한국정보전자통신기술학회논문지(jkiiect)'15-02, Vol.8 No.1
논문 15-08-01-051 http://dx.doi.org/10.17661/jkiiect.2015.8.1.051

안전한 사물 인터넷 환경을 위한 인증 방식

이영석*

Authentication Method for Safe Internet of Things Environments

Young-Seok Lee*

요 약 사물 인터넷(Internet of Thing)은 다양한 기술 요소의 집합체로서, 최근 IoT 플랫폼의 개방화를 통하여 이기종 단말, 네트워크, 애플리케이션 간의 연동이 가속화될 것으로 예상된다. 이에 따라, IoT 환경에서 많은 기술적이고 관리적인 보안 위협이 발생할 것이다. 본 논문에서는 안전한 IoT 서비스를 위해 최근에 연구되었던 인증 기술을 분석하여 더욱 안전한 통신을 제공하기 위한 상호 인증 프로토콜을 제안한다. 제안한 인증 프로토콜은 게이트웨이와 IoT 디바이스 간 상호 인증을 제공함으로써 악의적인 게이트웨이나 불법적인 디바이스로 위장을 방지할 수 있다. 제안된 인증 프로토콜의 성능분석과 평가를 수행한다.

Abstract Internet of Thing is a collection of various technical components, and the interworking among heterogeneous devices, networks, applications is expected to be accelerated through the openness of IoT platform. For this reason, many technical and administrative security threats will occur in IoT environments. In this paper, authentication methods of recent researches are analyzed for safe IoT services, and new mutual authentication protocol is proposed to provide more secure communication. The proposed protocol prevents an impersonation as malicious gateway or illegal device providing mutual authentication between gateway and IoT device. The performance analysis and evaluation of proposed authentication protocol are performed.

Key Words : Internet of Things, authentication, access server, gateway, IoT device

1. 서론

사물 인터넷(IoT, Internet of Thing) 서비스는 IoT 기술 특성상 다양한 보안 위협에 취약하다는 단점이 존재한다. 특히, 낮은 전력량 및 계산량, 적은 메모리 등과 같은 제한적인 하드웨어 사양을 가지며, 환경적으로도 관리가 쉽지 않은 지역에 분포되는 경향이 많기 때문에 물리적인 공격을 비롯해 다양한 보안 위협 요인을 잠재적으로 가진다. 이러한 특성은 IoT 서비스 플랫폼의 안전한 운영에 치명적인 오류를 일으키거나 잘못된 정보를 기반으로 서비스를 제공하게 되어 IoT 서비스 플랫폼이 자체적으로 기능을 상실하는 결과를 초래할 수 있다[1].

최근에는 IoT 플랫폼의 개방화를 통한 이기종 단말, 네트워크, 애플리케이션 간 연동이 가속화될 것으로 예상되는 가운데, 이로 인한 기술적, 관리적 측면의 다양한 보안위협들이 발생할 것으

In this paper, Kunsan National University in 2014 under its own academic research by funding projects collusion.
*Corresponding Author : School of Computer & Information Communication, Kunsan National University, Kunsan, Korea(leeys@kunsan.ac.kr)
Received January 7, 2015 Revised January 29, 2015 Accepted February 8, 2015

로 예상된다. IoT 환경에서 발생할 수 있는 보안 위협들은 기존의 정보통신 환경에서 나타날 수 있는 위협들을 상속한다. 흔히 정보보안의 3대 요소라고 할 수 있는 CIA, 즉 기밀성(Confidentiality), 무결성(Integrity), 가용성(Availability)을 침해함으로써 정상적인 서비스의 이용 및 제공을 방해하는 보안위협들이 나타날 수 있다. IoT의 각 구성요소에서 발생할 수 있는 보안위협들을 살펴보면 아래의 [표 1]과 같다[2].

이에 따라, IoT 장치들이 다양한 환경의 서비스 플랫폼에서 개별 사용자의 플랫폼 내부 인증과 인가되지 않은 사용자에 의한 임의적인 접근으로부터 장치를 보호하기 위한 접근제어 방식이 필요하며, IoT 서비스 플랫폼에 가입되거나 제휴된 다양한 플랫폼 응용서비스까지 통합적으로 인증되는 기술 연구가 요구된다.

