International Journal of Security and Its Applications
Vol. 10, No. 8 (2016), pp.365-374
http://dx.doi.org/10.14257/ijsia.2016.10.8.32

A Study on the Device Authentication and Key Distribution Method for Internet of Things

Jae-young Lee[1] and Do-Eun Cho[2*]

[1] *School of Information & Communication Systems, Semyung University, Jecheon-city, 27136, Korea*
[2]*School of Information and Communication Convergence Engineering, Mokwon University, Doanbuk-ro 88, Seo-gu, Daejeon, 35349, Korea*
[1]*kiltie@semyung.ac.kr,* [2]*decho@mokwon.ac.kr*

Abstract

The internet of things (IoT) is a technology exchanging and sharing information without an operation and a help of a human. The technology is commercialized rapidly. However, IoT processes and transmits various forms of data at complex and different networks and it is exposed to the risks of information leakage, manipulation, and falsification. Moreover, the security vulnerability of IoT increased even further because IoT is composed of many low-performance devices and it is hard to apply the conventional security technologies to these low-performance devices. This study proposed a security method using a hash function and a symmetric encryption method to enhance confidentiality, mutual authentication, and data privacy under the IoT environment with limited resources. The proposed method authenticated a device by using a secret key, a device ID, and a random number and produced a session key, which was necessary to encrypt the transmitted data. This method could properly respond to the counterfeit, falsification, disguise, and replay attacks and secure the confidentiality of the data.

Keywords: *Internet of Things; wireless sensor network, integrity; authentication; session key*

1. Introduction

Interests on the Internet of Things (IoT) technology are growing in various fields. Gartner, a US market research agency, selected IoT as one of promising IT technologies in the next 10 years [1]. Global System for Mobile communications (GSMA) projected that more than 24 billion devices will be connected by 2020 and communication carriers would create a new profit of 1.2 trillion USD [2].

The outlook of IoT related market is bright. South Korea is working on identifying IoT based new services, supporting R&D, and establishing IoT test environment infrastructure to extend the IoT service, which were selected as main tasks to foster new internet businesses and led by Ministry of Science, ICT, and Future Planning. Besides, government agencies, the academic sector, and the private sector also have conducted various studies.

The IoT technology makes various devices exchanging and sharing information with each other on the internet without an operation or a help of a human. It is rapidly commercialized and applied to various fields including the smart healthcare, the smart car, the smart energy, and the smart factory. The IoT is expected to create a new service and a new market because it allows people and things communicating freely.

The IoT is a principal axis of various services directly related to the human life. Security of it must be secured to activate and guarantee the safety of related industries and

* Corresponding Author

ISSN: 1738-9976 IJSIA

services. The IoT processes and transmits various forms of data on a complex and heterogeneous networks. Therefore, it is exposed to information security risks such as information leakage, counterfeit, and falsification due to hackers or malicious software and virus. Moreover, it is expected the new security vulnerabilities will appear due to the opening of the IoT platform and interlocking among various heterogeneous terminals, sensors, and wired and wireless networks [3].

The security of the IoT has similar security issues with a sensor network and the internet (*e.g.*, privacy, authentication, access control, and information storage and management) [4,5].

The security domain of the IoT can be divided into the device security, the network security, and the service security. The device security is a security technology specialized for the gateway at a lightweight and low power demand center and high-performance device

The network security responds to various attacks under an environment connecting /linking networks using different hardware resources, communication systems, and security structures. It is a technology to provide a reliable end-to-end communication

The service security technology is specialized to satisfy security requirements of various IoT application services such as the smart healthcare, the smart car, the smart transportation, and the smart energy. In addition to them, there are other fundamental technologies including lightweight coding, authentication platform, and privacy protection technologies. This study proposed a session key distribution method for authenticating devices and protecting data under the IoT environment.

This study is composed as follows. Chapter 2 reviewed previous studies on the concept and the security threat of the IoT. Chapter 3 proposed a device authentication method and a session key distribution method on the IoT. Chapter 4 analyzed the security of proposed methods. The study was concluded in Chapter 5.

2. Related Works

2.1. IOT

The IoT can be defined as ‘a global infrastructure where people and things (physical or virtual) or things and things communicate with each other and which provides an intellectual service by combining knowledge base situational awareness’ [6].

