ISSN 2234-4438
융합정보논문지 제7권 제3호 pp. 91-96, 2017 DOI : https://doi.org/10.22156/CS4SMB.2017.7.3.091

IoT에서 게이트웨이에 대한 인증 프로토콜에 관한 연구

이재영*
세명대학교 정보통신학부

A Study on gateway authentication protocol in IoT

Jae-Young Lee*
School of Information & Communication Systems, Semyung University

요 약 사람과 사람, 사물과 사물이 유·무선 네트워크로 연결되어 서비스를 제공하는 것이 IoT이다. 인터넷을 통해 각 디바이스가 직접 연결되는 IoT의 특성으로 인해 보안에 대한 중요성이 더욱 강조되고 있다. 때문에 IoT 환경에서 발생할 수 있는 다양한 보안 문제를 해결하기 위한 인증 프로토콜을 비롯한 보안 모듈이 계속적으로 개발되어 왔으나 여전히 취약점이 발견되고 있다. 이에 본 논문에서 제안한 인증 프로토콜에는 기존의 인증 프로토콜에서 생략되어 있는 게이트웨이에 대한 인증 절차와 디바이스와 게이트웨이 상호간의 인증 절차를 추가하였다. 인증 절차가 추가된 프로토콜은 공격자의 위장 공격에 대응할 수 있다. 또한, 인증에 이용되는 메시지에 중요한 정보는 암호키로 암호화하거나 해시 함수를 이용하여 보호함으로써 도청 공격에 대응할 수 있게 하였다.

키워드 : IoT, 인증, 디바이스, 암호화, 무선 네트워크

Abstract IoT which is an abbreviation of Internet of Things refers to the communication network service among various objects such as people-people, objects-objects interconnection. The characteristic of IoT that enables direct connection among each device makes security to be considered as more emphasized factor. Though a security module such as an authentication protocol for resolving various security problems that may occur in the IoT environment has been developed, some weak points in security are still being revealed. Therefore, this paper proposes a method for including a protocol including gateway authentication procedure and mutual authentication between the devices and gateways. Protocols with additional authentication procedures can appropriately respond to attackers' spoofing attacks. In addition, important information in the message used for authentication process is protected by encryption or hash function so that it can respond to wiretapping attacks.

Key Words : Internet of Things, Authentication, Device, Encryption, Wireless network

1. 서론

사물인터넷은 사람과 사물 사물과 사물의 연결을 통해 언제 어디서나 정보를 전송할 수 있는 정보통신기술의 개념에 무엇을 추가하여 생활 속 모든 것을 상호 연결시키는 기술이다[1]. 사물인터넷이 발달함에 따라 그에 대한 보안 위협도 증가하고 있다. 그러나 다양한 종류의 사물들이 연결되어 있는 사물인터넷의 특성상 하드웨어의 성능이 낮은 사물들도 서로 연결되어 있어 기존의 강도 높은 보안 모듈이 적용되기 어렵기 때문에 사물인터넷 환경에 적당한 보안 기술이 개발되고 있다[2-4].

특히 사물인터넷 네트워크 내에 연결되어 있는 디바이

Received 2017-06-08 Revised 2017-06-12 Accepted 2017-06-20 Published 2017-06-30
*Corresponding author : Jae-Young Lee (klitie@semyung.ac.kr)

스에 대한 인증은 사물인터넷 환경에서 발생할 수 있는 보안상의 취약점을 해결하는데 중요한 역할을 담당한다.

본 논문에서는 기존의 인증 프로토콜의 문제점을 개선하는 인증 프로토콜을 제안하려 한다.

제안하는 인증 프로토콜에서는 사물인터넷을 구성하는 디바이스와 게이트웨이가 서로를 인증하는 절차를 포함하여 위장 공격에 대응할 수 있게 하였고, 전송되는 메시지에 포함되는 중요한 정보는 비밀키로 암호화 하거나, 해시 함수를 이용하여 보호함으로써 도청 공격에 대응할 수 있게 하였다.