표 1. IoT 구성 요소별 보안 위협
Table 1. Security Threats of IoT Components

구분	보안 위협
단말	분실/도난, 물리적 파괴
네트워크	무선신호 교란, 정보유출, 데이터 위변조, 서비스 거부
어플리케이션	정보유출, 데이터 위변조, 서비스 거부

현재 IoT 환경에서 발생할 수 있는 보안 문제를 해결하기 위해 지금까지 많은 연구자들에 의해 다양한 인증 프로토콜(Authentication protocol)들이 최근까지 개발되어져 오고 있다. 하지만 현재까지 제안되어져 오고 있는 대부분의 인증 프로토콜들은 다비이스의 위치추적으로 위치 트래킹 공격(Location tracking attack)이 쉬우며, 재전송 공격(Replay attack)이나 스푸핑 공격(Spoofing attack)에 취약하며, 다양한 보안 취약점과 프라이버시 침해 문제들을 가짐을 많은 연구자들에 의해 발견되어 지고 있다[3][4].

2007년에 연구[5]에서는 USN(Ubiquitous Sensor Network) 환경을 위한 해쉬 함수와 배타적 논리합(XOR) 연산을 이용한 인증 프로토콜을 제안하였다. 여기서 제안한 인증 프로토콜의 안전성 분석을 통하여 재전송 공격, 스푸핑 공격, 위치 트래킹 공격, 태그 키 유출 공격(Key exposure attack) 등에 안전함을 주장하였다.

본 논문에서는 기존에 제안된 인증 프로토콜의 문제점을 개선하면서 IoT 디바이스와 게이트웨이 사이에 상호인증을 제공하는 새로운 인증 프로토콜을 제안하고 검증한다. 본 논문의 구성은 다음과 같다. 2장에서는 기존 인증프로토콜 연구 동향에 대해 살펴보고, 3장에서는 본 논문에서 제안한 프로토콜을 기술한다. 4장에서는 기존에 제안된 인증 프로토콜들과 본 연구에서 제안한 프로토콜의 성능을 비교하고, 제안 프로토콜의 효율성에 대해 살펴본다. 5장에서는 제안된 상호 인증 프로토콜과 기존 인증 프로토콜들의 효율성을 분석하기 위해 시뮬레이션을 수행하고 성능 평가의 결과를 기술한다. 6장에서 결론을 맺는다.

2. 관련연구

2.1 인증 시스템 구성

IoT 환경에서 디바이스와 게이트웨이 사이의 인증은 3가지 구성요소로 이루어져 있다. [그림 1]에서 보듯이, 도메인 내에 게이트웨이가 존재하며 게이트웨이는 동일한 도메인의 디바이스로부터 데이트를 수신한다. 데이터를 전송하는 디바이스를 인증하기 위해 접근 서버에 디바이스의 사전 공유키가 저장되어 있다고 가정한다. 접근 서버는 여러 도메인 상에 존재하는 게이트웨이와 사전 공유키가 저장된다.

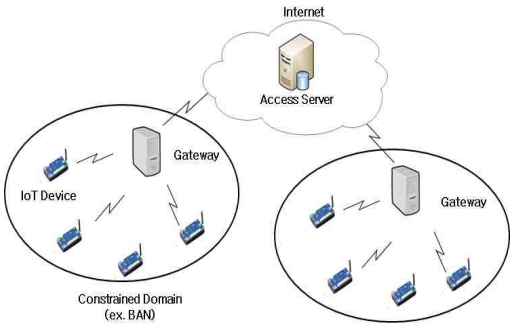

그림 1. 시스템 구성도
Fig. 1. System Architecture

2.2 기존 인증 프로토콜 절차

본 절에서는 연구[5]에서 제안한 인증 프로토콜에 관해 설명한다. [표 2]은 본 연구에서 사용되는 시스템 파라미터들을 보여준다.