The IoT began on the proposal of Kevin Ashton, the director of MIT’s Auto-ID Center, in 1999. It has been popularized upon the announcements of related market analysis data. The term IoT has been evolving. It has been interchangeably used with various terminologies (Table 1) [7][8].

IoT has been extended to IoE (Internet of Everything) through the concepts of M2M (Machine to Machine) and IoT (Internet of Thing). The concept of IoT is not a newly emerged concept. It should be considered a concept by merging, fusing, and extending existing technologies and it will develop more in the future [9].

IoT can be divided into three main areas. The first is the device area. The device area is the sum of a terminal and a sensor. It transmits data collected and extracted from specific things to other things. The second is the network area. The network area is a path transmitting data between a thing and a thing or a thing and a person. Lastly, the application area is to produce information by processing data and control and manage various devices [9].

Table 1. Internet of Things

Agency	Definition	
AIM	IOT	A global network infrastructure, linking physical and virtual object through the use of interoperable data capture and communication methods
ITU-T	IOT	A global infrastructure for the information society, enabling, advanced services by interconnecting things based on existing and evolving, interoperable information and communication technologies
IETF	IOT	A world-wide network of interconnected objects uniquely addressable, based on standard communication protocols
EU FP7	IOT	A global network infrastructure, linking physical and virtual object through the exploitation of data capture and communication capabilities
ETSI	IOT	Communication between two or more entities that do not necessarily need any direct human intervention
IEEE	IOT	Information exchange between a subscriber station and a server in the core network or between subscriber station, which may be carried out without any human interaction

2.2. Security Threats to the IoT

In the IoT environment, everything has a built-in sensor and an IoT user communicates with things through the sensor. However, more low-performance devices compose the IoT and it became harder to apply the existing security technologies to the IoT as they are. Therefore, the security threats to the IoT are increasing.

The IoT security can be divided into the device security, the application security, and the network security.

Devices composing the IoT are diversified and there are more low-performance devices than before. It is hard to apply the conventional security technologies to low-performance devices so security vulnerability increases.

The application execution environment of the IoT does not provide a uniform execution environment, unlike the conventional internet environment. Furthermore, it has many devices with lower computing power than common computers. Therefore, it is hard to provide conventional security platforms.

The IoT connects everything regardless of a person or a thing. A networking connected with everything has a complex structure. The network can be penetrated through various paths since it has a complex structure. In the process of interlocking various networks such as Wi-Fi and Bluetooth, it is hard to maintain a certain level of security because only limited device authentication is supported [10].

Table 2. Security Threats of the IoT [11]

Division	Security threats
Device	Confidentiality of the Terminal / Integrity Violations / Unauthorized Access / Vulnerable to Replica Node Attacks
Application	Data Fabrication and Modification / Confidentiality of User Data / Integrity / Privacy Violations / Unauthorized Access
Network	Data Fabrication and Modification / Authentication Interfere/ Confidentiality of Signal Data / Integrity Violations / Information Leakage / Denial of Service

2.3. Security Technology of the IoT

ZigBee, Wi-Fi, and RFID are main communication technologies in the IoT.

ZigBee is a short-range wireless communication protocol, which is based on IEEE 802.15.4 standard PHY layer and MAC sub layer with additional definitions of APS layer, ZOD, ZDP, AF, NWK, and ZigBee security layer [7]. ZigBee network is not high functional but it provides sufficient performance to send messages in conjunction with sensors and it has an advantage of connecting multiple devices. However, it is hard to apply high-level security technologies because the quantity of communicable information is limited [11-13].

There are two security technologies for ZigBee network (*i.e.,* Standard Security Mode (SSM) and High Security Mode (HSM)). SSM provides a low security level and HSM supports a high security level [14].

Wi-Fi is a wireless LAN technology based on IEEE 802.11 standard. Wi-Fi is particularly vulnerable to security threats because it communicates wirelessly. If transmitting data is not encrypted, various attacks including tapping, snapping, and unauthorized access can occur. Wired Equivalent Privacy (WEP) protocol is a way to protect data within a wireless section. There are also Wi-Fi Protected Access (WPA) and WPA2, which improved the shortcomings of WEP. Moreover, it is recommended to use an encryption algorithm (*e.g.,* Temporal Key Integrity Protocol (TKIP) and Counter mode with CBC-MAC Protocol (CCMP)) for the security in the access process additional to the communication process within a wireless section [11].

