Mutual Authentication Scheme for Lightweight IoT Devices

Seungyong Yoon, Jeongnyeo Kim
Information Security Research Division
Electronics and Telecommunications Research Institute
Daejeon, Rep. of Korea
e-mail: syyoon@etri.re.kr, jnkim@etri.re.kr

***Abstract*— Since the Internet of Things (IoT) network is a resource-limited and heterogeneous interconnection environment, lightweight security technology is required that takes into consideration various environmental features, such as computing power, memory capacity, battery power, and communication bandwidth. In this paper, we analyze the problems of the existing Datagram Transport Layer Security (DTLS) authentication protocol and simplify the handshaking procedure of this authentication process so that it is applicable to lightweight IoT devices with very limited resources.**

Keywords-IoT; security; authentication.

I. INTRODUCTION

The IoT environment is a Low power and Lossy Network (LLN) environment to which it is difficult to apply the existing IP-based security protocol considering the communicational capability. Therefore, a hardened security protocol considering computing power and limited resources is needed. It is necessary to minimize the number and size of transmitted messages and to apply a lightweight cryptographic algorithm, for example, Elliptic Curve Cryptography (ECC) [1] and Lightweight Encryption Algorithm (LEA) [2], without performance degradation. The Internet Engineering Task Force (IETF) classifies resource-constrained IoT devices into three classes [3]. Since class 0 and class 1 devices have a lot of restrictions on Random Access Memory (RAM) and Flash, it is difficult to apply cryptographic modules and messages used in security protocols such as existing DTLS. Therefore, in this paper, we analyze the requirements of DTLS authentication protocol and propose a mutual authentication scheme for lightweight IoT devices to solve it.

II. RELATED WORK

Open Mobile Alliance (OMA) has proposed the Constrained Application Protocol (CoAP) [4] based on the User Datagram Protocol (UDP) and the DTLS in IoT environments. DTLS is proposed as a security protocol that provides data confidentiality, integrity, and authentication function to application services using UDP protocol, but it has many limitations to be applied to lightweight IoT devices. This is described in detail in Section III. Therefore, various lightweight techniques have been studied to overcome the limitations of DTLS [5]-[7].

III. ANALYSIS OF DTLS AUTHENTICATION PROTOCOL

DTLS is a security protocol that provides data confidentiality, integrity, and authentication function to application services using the UDP protocol. It was presented as a protocol that can add security to IoT based on UDP protocol. However, DTLS has the following limitations:

- Due to the complexity of the handshake procedure and the large number of messages transmitted, there is a limit to use on lightweight IoT devices.
- The handshake message of DTLS has fate-sharing characteristic, so if one packet is lost, the entire message must be retransmitted. Retransmission causes increase in throughput and performance degradation.
- Fragmentation - The Maximum Transmission Unit (MTU) size of the 802.15.4 Media Access Control (MAC) layer used in the IoT environment is 127 bytes, which causes performance degradation by transmission delay and reassembly process due to fragmentation in lightweight IoT devices.

IV. THE PROPOSED MUTUAL AUTHENTICATION SCHEME

The mutual authentication scheme for the lightweight IoT devices proposed in this paper has the following characteristics. First, the mutual authentication function is performed between the security management server (shortly, server) and the lightweight IoT device, including the authentication process as well as the session key exchange process used for the encrypted communication channel. Peer-to-peer authentication is out of scope in this paper, for example, between two IoT devices. In the mutual authentication process, the gateway is included in the authentication. The proposed scheme basically begins with assuming that it has a pre-shared secret key between the server and the IoT device or between the server and the gateway. The server stores and manages the identifier (ID) of the IoT device and the gateway, and the pre-shared key in the Database (DB). After the mutual authentication process, the session key exchange used in the encrypted communication channel for data transmission is usually performed. However, the lightweight IoT device having limited computing power or resources does not participate in the session key generation process, both session key generation and key distribution functions are performed on the server. The

 ISBN: 978-1-61208-582-1

proposed scheme reduces the amount of messages transmitted by simplifying the handshaking process for mutual authentication and session key distribution, solving the problems of the DTLS protocol. In addition, it provides an encrypted communication channel by creating and exchanging new session keys each time a new session is established through a lightweight mutual authentication scheme, thereby further enhancing the security of the lightweight IoT device. The lightweight mutual authentication scheme proposed in this paper can be roughly divided into two cases. The first case does not include a gateway. This is the case where mutual authentication is performed directly between the server and the IoT device, and there is no gateway in the IoT network environment. The second case involves a gateway, where the gateway acts as an intermediary between the server and the IoT device and participates in authentication. Table 1 defines the parameters used in the lightweight mutual authentication scheme.