표 2. 프로토콜 파라미터
Table 2. Protocol Parameters

기호	설명
Access Server	접근 서버
Gateway	게이트웨이
Device	IoT 디바이스
IDG	게이트웨이 식별자(ID)
IDS	IoT 디바이스 식별자(ID)
k	IoT 디바이스와 접근 서버 사이의 사전 공유 비밀키
gk	게이트웨이와 접근 서버 사이의 사전 공유 비밀키
E()	대칭키 암호
h()	해쉬 함수
r	게이트웨이가 생성한 난수
t	IoT 디바이스가 생성한 난수
⊕	배타적 논리합(XOR)
||	연접 연산

기존 인증 프로토콜에서 접근 서버와 게이트웨이 사이에는 사전에 안전한 세션키 gk가 설정되어 있음을 가정하며, 각 IoT 디바이스의 비밀키 k는 접근 서버에 등록되어 있음을 가정한다. IoT 디바이스는 자신의 식별자 IDS와 비밀키 k를 갖고 있으며, 게이트웨이는 자신의 식별자 IDG와 비밀키 gk를 갖고 있다고 가정한다. 또한, 접근서버는 디바이스와 게이트웨이의 식별자와 해당 비밀키를 갖는다고 가정한다. [그림 2]는 기존 인증 프로토콜의 구성과 동작 과정을 보여주며, 다음의 5단계를 거쳐 인증 과정이 이루어진다.

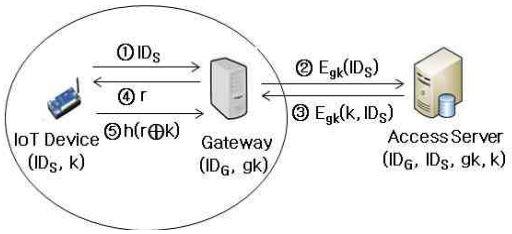

그림 2. 기존 인증 프로토콜 수행 절차
Fig. 2. Existing Authentication Protocol

(1) 디바이스는 자신의 IDS를 게이트웨이에게 전송한다.

(2) 게이트웨이 접근서버와 설정된 세션키 gk를 사용하여 디바이스의 IDS를 암호화하여 Egk(IDS)를 접근서버에게 전송한다.

(3) 접근서버는 게이트웨이로부터 전송받은 Egk(IDS)을 세션 키 gk를 사용하여 복호화 한다. 그런 다음, 디바이스 IDS의 비밀 키 k를 이용하여 암호화한 후, Egk(k, IDS)을 게이트웨이에게 전송한다.

(4) 게이트웨이 접근서버로부터 수신한 Egk(k, IDS)을 복호화하여 디바이스의 비밀 키 k를 저장하고, 디바이스에게 랜덤 값 r을 전송한다.

(5) 디바이스는 게이트웨이로부터 수신한 랜덤 값 r과 자신의 비밀 키 k를 이용하여 h(r⊕k)을 계산하여 게이트웨이에게 전송한다. 게이트웨이는 h(r⊕k)을 계산하여 수신한 h(r⊕k)과 동일한지를 비교한다. 만약 두 값이 같으면 디바이스를 인증하고, 다르면 인증을 중단한다.

이러한 인증 프로토콜에서 디바이스는 게이트웨이를 전혀 인증하지 않기 때문에 공격자가 게이트웨이로 위장하여 스푸핑 공격을 성공할 수 있다. 또한, 임의의 공격자가 단계 (2)에서 디바이스가 전송한 IDS를 도청하여 소유하고 있다고

가정하자. IDS는 공개된 통신 채널을 통해 전송됨으로 공격자는 쉽게 획득할 수 있다. 그러면 해당 공격자는 임의의 세션에서 게이트웨이로 위장하여 위치 트래킹 공격을 성공할 수 있다. 그리고, 단계 (3)에서 임의의 디바이스 대한 비밀키 k를 획득하기 위한 악의적인 목적을 가진 게이트웨이가 존재한다고 가정할 때, 해당 게이트웨이는 디바이스 키 유출 공격을 수행하여 간단히 디바이스의 비밀 키 k를 획득한 후 해당 디바이스로의 스푸핑 공격 등을 수행 할 수 있다.