RFID is a wireless network technology to recognize tag information attached to things. It has drawn attention to establishing* a Ubiquitous Sensor Network (USN) environment. The tag used in RFID system is vulnerable to security threats (information leakage) because it is hard to apply a sophisticated security technology owing to the limited calculation capability and restricted power usage. Various methods have been studied for enhancing data security by authenticating among nodes during data transmission under a RFID/USN environment.

2.4. Methods for Device Authentication and Key Distribution under the IoT

The IoT is similar to the sensor network as it is a network using sensor nodes. However, the main difference between them is that the sensor network is a communication between a sensor node and a sink node (base station) while the IoT is mainly a communication among sensor nodes.

Juang *et al.,* (2006) proposed a shared key installation among sensor nodes and a method to distribute a session key by using a base station and a key station. However, a sensor node must communicate with a base station to share a session key among sensor nodes and then with a key distribution center, which is an inconvenient process [14].

Other studies proposed a session key distribution method using an open key encryption method. However, it is problematic that the resource of a sensor node is insufficient to install both RSA and ECC encryption modules.

Kim *et al.*, (2015) proposed a device authentication and session key distribution method based on ID by using a matching key encryption method (Figure 1).

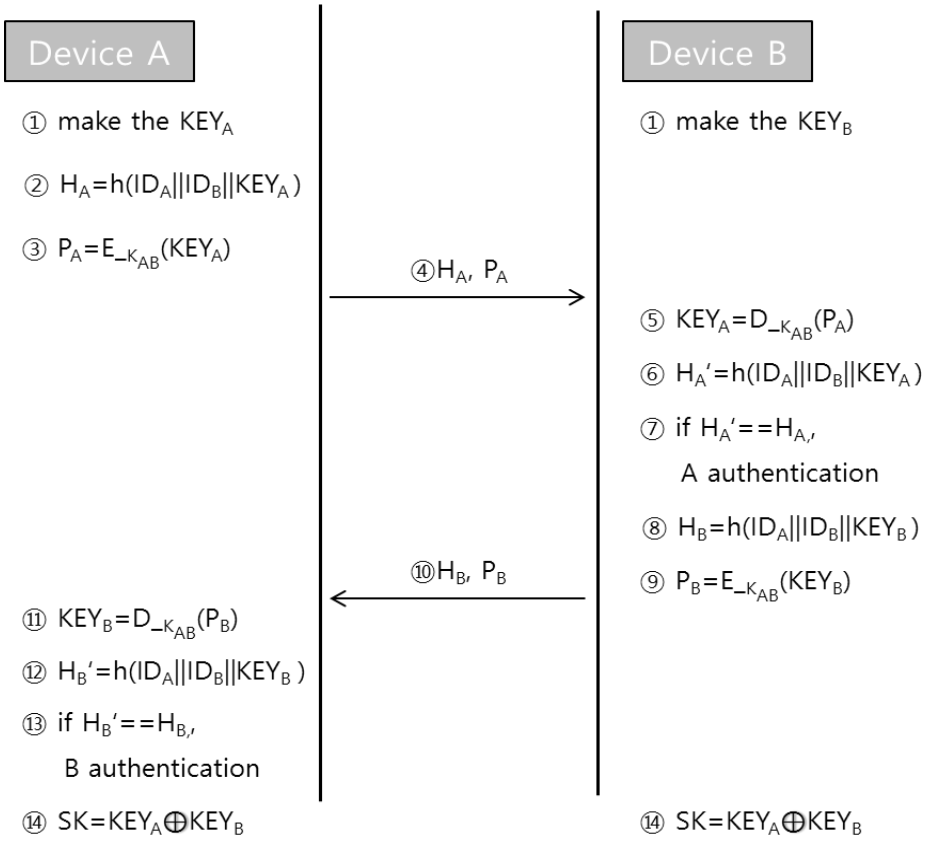

Figure 1. Protocol of Key Distribution

3. Proposed Method

A method to authenticate a device in the IoT and a method to create and distribute a session key, which is used for ensuring the confidentiality of transmitting data among devices, were proposed in Chapter 3.

