Advanced Science and Technology Letters
Vol.43 (Multimedia 2013), pp.162-165
http://dx.doi.org/10.14257/astl.2013.43.35

# Designing a Secure Service Manager for Internet of Things

Jiye Park, Namhi Kang[1],
Digital Media Department, Duksung Women's University,
Seoul, Korea
{jiyepark, kang}@duksung.ac.kr

**Abstract.** The Internet of Things (IoT) provide constrained devices in low-power and lossy networks (LLNs) with Internet access. Security is a major concern to deploy various services. DTLS specified by IETF is a candidate protocol to support security services in IoT environment. However, the protocol cannot cover all highly constrained devices. To solve the problem, we design a secure IoT architecture based on the proposed secure service manager (SSM).

**Keywords:** Internet of Things, Web of Things, Security Manager, DTLS

## 1 Introduction

IoT is one of the most highlighted internet technologies to realize various services by using small things such as sensors and actuators. IoT can be applied to many traditional industries. In these areas, many applications are required to support services in a secure fashion. However, limited device resources and LLNs make difficult for devices to compute cryptographic primitives. In sensor networks, communication entities are generally protected within a closed network. By contrast, IoT entities are connected to the Internet such that data is transferred over the global and public Internet. Consequently, this entails much more threats and vulnerabilities. For these reasons, there is a need to consider additional problems that are not applicable to the Internet.

To consider differences in device performance, the IETF Light-Weight Implementation Guidance (LWIG) working group classifies devices into three classes based on their capability [1]. The IETF Constrained RESTful Environment (CoRE) working group standardizes the constrained application protocol (CoAP) for resource-constrained devices. And several security protocols such as IKEv2, PANA, TLS, HIP, and EAP have been considered for IoT devices [2].

Because CoAP runs over UDP, Datagram Transport Layer Security (DTLS) is being discussed as a standard for the IoT security protocol. However, DTLS is too heavy for highly constrained devices in classes 0 and 1. In addition, the DTLS handshake message reduces LLN performance. In this regard, lightweight DTLS has

[1] Corresponding author: kang@duksung.ac.kr

ISSN: 2287-1233 ASTL

been proposed (see Section 2 in detail), but some problems remain such as low scalability and low practicality. Devices consisting of IoT are heterogeneous and show performance differences. Therefore, the security protocol should be provided according to the class.

This paper presents an alternative network model to address these problems. The rest of this paper is organized as follows: Section 2 provides a literature review. Section 3 describes an alternative IoT system model. Section 4 presents a use case to show applicability of the proposed model, and we conclude in Section 5.

## 2 Related Work

In IoT, smart devices in LLNs can be connected with systems over the Internet. Therefore, mapping of CoAP/DTLS to/from HTTP/TLS must be considered. The 6LoWPAN border router (6LBR) or proxy server can be used to interconnect the LLN with the Internet and performs the mapping between TLS and DTLS. During this process, End-to-End (E2E) security can be broken. As a solution, the DTLS capsulation for support E2E security has been proposed in [3], but it not only causes a lot of overheads in the LLN but also requires many changes in standard protocols.

To reduce code size for constrained devices, tinyDTLS based on Contiki OS has been proposed [4]. But the tinyDTLS is still heavy for constrained devices in classes 0 and 1 since it requires 11 KiB RAM and more than 77 KiB ROM. To reduce more, a modified tinyDTLS version has been implemented in [5] for devices categorized in class 1. However, there is a limitation in that it must use only a symmetric key.

Other issue is related to that the DTLS protocol has six message flights during the handshake phase. A single loss of message leads to restarting the handshaking process again. Packet delay and loss can be frequently happen in LLNs. In addition, performance of constrained devices can be degraded because of the reordering process. These result in difficulty in adopting DTLS protocol to IoT devices.

## 3 Proposed System Model

The proposed system architecture is motivated by a conventional web service model. The web service architecture using traditional TCP/IP networks is divided into two: front-end part and back-end part. A client (i.e. web browser) and web server are included in the front-end part. On the other hand, application processes, database, and authentication servers belong to the back-end part.

To realize web services in a secure manner, from the client perspective, the client requests TLS connections to the web server by using HTTPS and considers only the security between them as two end nodes in the front-end part. Namely, the client just handles and considers security between himself and the web server. Then, physical and logical security in the back-end part is managed by internal security policy. Therefore, even when there is no direct TLS connection between the client and the database server (i.e. contents), E2E security is not generally assumed to be broken.