2.3 개선된 기존 인증 프로토콜 절차

기존 인증 프로토콜에서의 스푸핑 공격 및 위치 트래킹 공격에 대한 취약점을 제거하고 디바이스 익명성을 제공하는 개선된 기존 인증 프로토콜이 제안되었다. 제안한 프로토콜에서는 스푸핑 공격 및 위치 트래킹 공격에 안전하기 위해 디바이스에서도 게이트웨이와 마찬가지로 임의의 랜덤 값을 생성하도록 설계하였다[6].

기존 인증 프로토콜과 마찬가지로 접근 서버와 게이트웨이 간에 사전에 안전한 세션키 gk가 설정 되어 있다고 가정하며, 각 디바이스의 비밀키 k는 접근 서버에 등록되어 있다고 가정한다. [그림 3]은 개선된 기존 인증 프로토콜의 동작 과정을 보여주며, 다음의 4단계를 거쳐 인증 과정이 이루어진다.

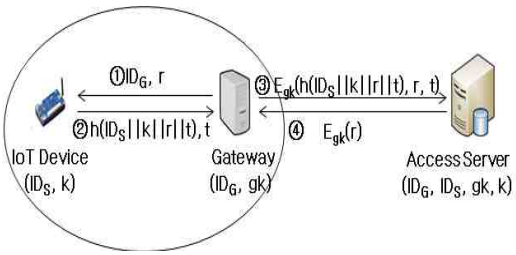

그림 3. 개선된 기존 인증 프로토콜 수행 절차
Fig. 3. Enhanced Authentication Protocol

(1) 게이트웨이는 랜덤 값 r을 생성한 후, 디바이스에게 IDG와 함께 r을 전송한다.

(2) 디바이스는 랜덤 값 t를 생성한 후, 게이트웨이로부터 수신한 r과 자신의 IDS 및 비밀 키 k을 이용하여 랜덤 해쉬 값 h(IDS||k||r||t)을 계산한 후, h(IDS||k||r||t)과 t를 게이트웨이에게 전송한다.

(3) 게이트웨이는 접근 서버와 설정된 세션 키 gk를 사용하여 디바이스로부터 수신한 h(IDS||k||r||t)과 t 그리고 자신이 생성한 r을 암호화하여 Egk(h(IDS||k||r||t), t, r)를 접근 서버에게 전송한다.

(4) 접근 서버는 게이트웨이로부터 전송 받은 Egk(h(IDS||k||r||t), t, r)을 세션 키 gk를 사용하여 복호화 한 후, h(IDS||k||r||t)을 계산하여 자신의 데이터베이스 내에 저장하고 있는 모든 ID와 k 쌍을 이용하여 게이트웨이로부터 수신한 h(IDS||k||r||t)값과 일치하는 IDS와 k 쌍을 검색한다. 만약 일치하는 값이 검색되지 않으면, 오류 메시지를 게이트웨이에게 전송하고, 일치하는 값이 검색되면 디바이스를 인증하고 게이트웨이가 생성한 랜덤 값 r과 함께 세션 키 gk로 암호화하여 Egk(r)을 게이트웨이에게 전송한다. 게이트웨이는 접근 서버로부터 수신한 값이 오류일 경우, 디바이스와의 통신을 중단하고, 정상적인 인증이 되었을 경우에서는 접근 서버로부터 수신한 Egk(r)을 복호화하여 r을 얻는다. 상호인증을 위해 복호화된 r이 자신이 생성한 랜덤 값 r과 동일한지를 검증한다. 만약 동일한 r이 맞으면, 게이트웨이는 디바이스에 대해 원하는 작업을 수행한다.