It is assumed in the proposed method that the secret key KAB between two devices is securely stored in advance at the early device installation stage Random number R is added to prevent a duplicated message and a replay attack.

Table 3 summarized parameters used in the proposed method.

Table 3. Symbol of Protocol

Symbol	Definition
ID_A	ID of Device A
ID_B	ID of Device B
K_{AB}	Secret key shared by A and B

R	Random number
SK	Session Key
h()	Hash value

(1) Device A concatenates random number R_A in its secret key K_{AB} to prevent message duplication and generates P_A by applying a hash function to the value.

$$P_A=h(K_{AB}||R_A)$$

(2) Device A concatenates ID_A, its own ID, ID_B, an ID of the mating Device B, and P_A and calculates H_A by applying a hash function to it.

$$H_A=h(ID_A||ID_B||P_A)$$

(3) Device A sends H_A and random number R_A to Device B.

(4) Device B concatenates its secret key K_{AB} and random number R_A and creates P_A' by applying a hash function.

$$P_A'=h(K_{AB}||R_A)$$

(5) Device B concatenates ID_B, its own ID, ID_A, an ID of the mating Device A, and P_A' and estimates H_A' by applying a hash function to it.

$$H_A'=h(ID_A||ID_B||P_A')$$

(6) Device B compared the transferred H_A with self-made H_A'. If the two values are identical, it will confirm that H_A and R_A are successfully transferred from Device A and authenticate Device A.

(7) Device B concatenates its secret key K_{AB} and newly generated random number R_B and generates P_B by applying a hash function.

$$P_B=h(K_{AB}||R_B)$$

(8) Device B concatenates ID_B, its own ID, ID_A, an ID of the mating Device A, and P_B and estimates H_B by applying a hash function to it.

$$H_B=h(ID_A||ID_B||P_B)$$

(9) Device B transfers H_B and random number R_B to Device A.

(10) Device A concatenates random number R_B to its own secret key K_{AB} and creates P_B ' by applying a hash function.

$$P_B' =h(K_{AB}||R_B)$$

(11) Device A concatenates IDA, its own ID, ID_B, an ID of the mating Device B, and P_B' and calculates H_B' by applying a hash function to it.

$$H_B' =h(ID_A||ID_B||P_B')$$

(12) Device A compared the transferred H_B with H_B'. If the two values are identical, it will confirm that H_B and R_B are successfully transferred from Device A and authenticate Device B.

(13) If both are authenticated as normal devices, each device conducts a XOR calculation on its secret key K_{AB}, R_A, and R_B to create a session key.

(14) After producing a session key, Device A and Device B encrypt data using the session key and transmit it.

(15) When the session ends, two devices discard the used session key.