 

We utilize this concept to solve scalability, practicality, and security issues in IoT. That is mainly because various IoT service inherits many properties from such a web service. Fig. 1 shows the proposed IoT architecture.

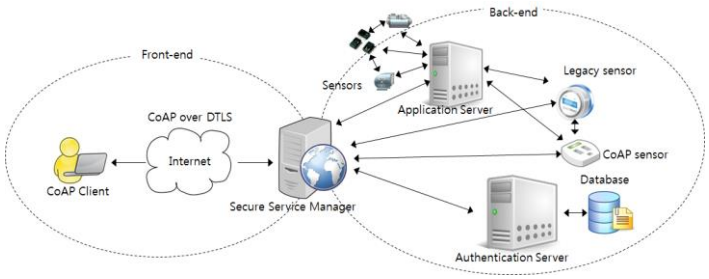


**Fig. 1.** Proposed IoT Service Architecture

In the proposed architecture, CoAP sensors are not considered as devices but as data contents and the CoAP server or proxy is regarded as an application server. Thus role of the SSM is similar to the web server in traditional Web. The client can request a DTLS connection to the SSM. Then, lightweight DTLS methods can be used for building DTLS connections between the CoAP client and the SSM. When the CoAP client wants to get data from a CoAP sensor, the end node of this communication is SSM. Therefore, there is no end-to-end security problem. In the back-end system, various security protocols can be applied between the SSM and sensors depending on the performance of each sensor and the importance of sensed data. As a result, both legacy and CoAP devices can communicate with each other securely by using the secure manner regardless of presence of DTLS connection.

## 4 Applied Scenarios

The proposed system architecture is well suited for various IoT services. This section presents a building automation system as a use case. Fig. 2 shows the BAS scenario in which the SSM is used.

The CoAP client sends initial request message and creates a secure tunnel with the SSM. If the secure channel is successfully created, then the SSM sends information on the placement of grouped sensors to the CoAP client. CoAP client sends a message about settings for light sensors grouped as a single content to the SSM. Then the SSM sends the message received from the CoAP client to the application server after creating a secure channel which is created by a predefined manner. Then the application server creates a secure channel with each light sensor. After the secure channel is created, the application server sends the command to each light sensor. When the application server receives a response from each sensor, it sends results to the SSM. Finally, the SSM responds to the CoAP client. Because each light sensor is grouped together logically, the client needs no DTLS connection to each sensor.

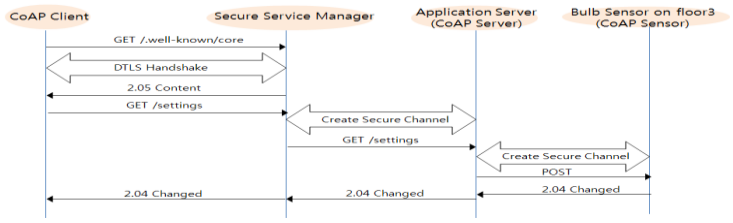


**Fig. 2.** Message Transactions for BAS

## 5 Conclusion

In this paper we propose an alternative system model that provides security, scalability, and practicality for IoT services in which the SSM is the major entity. Through the proposed model, resource-limited sensors such as those in classes 0 and 1 can communicate with the CoAP server or client in a secure manner with no direct DTLS connection. We also present an applicable scenario, where the proposed architecture is well suited and practical for IoT based service.

## Acknowledgments

This research was supported by the MSIP(Ministry of Science, ICT&Future Planning), Korea, under the ITRC(Information Technology Research Center)) support program (NIPA-2013-H0301-13-1003) supervised by the NIPA(National IT Industry Promotion Agency). Also, this research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Science, ICT & Future Planning(No. 2013023700).

## References

1. C. Bormann, M. Ersue.: Terminology for Constrained Node Networks. IETF Internet-Draft (2013)
2. O. Garcia-Morchon, S. Keoh, S. Kumar, R. Hummen, R. Struik.: Security Considerations in the IP-based Internet of Things. IETF Internet-Draft (2013)
3. M. Brachmann, S. Keoh, O. Morchon, S. Kumar.: End-to-end Transport Security in the IP-based Internet of Things. In: 21st International Conference on Computer Communications and Networks (ICCCN) pp. 1--5, IEEE, Munich (2012)
4. Tinydtls Documentation, http://tinydtls.sourceforge.net/
5. O. Bergmann, S. Gerdes, C. Bormann.: Simple Keys for Simple Smart Objects. In: Smart Object Security Workshop, IETF (2012)

 