본 논문의 구성은 다음과 같다. 2장에서는 사물인터넷에 대한 설명과, 기존의 인증 프로토콜에 대해 설명하고 3장에서는 개선된 인증 프로토콜을 제안한다. 4장에서는 제안한 인증 프로토콜의 안전성을 평가하고, 마지막 5장에서 결론을 맺는다.

2. 관련연구

2.1 사물인터넷(IoT, Internet of Things)

유·무선 네트워크와 스마트 디바이스의 발전으로 사람과 사물 등의 각 객체 간에 언제, 어디서나, 어떤 것이든 연결이 가능한 사물인터넷(Internet of Things, IoT)에 대한 관심이 높아지고 있다. IoT는 Fig. 1과 같이 '언제' '어디서'나 정보를 전송할 수 있다는 기존의 정보통신 기술 개념에 '무엇'이라는 개념을 추가하여 사물과 사물 간의 동적 연결을 가능하게 함으로써 진정한 유비쿼터스 환경을 실현시킬 수 있는 기술이다[2,5].

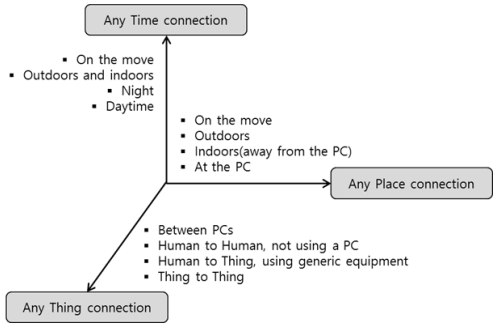

Fig. 1. Concept of the IoT

IoT는 크게 세가지 영역으로 구성된다. 사물에 내장된 센서를 이용하여 데이터를 수집하고 전송하는 디바이스 영역, 사람과 사물, 사물과 사물 간 전송되는 데이터의 유·무선 통로인 네트워크 영역, 마지막으로 전송된 데이터를 처리하여 정보를 생성하고, 생성된 정보를 이용하여 디바이스를 제어하고 관리하는 어플리케이션 영역 등이다[2,3].

IoT의 디바이스와 사용자는 디바이스에 내장된 센서를 통하여 정보를 통신한다. 그러나 IoT를 구성하는 디바이스의 종류가 다양해져서 성능이 낮은 사양을 가지는 디바이스가 많아지고, 환경적으로도 관리가 쉽지 않은 경우가 많기 때문에 물리적 공격을 비롯한 다양한 보안 위협이 존재하게 되었다[6]. 게다가 IoT를 구성하는 디바이스 중 성능이 낮은 디바이스에는 기존의 네트워크에서 이용되는 보안 기술을 그대로 적용하기가 어렵기 때문에 보안상의 위협이 더욱 증가하고 있다.

Table 1은 IoT 환경에서의 보안 취약점을 정리한 것이다[2,7-9].

Table 1. Security Threats of the IoT

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

이에 따라 IoT 환경에서 발생할 수 있는 보안 위협을 해결하기 위해 낮은 성능의 디바이스에도 적용할 수 있는 인증 프로토콜 등의 보안 기술이 계속적으로 개발되어 왔지만 대부분의 보안 기술에서 여전히 취약점이 발견되고 있다. 특히 IoT를 구성하는 디바이스를 확인하는데 필수인 인증 프로토콜에서 발생할 수 있는 취약점에는 다음과 같은 것들이 있다[4].

- 위장 공격(Impersonation Attack) : 공격자가 정당한 서버로 위장하여 클라이언트의 인증 절차에 개입하여 디바이스와 사용자의 인증에 이용되는 키를

불법으로 획득하는 공격.

- 재전송공격(Replay Attack) : 공격자가 인증 절차에 이용되었던 메시지를 저장하여, 이후의 다른 정당한 인증 절차에 그 메시지를 재사용하는 공격.
- 인증키 추측공격(Authentication Key Guessing Attack) : 공격자가 사용자와 디바이스, 디바이스와 디바이스 간의 인증 절차에 이용된 메시지를 확인하여 정당한 사용자와 디바이스의 인증키를 추측하는 공격.
- 서비스 거부 공격(Denial of Service Attack) : 공격자가 인증 절차에 관여하여 디바이스나 사용자의 인증 요청에 대한 응답을 막아서 인증 서비스를 거부하는 공격[11].
- 프라이버시 침해(Invasion of Privacy) : 인증 절차에 이용되는 메시지를 분석하여 인증 절차에 참여하는 주체를 노출시키는 공격[12].