개선된 기존 인증프로토콜 역시 디바이스는 게이트웨이에 대한 인증을 하지 않기 때문에 악의적인 게이트웨이로의 위장이 가능하다. 만약 읽고 쓰기가 가능한 디바이스의 경우, 공격자는 악의적인 게이트웨이를 이용하여 인증과정을 무시하고 디바이스에게 직접적으로 요금을 부과하거나 부당한 명령을 전달할 수 있다[7].

기존 인증 프로토콜은 재전송 공격만을 방지할 수 있으며, 개선된 기존 인증 프로토콜은 재전송 공격, 센서 익명성, 센서 키 노출은 방지할

수 있지만 스푸핑 공격과 상호 인증은 제공하지 못한다. 두 인증 프로토콜의 안전성 분석을 비교한 내용이 [표 3]에 보여진다[8].

표 3. 기존 인증 프로토콜 안전성 분석
Table 3. Safety Analysis for Authentication Protocols

위협요인	기존 인증 프로토콜	개선된 인증 프로토콜
상호 인증	X	X
재전송 공격	O	O
스푸핑 공격	X	X
디바이스 익명서	X	O
위치 트래킹	X	O
디바이스 키 노출	X	O

3. 게이트웨이와 디바이스의 인증 모델

3.1 인증 프로토콜 절차

기존에 제안된 인증 프로토콜의 문제점을 해결하면서 게이트웨이와 디바이스 사이에 상호인증을 제공하는 개선된 인증 프로토콜을 제안한다.

제안된 프로토콜을 수행하기 전에 디바이스의 IDS와 비밀 키 k는 안전하게 접근 서버에 등록되어 있으며, 오직 디바이스와 접근 서버만이 알고 있다고 가정한다. 또한 게이트웨이와 접근 서버는 사전에 세션 키 gk를 공유하고 있으며 안전한 통신채널을 이용한다고 가정한다. 제안하는 상호 인증 프로토콜의 동작과정은 다음과 같다.

[그림 4]는 제안된 상호 인증 프로토콜의 메시지 교환 절차를 보여준다. 상호 인증 프로토콜은 5단계의 인증 절차를 포함한다.

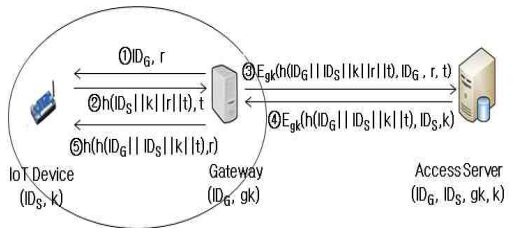

그림 4. 제안된 인증 프로토콜 수행 절차
Fig. 4. Proposed Authentication Protocol

(1) 게이트웨이는 랜덤 값 r을 생성한 후, 디바이스에게 자신의 IDG와 함께 r을 전송한다.

(2) 디바이스는 난수 t를 생성하고, 게이트웨이로부터 수신한 난수 r을 사용하여 인증메시지 h(IDG||IDS||k||t||r)을 계산하여 t와 함께 게이트웨이에게 전송한다.

(3) 게이트웨이는 디바이스로부터 수신한 h(IDG||IDS||k||t||r)와 자신의 IDG,디바이스 난수 값 t, 그리고 자신이 생성한 난수 r을 세션 키 gk를 사용하여 암호화한 후, 접근 서버에게 Egk(h(IDG||IDD||k||t||r),IDG,r,t)를 전송한다.

(4) 접근 서버는 Egk(h(IDG||IDD||k||t||r), IDG,r,t)를 복호화한 후, 저장된 디바이스들의 ID와 게이트웨이 ID, 난수 t, r을 이용하여 h(IDG||IDS||k||t||r)를 만족하는 해쉬 값을 검색한다. 만일 일치되는 해쉬 값이 없으면 게이트웨이에게 인증 실패 메시지를 전송하고, 일치되는 값이 있으면 디바이스를 인증하고 Egk(h(IDG||IDS||k||t))를 생성하여 게이트웨이에게 전송한다.