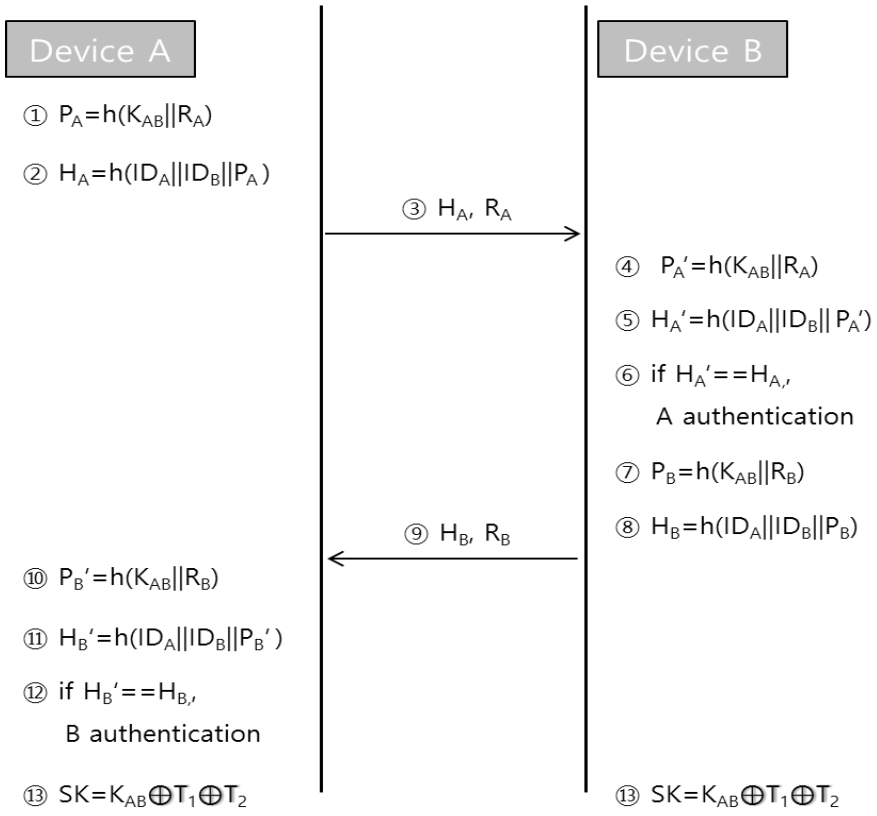

Figure 2. Proposed Method

The proposed method can authenticate with each other by two data transmission and calculation is fast because it uses a one directional hash function.

First, each device authenticates the other device by using a joint secret key KAB, random number, and own ID.

Secondly, a new random number is generated whenever a device authentication starts and a newly generated number is included in a new session key. Therefore, it can respond to a replay attack, which is made after the lapse of time. Even if a previously used session key were exposed, it would maintain a confidentiality regarding other information. Consequently, it can respond to a message falsification attack.

Thirdly, existing methods to authenticate devices and create session keys required each device creating a key value additional to a joint secret key KAB. However, the proposed method only used a secret key KAB readily shared at the device installation step so it reduced unnecessary operation and helped to operate a system with insufficient resources.

4. Security Analysis

Chapter 4 analyzed the security of the proposed method.

The conventional ID based device authentication method is vulnerable to disguise attack due to an ID exposure. However, the proposed device authentication method using an ID creates a value by concatenating an ID of each device, a safely readily shared secret key, and a random number to prevent replay attack and applies a hash function to it. The concatenated value varies each time because of a random number, which changes whenever an authentication starts. Moreover, it is hard to estimate the original value

owing to the use of a hash function, a one-directional function. Therefore, it is impossible to counterfeit data required to authenticate. Consequently, the integrity of authentication data is guaranteed. If the integrity of authentication data is guaranteed, it can protect it from data counterfeit, falsification, and disguise attacks.

Intermediate attack means that an attacker participates in the device authentication process, the session key production, and the distribution process and the attacker attack with using the acquired information. For an attacker to participate in the device authentication and the session key production, the attacker must know the secret key. However, two devices shared the key during an installation process and it is not a transmitting data. Therefore, an attacker cannot guess the secret key from the acquired information. Since an attacker cannot get the secret key, the intermediate attack can be prevented. An attacker may acquire the session key by using other methods instead of breaking codes. An attacker can descramble data with using the acquired session key and an attacker may code a new data to disguise it as the data of a legitimate device. The proposed method uses a readily shared secret code and a random number, which is newly made for each authentication. It is discarded after one use. Even if an attacker acquires a discarded session key, the past session key cannot predict a new session key.

The proposed method does not require a separate key value produced by each device for authenticating and producing a session key, unlike other studies. Because it only uses a readily shared secret key and a random number, it reduces an unnecessary operation and helps the operation of the IoT, which has only limited resources.

5. Conclusions

This study proposed a key distribution method for authenticating a device and protecting data in the IoT environment.

The proposed method starts from an assumption that the secret key, which was shared since the initial installation, has been stored safely. The device authentication and the session key rely on the shared secret key and a random number generated for each authentication.

The secret key used to authenticate a device is shared during the initial installation stage. Therefore, it is impossible to know, unless it is a designated device, and the random number changes for each authentication. A hash function used for an authentication is a one-directional function, so it is hard to estimate an initial value from the final value. Consequently, it is impossible of an attacker to launch counterfeit and falsification attacks.

Even if transmitting data is exposed during a device authentication process, a session key production process, and a distribution process to an attacker, the attacker cannot acquire the secret key because it was shared during the installation. Consequently, the attacker cannot acquire the secret key. Therefore, an attacker without the secret key cannot start an authentication or produce a session key.