2.2 기존의 인증 프로토콜

사물인터넷 시스템 구성은 Fig. 2와 같이 하나의 접근 서버(Access server)에 여러 개의 도메인이 존재하고 도메인 내에 하나의 게이트웨이가 존재하며 게이트웨이에 여러 개의 디바이스들이 연결되어있는 형태이다[6].

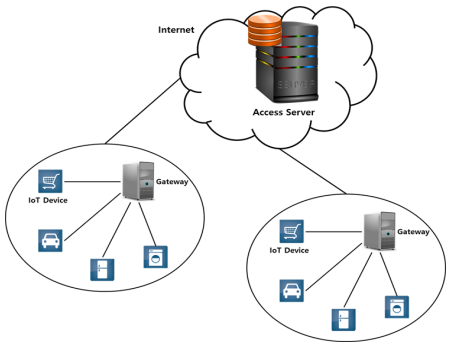

Fig. 2. System Architecture

게이트웨이는 디바이스로부터 정보를 수집하는데, 디바이스가 게이트웨이로 데이터를 전송하기 위해서는 먼저 인증 절차를 거쳐야한다. 이때 디바이스의 비밀키와 ID, 게이트웨이의 비밀키와 ID는 접근 서버에 미리 저장되어있다고 가정한다. Table 2는 프로토콜에서 이용되는 파라미터를 정리한 것이다.

Table 2. Protocol Parameters

symbol	explanation
ID_D	ID of device
ID_G	ID of gateway
k_D	Secret key of device
k_G	Secret key of gateway
E()	Symmetric-key Algorithm
h()	Hash function
r_D	Random number of device
r_G	Random number of gateway
$\oplus$	XOR
$\|\|$	Concatenation operation

다음에 설명하는 인증 프로토콜은 연구에서 제안한 것이고, 인증 과정은 다음과 같다[13].

1) 디바이스는 자신의 ID를 게이트웨이에게 전송한다.
D->G : ID_D

2) 게이트웨이는 자신의 비밀키를 이용하여 디바이스로부터 수신한 디바이스의 ID를 암호화하여 접근 서버에 전송한다.
G->A : E_{k_G}(ID_D)

3) 접근 서버는 게이트웨이로부터 수신한 값을 복호화하여 디바이스의 ID를 얻는다. 디바이스의 ID와 디바이스의 비밀키를 게이트웨이의 비밀키로 암호화하여 게이트웨이로 전송한다.
A->G : E_{k_G}(ID_D, k_D)

4) 게이트웨이는 접근 서버로부터 수신한 값을 복호화하여 디바이스의 비밀키를 얻고, 디바이스에게 자신의 난수를 전송한다.
G->D : r_G

5) 디바이스는 게이트웨이로부터 수신한 난수와 자신의 비밀키의 해시 값을 계산하여 게이트웨이로 전송한다.
D->G : h(k_D$\oplus$r_G)

게이트웨이는 디바이스로부터 수신한 값과 자신의 생성한 값을 비교하여 두 값이 동일하면 디바이스를 인증하고, 동일하지 않으면 인증을 중단한다.

이와 같은 인증 프로토콜에는 게이트웨이를 인증하는 절차가 없어서 공격자가 게이트웨이로 위장하는 공격에

취약할 수 있다. 또한 1)에서 디바이스가 자신의 ID를 게이트웨이로 전송할 때 ID가 암호화되어 있지 않아 공격자의 도청 공격에 취약하다.

