. Manner, "A Survey of Ethernet LAN Security", IEEE communications surveys & tutorials, vol. 15, no.34, pp. 1477 – 1491, 2013.

[6] A. Boukerche and Y. Ren, "A Secure Mobile Healthcare System using Trust-Based Multicast Scheme", IEEE Journal on selected areas in communications, vol 27, no. 4, pp. 387 – 399, May 2009.

[7] M. M. Carvalho and E. A. De Souza, "A Novel Protection Mechanism in TDM-PON", 11th International Conference on Transparent Optical Networks (ICTON), pp. 1-4, July 2013.

[8] IEEE 802.3ah Ethernet in the First Mile Task Force.

[9] S. Roh and S. Kim, "Security model and authentication protocol in EPON-based optical access network", 5th International Conference on Transparent Optical Networks (ICTON), pp. 99-102, July 2003.

[10] M. Hajduczenia, P. Inacio, H. Silva, M. Freire, and P. Monteiro, "On EPON Security Issues", IEEE Communications Surveys & Tutorials, pp. 68-83, May 2007.

[11] YD/T 1771-2008, "Technical Requirements for Access Networks – Interoperability of EPON Systems", Mar 2008.

[12] "IEEE 802.1AE – Media Access control (MAC) Security", 2006.

[13] X. Chen, G. Shou, Z. Guo and Y. Hu, "Encryption and Authentication Mechanism of 10G EPON systems Based on GCM", 2nd International Conference on e-Business and Information System Security (EBISS), pp. 1-4, May 2010.

[14] X. Xu, G. Shou, Z. Guo and Y. Hu, "Encryption Method of Next Generation PON systems", 3rd International Conference on Broadband Network and Multimedia Technology (IC-BNMT), pp. 384-387, Oct 2010.

[15] G. Kramer, L. Khermosh, F. Daido, A. Brown, H. Yoon, K. Suzuki, and W. Bo, "The IEEE 1904.1 Standard: SIEPON Architecture and Model", IEEE Communications Magazin, pp. 98-108, September 2012.

[16] "1904.1-2013 - IEEE Standard for Service Interoperability in Ethernet Passive Optical Networks (SIEPON)", September 2013.

[17] T. Clancy, and H. Tschofenig, "Extensible Authentication Protocol - Generalized Pre-Shared Key (EAP-GPSK) Method", RFC 5433, IETF Request for Comments, February 2009

[18] A. Stok and E. H. Sargent, "The Role of Optical CDMA in Access Networks", IEEE Communication Magazine, vol. 40, iss. 9, pp. 83 – 87, 2002

[19] H. A. Bakarman, T. Eltaif, P. S. Menon, M. Muqaibel, and S. Shaari, "Optical Access Network based on OCDMA Systems: Transmission and Security Performance", Journal of Communications , vol. 7, pp. 35-41, 2013.

[20] A. Harris, A. Sierra, S. Kartalopoulos, and J. Sluss, "Security Enhancements in Novel Passive Optical Networks", IEEE International Conference on Communications (ICC), pp. 1399-1403, 2007.

[21] S. Chowdhury and M. Maier, "Security Issues in Integrated EPON and Next Generation WLAN Networks", IEEE Consumer Communications and Networking Conference (CCNC), pp. 1-2, Jan 2010

[22] W. Gu, P. K. Verma and S. V. Kartalopoulos, "A Unified Security Framework for WiMAX over EPON access Networks" Security and Communication Networks, vol 4, iss. 6, pages 685–696, June 2011.

[23] Patient at Home project. Website: http://www.patientathome.dk/