(5) 게이트웨이는 접근 서버로부터 수신한 Egk(h(IDG||IDD||k||t))를 복호화하고 디바이스가 정당함을 인증한 후, h(h(IDG||IDD||k||t),r)를 계산하여 디바이스에게 전송한다. 다비이스는 자신의 비밀 키 k를 이용하여 h(h(IDG||IDD||k||t),r)를 계산하여 수신된 해쉬 값과 일치하는지 확인한다. 일치하는 경우 정당한 게이트웨이로 인증하고, 일치하지 않을 경우 통신을 중단한다.

제안하는 프로토콜에서 디바이스의 ID는 접근 서버만이 알고 있으며, 디바이스의 ID가 전송될 때에도 게이트웨이와 디바이스가 각각 생성한 난수 t, r과 함께 디바이스의 ID를 해쉬한 결과 값을 전송함으로써 디바이스의 익명성을 보장할 수 있다.

또한, 스푸핑 공격은 디바이스의 비밀 키를 얻어 디바이스로 위장하거나 게이트웨이와 디바이스간의 상호인증이 이루어지지 않을 경우 악의적인 게이트웨이로 위장하는 것이다. 제안하는 프로토콜에서 전자의 경우, 디바이스의 비밀 키 k

는 안전한 해쉬 함수에 의해 변형된 값으로 전송되므로 디바이스의 비밀 키는 보호된다. 후자의 경우, h(IDG||IDS||k||t||r)과 h(h(IDG||IDS||k||t),r)의 검증을 통해 게이트웨이와 디바이스간 상호인증을 제공하기 때문에 악의적인 게이트웨이로의 위장은 불가능하다. 따라서 제안하는 프로토콜은 스푸핑 공격에 대해 안전하다고 볼 수 있다.

3.2 인증 모델의 통신량 분석

통신량은 디바이스와 게이트웨이 사이의 통신량과 게이트웨이와 접근서버 사이의 통신량으로 구분된다. 기존 인증 프로토콜에서 디바이스와 게이트웨이 사이의 통신량을 분석해 보면, 디바이스 ID에 해당하는 정보 t의 1회 전달, 해쉬 값 h의 1회 전달, 난수 값 r의 1회 전달로서 log(t) + log(h) + log(r) = log(thr)의 통신량을 갖는다. 게이트웨이와 접근서버 사이의 통신량은 디바이스 ID에 해당하는 정보 t의 2회 전달과 게이트웨이/접근서버 사이의 비밀 키 k의 1회 전달로서 log(t) + log(t) + log(k) = log(t2k)의 통신량을 갖는다.

개선된 인증 프로토콜에서 디바이스와 게이트웨이 사이의 통신량을 분석해 보면, 해쉬 값 h의 1회 전달, 난수 값 r의 2회 전달로서 log(h) + log(r) + log(r) = log(hr2)의 통신량을 갖는다. 게이트웨이와 접근서버 사이의 통신량은 해쉬 값 h의 1회 전달, 난수 값 r의 3회 전달로서 log(h) + log(r) + log(r) + log(r) = log(hr3)의 통신량을 갖는다.

제안된 인증 프로토콜에서 디바이스와 게이트웨이 사이의 통신량을 분석해 보면, 해쉬 값 h의 2회 전달, 난수 값 r의 2회 전달로서 log(h) + log(h) + log(r) + log(r) = log(h2r2)의 통신량을 갖는다. 게이트웨이와 접근서버 사이의 통신량은 해쉬 값 h의 2회 전달, 난수 값 r의 2회 전달로서 log(h) + log(h) + log(r) + log(r) = log(h2r2)의 통신량을 갖는다. 각 방식의 통신량을 비교해 보면 [표 4]와 같다.

표 4. 인증 프로토콜 통신량 비교
Table 4. Comparison of Communication Quantity

구분	기존 인증 프로토콜	개선된 인증 프로토콜	제안된 인증 프로토콜
디바이스와 게이트웨이	log(thr)	log(hr2)	log(h2r2)
게이트웨이와 접근서버	log(t2k)	log(hr3)	log(h2r2)

- t : 디바이스 식별자(ID)
- h : 해쉬 값
- r : 랜덤 값
- k : 비밀키

4. 성능 평가

제안하는 인증 프로토콜과 이전 인증 프로토콜들의 효율성을 분석하기 위해 시뮬레이션을 수행하였다. 시뮬레이션은 IoT 시스템 환경에서 기존 방식, 개선된 방식, 그리고 제안된 상호 방식의 프로토콜을 통신량 측면에서 비교한다.