3. 제안하는 인증 프로토콜

기존의 인증 프로토콜에는 게이트웨이를 인증하는 과정에 생략되어 공격자가 정당한 게이트웨이로 위장할 수 있고. 공격자가 정당한 게이트웨이로 위장을 하는 경우 스푸핑 공격에 노출될 수 있다. 또한 인증 절차 1)에서 디바이스가 자신의 ID를 암호화하지 않고 공개된 채널을 이용하여 게이트웨이에 전송함으로써 공격자의 도청 공격에 노출될 수 있다. 디바이스의 ID를 도청한 공격자는 정당한 게이트웨이로 위장한 후, 접근 서버에 디바이스의 인증을 요청할 수도 있고, 인증 절차가 끝나면 공격자는 디바이스의 비밀키를 얻어 다양한 공격에 활용할 수 있다.

본 논문에서는 첫째, 디바이스와 게이트웨이의 상호 인증 절차를 추가하고, 둘째, 게이트웨이에 대한 인증을 추가하여 공격자의 위장 공격에 대응한다. 마지막으로 전송되는 메시지의 중요한 정보는 비밀키로 암호화하거나, 해시 함수를 이용하여 보호하게 함으로써 공격자의 도청 공격에 대응할 수 있는 개선된 인증 프로토콜을 제안한다.

본 논문에서 제안하는 인증 프로토콜은 기존의 인증 프로토콜과 동일하게 접근 서버에 디바이스의 ID와 비밀키, 게이트웨이의 ID와 비밀키가 미리 안전하게 저장되어 있다고 가정한다.

제안하는 인증 프로토콜의 절차는 다음과 같다.

1) 게이트웨이는 난수를 생성하여 디바이스에게 전송한다.
   G->D : r_G

2) 디바이스는 ID, 비밀키, 난수의 해쉬 값과, 난수를 비밀키로 암호화하여 게이트웨이에게 전송한다.
   D->G : E_{k_D}(h(ID_D||k_D||r_D),r_D)

3) 게이트웨이는 수신한 암호 값과, 자신의 ID, 비밀키, 난수의 해시 값, 그리고 자신의 난수를 비밀키로 암호화하여 접근 서버에게 전송한다.
   G->S : E_{k_G}(E_{k_D}(h(ID_D||k_D||r_D),r_D), h(ID_G||k_G||r_G), r_G)

4) 접근 서버는 수신한 암호 값을 게이트웨이의 비밀키 k_G로 복호화 하여 Ek_D(h(ID_D||k_D|r_D), r_D), h(ID_G||k_G||r_G), 그리고 r_G를 얻고 다시 디바이스의 비밀키로 암호 값을 복호화 하여 h(ID_D||k_D||r_D)와 r_D를 얻는다.

먼저 h(ID_G||k_G||r_G)를 만족하는 해시 값을 게이트웨이 테이블에서 검색한다. 만족하는 값을 찾으면 게이트웨이를 인증한다.

다시 h(ID_D||k_D||r_D)를 만족하는 해시 값을 디바이스 테이블에서 검색하고 만족하는 값을 찾으면 디바이스를 인증한다.

5) 접근 서버는 디바이스의 난수를 게이트웨이의 비밀키로 암호화하여 게이트웨이로 전송한다.
   S->G : E_{k_G}(r_D)

6) 게이트웨이는 전송 받은 암호 값을 복호화 하여, 디바이스의 난수를 얻고, 디바이스의 난수와 와 자신의 난수의 해시 값 H를 생성하여 디바이스에게 전송한다.
   G->D : h(r_D||r_G)

7) 디바이스는 1단계에서 수신한 게이트웨이의 난수와 자신의 난수를 이용하여 H'을 만들어 수신한 H와 비교하여 게이트웨이를 인증한다.

Fig. 3은 인증 프로토콜의 절차이다.

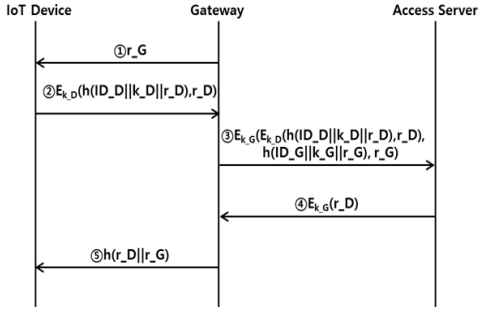

Fig. 3. Proposed Authentication protocol

제안하는 인증 프로토콜에서는 게이트웨이와 디바이

스의 상호 인증과 접근 서버에 의한 게이트웨이 인증을 추가하여 공격자가 게이트웨이로 위장하여 발생할 수 있는 문제점에 대응할 수 있게 하였다. 또한 기존의 인증 프로토콜에서 디바이스가 자신의 ID를 암호화하지 않고 전송함으로써 발생할 수 있는 공격자의 도청 공격에 대응하기 위해 전송되는 메시지의 중요한 정보는 암호화와 해시함수를 이용하여 보호할 수 있게 하였다.