TABLE I. LIGHTWEIGHT MUTUAL AUTHENTICATION PARAMETER

Parameter	Definition
Server	Security management server (Authentication server)
Gateway	IoT gateway
IoT Device	IoT Device
IDd	IoT device identifier
IDg	IoT gateway identifier
Kd	The pre-shared secret key between server and IoT device
Kg	The pre-shared secret key between server and gateway
SK	The session key between server and IoT device
eK()	Symmetric encryption function
dK()	Symmetric decryption function
Rg	Random number generated by gateway
Rd	Random number generated by IoT device
Rs	Random number generated by server
||	Concatenation operation

In this paper, in the case of mutual authentication without a gateway, the authentication procedure is relatively simple. Figure 1 shows the mutual authentication process between the server and the IoT device in this case.

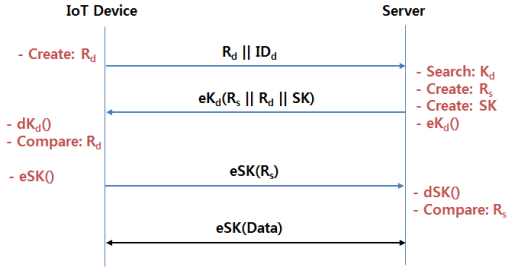

Figure 1. The case of mutual authentication without a gateway.

Figure 2 shows the mutual authentication process between the server and the IoT device including the gateway as an intermediary. When communicating via gateways in an IoT network environment, gateway impersonation attacks are possible, so a gateway authentication must be included to ensure that it is a trusted gateway. The attacker has communication information between the device and the server, and can perform a replay attack on a target after a predetermined time. This attack can be prevented because a new random number is generated and authenticated for every session for communication.

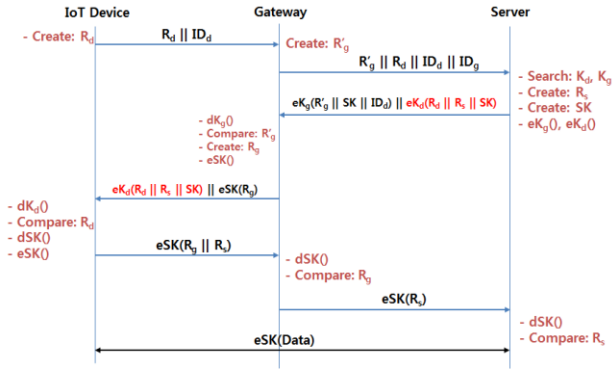

Figure 2. The case of mutual authentication with a gateway.

In addition, since the encrypted communication is performed using the exchanged session key during the authentication process, it is safe even if the attacker makes a spoofing or sniffing attack. Since it is authenticated including the gateway, it is possible to prevent gateway impersonation attack and man-in-the-middle attack.

V. CONCLUSION

In this paper, we propose a mutual authentication scheme that can be used for lightweight IoT devices with high computing power and resource constraints. It simplifies the handshaking process for mutual authentication and reduces the amount of messages transmitted, making it suitable for use in lightweight IoT devices.

ACKNOWLEDGMENT

This work was supported by Institute for Information & communications Technology Promotion (IITP) grant funded by the Korea government (MSIT) (2015-0-00508, Development of Operating System Security Core Technology for the Smart Lightweight IoT Devices).

REFERENCES

[1] V. Miller, “Use of elliptic curves in cryptography”, Proc. LNCS CRYPTO, 1985, pp. 417-426.

[2] D. Hong, et al., “LEA: a 128-bit block cipher for fast encryption on common processors”, Proc. LNCS WISA, Aug. 2013, pp. 3-27.

[3] C. Bormann, M. Ersue, and A. Keranen, “Terminology for Constrained-Node Networks”, IETF, RFC 7228, 2015.

[4] Z. Shelby, K. Hartke, and C. Bormann, “The constrained application protocol (CoAP)”, IETF, RFC 7252, 2014.

[5] R. Hummen, J. Ziegeldorf, H. Shafagh, S. Raza, and K.Wehrle, “Towards viable certificated-based authentication for the Internet of Things”, Proc. ACM HotWiSec, Apr. 2013, pp. 37-42.

[6] S. Raza, D. Trabalza, and T. Voigt, “6LoWPAN compressed DTLS for CoAP”, Proc. IEEE DCOSS, May 2012, pp. 287-289.

[7] S. Raza, et al., “Securing communication in 6LoWPAN with compressed IPsec”, Proc. IEEE DCOSS, Jun. 2011, pp. 1-8.

 ISBN: 978-1-61208-582-1