시뮬레이션은 OPNET 17.1[9]을 이용하여 수행되었고, 시뮬레이션을 위해 디바이스 데이터 전송율은 1Mbps로 가정하였고, 게이트웨이 데이터 전송율은 11Mbps로 가정하였다[10]. [그림 5]는 OPNET을 이용한 프로세스 모델링을 보여준다.

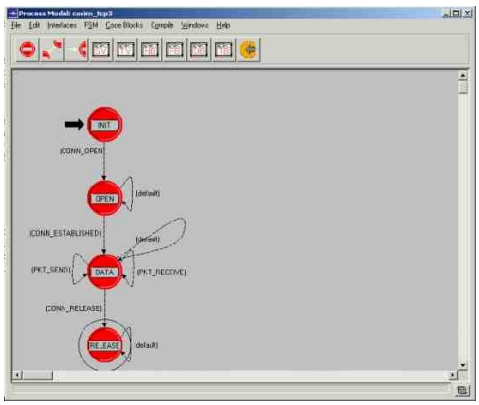

그림 5. OPNET 프로세스 모델링
Fig. 5. OPNET Process Modeling

통신량에 대한 비교 그래프는 디바이스와 게이트웨이 구간, 게이트웨이와 접근 서버 구간으로 표현하였다. [그림 6]에서 보듯이, 디바이스와 게이트웨이 사이의 통신량은 제안 프로토콜과 거의 같음을 알 수 있다.

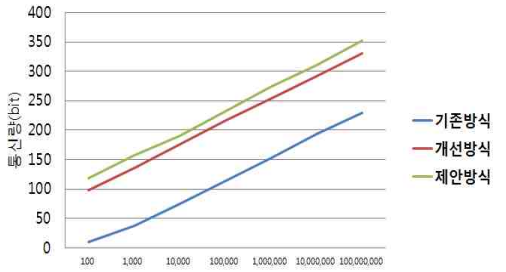

그림 6. 통신량 비교(디바이스-게이트웨이)
Fig. 6. Comparison of Communication Quantity (Device-Gateway)

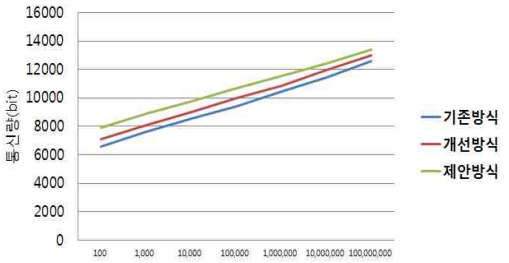

그림 7. 통신량 비교(게이트웨이-접근서버)
Fig. 7. Comparison of Communication Quantity (Gateway-Access Server)

게이트웨이와 접근 서버 사이에서의 통신량은 [그림 7]과 같이 1억 개의 디바이스를 저장하고 있는 접근 서버를 사용 시 기존 프로토콜은 12,561 비트의 통신량을 필요로 하며, 개선된 프로토콜은 약 13,000 비트정도의 통신량을 필요로 한다. 그리고 제안 프로토콜은 13,400 비트의 통신량만을 필요로 한다. 그래프에서 보듯이 거의 같은 수준의 통신량을 요구한다.

5. 결론

IoT 서비스는 IoT 기술 특성상 다양한 보안 위협에 취약하다는 단점이 존재한다. 특히, 낮은 전력량 및 계산량, 적은 메모리 등과 같은 제한적인 하드웨어 사양을 가지며, 환경적으로도 관리가 쉽지 않은 지역에 분포되는 경향이 많기 때문에 물리적인 공격을 비롯해 다양한 보안 위협 요인을 잠재적으로 가진다. 이러한 특성은 IoT 서비스 플랫폼의 안전한 운영에 치명적인 오류를 일으키거나 잘못된 정보를 기반으로 서비스를 제공하게 되어 IoT 서비스 플랫폼이 자체적으로 기능을 상실하는 결과를 초래할 수 있다.