4. 안정성 분석

본 논문에서는 기존의 인증 프로토콜에는 게이트웨이를 인증하는 절차가 포함되지 않아서 게이트웨이로 위장하는 공격자의 위장 공격에 취약한 문제와, 인증 절차에 중요한 메시지가 암호화되지 않고 전송되어 공격자의 도청 공격에 취약한 점을 개선한 인증 프로토콜을 제안하였다.

첫째, 인증 절차 1)단계에서 디바이스는 게이트웨이가 전송한 난수를 저장하고, 게이트웨이는 6)단계에서 게이트웨이에 대한 인증을 마친 접근 서버가 전송하는 디바이스의 난수를 저장한다. 게이트웨이는 자신의 난수와 디바이스의 난수를 이용하여 해시 값 H을 만들어 디바이스에게 전송하면 디바이스는 게이트웨이의 난수와 자신의 난수를 이용하여 해시 값 H′를 만든다. 디바이스는 H와 H′를 비교하여 게이트웨이를 인증할 수 있다. 게이트웨이와 디바이스가 서로를 인증하면 위장 공격과 스푸핑 공격에 대응할 수 있게 된다.

둘째, 인증 절차에 필요한 메시지의 중요한 정보는 비밀키로 암호화 하거나, 해시 함수를 이용하여 보호함으로써 공격자의 도청 공격에 대응할 수 있게 하였다. 인증 절차에 필요한 모든 메시지가 도청의 위험에 노출되어 있다고 가정한다면, 암호키를 알지 못하는 공격자는 메시지에 포함된 중요한 정보를 알 수 없고를 해시 함수는 해시 값을 알더라도 원래의 정보를 복원하기는 어렵다. 인증에 필요한 ID나 비밀키는 해시 값으로 메시지에 포함된다. 메시지의 비밀성이 유지되면 프라이버시 침해 공격이나 인증키 추측 공격에 대응할 수 있다.

셋째, 제안한 인증 프로토콜에서도 기존의 인증 프로토콜에서와 마찬가지로 인증 절차에 필요한 메시지에 난수를 포함하게 하였다. 메시지에 포함된 난수는 공격자의 재전송 공격에 대응할 수 있다.

Table 3은 기존의 인증 프로토콜과 본 논문에서 제안한 프로토콜의 안전성을 비교한 것으로 기존의 인증 프로토콜은 재전송 공격에 대응할 수 있는 반면 제안한 프로토콜은 공격자의 다양한 공격에 대응할 수 있다.

Table 3. Safety Analysis for Authentication Protocol

Security threats	Existing protocol	Proposed
Mutual Authentication	X	O
Replay Attack	O	O
Spoofing attack	X	O
Invasion of Privacy	X	O
Impersonation Attack	X	O
Authentication Key Guessing Attack	X	O

5. 결론

생활 속의 모든 것들이 상호 연결되는 IoT는 IoT를 구성하는 디바이스의 특성상 기존의 보안 기술이 그대로 적용되기 어려워 IoT가 발전하는 만큼 보안 위협이 증가하고 있다. 이에 IoT환경에 맞는 다양한 인증 프로토콜이 개발되었지만 여전히, 위장 공격(Impersonation attack), 재전송 공격(Replay attack), 인증키 추측 공격(Authentication key guessing attack), 서비스 거부 공격(Denial of service attack), 프라이버시 침해(Invasion of privacy) 등에 취약하다

본 논문에서는 기존의 인증 프로토콜에 게이트웨이와 디바이스 상호 간에 인증 절차를 추가하고, 접근 서버에 의한 게이트웨이 인증 절차를 추가하여 공격자의 위장 공격에 대응할 수 있게 하였다. 또한 인증 절차에 이용되는 메시지의 중요 정보는 암호화하거나 해시 함수를 이용하여 보호함으로써 도청 공격에 대응할 수 있게 하였다.