A session key is created by running XOR on the secret key and a random number created by each device at the beginning of an authentication. Even if an attacker acquired the previous session key, it would be impossible of an attacker to predict the next session key unless the attacker knows the secret key of a device. It means that an attacker cannot decode other data except the data coded with the acquired session key. It means that confidentiality is quarantined.

Unlike conventional methods creating a new key whenever a device authentication and a session key production begins, this study creates a session key by using a secret key and a random number, which prevents a replay attack. It reduces operation steps and helps the operation of a system, which has limited resources.

However, the proposed method is based on the assumption that a secret key is stored from the initial installation and safe. If the secret code is exposed, the proposed method

will provide only limited security. The future study should study how to share a secret key safely.

Acknowledgments

This paper was supported by Semyung University Research Grant 2014.

References

[1] Gartner, "2012 Gartner's Hype Cycle for Emerging Technologies", http://www.gartner.com/newsroom/id/2124315, **(2012)**.
[2] Gigacom, "Internet of things will have 24 billion devices by 2020", https://gigaom.com/2011/10/13/internet-of-things-will-have-24-billion-devices-by-2020, **(2011)**.
[3] J. Cui and X. Zhao, "A Study on the Device Authentication and key distribution Method for Internet of Things", International Journal of Future Generation Communication and Networking, vol. 9, no. 6 **(2016)**, pp. 55-64.
[4] D. H. Kim, "Security for IoT Service", Journal of Korea Institute of Communication and Information Services, vol. 30, no. 8, **(2013)**, pp. 53-65.
[5] C. S. Pyo, H. Y. Kang, N. S. Kim and H. C. Bang, "IoT (M2M) technology trends and development prospects" , Journal of The Korean Institute of Communication Sciences, vol. 30, no. 8, **(2013)**, pp. 3-10.
[6] C. Lu, "Overview of Security and Privacy Issues in the Internet of Things", http://www.cse.wustl.edu/~jain/cse574-14/ftp/security/, **(2014)**.
[7] D. H. Shin, J. Y. Jung and S. H, Kang, "Internet of Things trends and development prospects", Journal of Internet Information, vol. 14, no. 2, **(2013)**, pp. 32-46.
[8] S. H. Kim, "Key Distribution Scheme between Lightweight Devices in Internet of Thing", Graduate School Sungkyunkwan University, Dept. of Information Security, **(2015)**.
[9] D. H, Kim and K. Kwak, "Design of Improved Authentication Protocol for Sensor Networks in IoT Environment", Journal of The Korea Institute of Information Security & Cryptology, vol. 25, no. 2, **(2015)**, pp. 467-478.
[10] H. I. Jung and C. S. Kim, "A Study on the Security Technology for the Internet of Things", Journal of Security Engineering, vol. 11, no. 5, **(2014)**, pp. 429-438.
[11] D. S. Kim, "Key distribution protocol for improved security in wireless sensor network", Graduate School Dankook University, **(2014)**.
[12] B. H. Kim, J. M. Lim and C. S. Park, "Analysis of ZigBee Security Mechanism", Journal of Security Engineering, vol. 9, no. 5, **(2012)**, pp. 417-428.
[13] J. H. Jun, "Analysis on the Security threat factors of the Internet of Things", Convergence security journal, vol. 15, no. 7, **(2015)**, pp. 47-53.
[14] J. Y, Park, S. M. Shin and N. H. Kang, "Mutual Authentication and Key Agreement Scheme between Lightweight Devices in Internet of Things", Journal of Communications and Networks, vol. 38, no 9, **(2013)**, pp. 707-714.

Authors

Jae-young Lee, She received the B.S. degree in computer science and M.S. degree in computer science education from Semyung University, Korea in 1996, 2000 and Ph.D degree in computer engineering from Chungbuk National University, Korea in 2007. She is currently an assistant processor in School of Information & Communication Systems, Semyung University, Korea. Her main research interest is Network Security.

Do-Eun Cho, She received her master's degree and Ph.D degree in Computer Engineering from Semyung and Chungbuk National University, Korea. She currently lectures at the Innovation Center for Engineering Education, Mokwon University, Korea. Dr. Cho's research interests include Security, Ubiquitous Computing and Ubiquitous Sensor Network.