본 연구는 접근 서버에 디바이스의 ID나 비밀키 등의 중요한 정보가 안전하게 저장되어 노출 공격에 안전하다는 것을 가정한다. 때문에 중요 정보의 안전한 공유와 저장에 대한 연구와 IoT에서의 디바이스들의 상호 인증과 더불어 사용자 인증에 대한 추가적인 연구가 필요하다.

ACKNOWLEDGMENTS

본 논문은 2015학년도 세명대학교 교내학술연구비 지원에 의해 수행된 연구임.

REFERENCES

[1] S. H. Hong, “Research on IoT international strategic standard model,” *Journal of the korea convergence society*, Vol. 8, No. 2, pp. 21-26, 2017,
DOI : 10.15207/JKCS.2017.8.2..021

[2] S. H. Kim, *Key distribution scheme between lightweight devices in internet of thing*, Graduate School Sungkyunkwan University, 2015.

[3] B. I. Jang and C. S. Kim, “A Study on the Security Technology for the Internet of Things,” *Journal of Security Engineering*, Vol. 11, No. 5, pp. 429-438, 2014.

[4] D. H. Kim and J. Kwak, “Design of Improved Authentication Protocol for Sensor Networks,” *Journal of The Korea Institute of Information Security & Cryptology*, Vol. 25, No. 2, 2015.

[5] C. W. Park and J. W. Kim, “An Empirical Research on Information Privacy Concern in the IoT Era,” *Journal of Digital Convergence*, Vol. 14, No. 2, pp. 65-72, Feb. 2016. DOI : 10.14400/JDC.2016.14.2.65

[6] J. O. Park, “A Study of Message Communication Method Using Attribute Based,” *Journal of Digital Convergence*, Vol. 14, No. 10, pp. 295-302, Oct. 2016.
DOI : 10.14400/JDC.2016.14.10.295

[7] E. Kim, *Secure device authentication method in the internet of things*, Graduate School Kyungnam University. 2014.

[8] Ministry of Science, ICT and Future Planning, *Internet of Things Information Security Roadmap*, Oct. 2014.

[9] H. J. Mun, G. H. Choi and Y. C. H, “Countermeasure to underlying security threats in IoT communication,” *Journal of convergence society for SMB*, Vol. 6, No. 2, pp. 37-44, Jun. 2016.
DOI : 10.22156/cs4smb.2016.6.2.037

[10] S. S. Shin, G. S. Chae, T. H. Lee, “An Investigation study to reduce security threat in the Internet of things environment,” *Journal of convergence society for SMB*, Vol. 6, No. 2, pp. 31-36, Jun. 2016.
DOI : 10.22156/cs4smb.2016.6.2.031

[11] Y. S. Lee, “Authentication Method for Safe Internet of Things Environments,” *The Journal of Korea Institute of Information, Electronics, and Communication Technology*, Vol. 18, No. 1, pp. 51-58, 2015.
DOI : 10.17661/jkiiect.2015.8.1.051

[12] S. G. Yeo and K. H. Lee, “Smart Phone and vehicle Authentication scheme with M2M device,” *Journal of the korea convergence society*, Vol. 2, No. 4, pp. 1-7, 2011.

[13] J. S. Shin and Y. H. Park, “An Authentication Protocol using the EXOR and the Hash Function in RFID/USN,” *Journal of the Korea Industrial Information Systems Research*, Vol. 12, No. 2, pp. 24-29, 2007.

저 자 소 개

이 재 영(Jae-Young Lee) [정회원]

- 1996년 2월 : 세명대학교 전자계산학과 학사
- 2000년 8월 : 세명대학교 전산교육과 석사
- 2007년 2월 : 충북대학교 컴퓨터공학과 박사
- 2012년 9월 ~ 현재 : 세명대학교 정보통신학부 조교수

<관심분야> : 네트워크 보안, 정보 보호