이에 따라, IoT 장치들이 다양한 환경의 서비스 플랫폼에서 개별 사용자의 플랫폼 내부 인증과 인가되지 않은 사용자에 의한 임의적인 접근으로부터 장치를 보호하기 위한 접근제어 방식이 필요하며, IoT 서비스 플랫폼에 가입되거나 제휴된 다양한 플랫폼 응용서비스까지 통합적으로 인증되는 기술 연구가 요구된다[11].

본 논문에서는 보다 안전한 IoT 서비스 위하여 최근에 연구되었던 인증 기술을 분석하여 보다 안전한 통신을 위해 상호인증을 제공하는 게이트웨이/디바이스 인증 프로토콜을 제안하였다. 제안한 인증 프로토콜은 게이트웨이와 디바이스 간 상호인증을 제공함으로써 악의적인 게이트웨이나 불법적인 디바이스로의 위장을 방지할 수 있으며, 손상된 게이트웨이에 대하여 디바이스의 비밀 키를 보호할 수 있다.

제안 프로토콜은 경량 프로토콜이므로 기존 저성능 IoT 디바이스에 적용가능하기 때문에, 대부분 인증 및 프라이버시 보호 서비스에 적용될 수 있을 것으로 기대된다.

REFERENCES

[1] O. Savry, F. Vacherand, "Security and privacy protection of contactless devices", In The Internet of Things, pp. 409-419, 2010.

[2] Hwa-jeon Seo, et al, "IoT Security Technical Trend", Korean Institute of Electromagnetic Engineering Society, Vol. 24, No. 4, pp. 27~35, 2013, 7.

[3] P. de Leusse, P. Periorellis, T. Dimitrakos, and S.K. Nair, "Self managed security cell, a security model for the internet of things and services", In Advances in Future Internet, 2009 First International Conference on, pp. 47-52, 2009.

[4] D. Hong, J. Sung, S. Hong, J. Lim, S. Lee, B. Koo, C. Lee, D. Chang, J. Lee, K. Jeong, H. Kim, J. Kim, and S. Chee, "Hight: a new block cipher suitable for low-resource device," In Proceedings of the International Conference on Cryptographic Hardware and Embedded Systems(CHES 06), pp. 46-59, 2006.

[5] Jin-seob Shin, Young-ho Park, "An Authentication Protocol using the EXOR and the Hash Function in RFID/USN," Korea Society of Industrial Information Systems, Vol. 12, No. 2, pp.24-29, 2007. 6.

[6] Hae-Soon Ahn, Ki-Dong Bu, "Improved Authentication Protocol for RFID/USN Environment," The Institute of Electronics and Information Engineers, Vol.46, No. CI-1, 2009.

[7] O. Savry, F. Vacherand, "Security and privacy protection of contactless devices", In The Internet of Things, pp. 409-419, 2010.

[8] D. Engels, M. J. O. Saarinen, P. Schweitzer, and E. M. Smith, "The hummingbird-2 lightweight authenticated encryption algorithm", In Proceedings of the 7th International Conference on RFID Security and Privacy(RFIDSec'11), pp. 19-31, 2011.

[9] http://www.opnet.com

[10] Taeyang Eom, Jeong-Hyun, "Performance Evaluation of Authentication Protocol for Mobile RFID Privacy", Korean Institute of Communication and Information Sciences, Vol. 36, No 6, 2011. 6.

저자약력

이 영 석(Young-seok Lee) [종신회원]

- 1992년 2월 : 충남대학교 컴퓨터공학과(학사)
- 1994년 2월 : 충남대학교 컴퓨터공학과(석사)
- 2002년 2월 : 충남대학교 컴퓨터공학과(박사)
- 1994년 1월 ~ 1997년 2월 : LG전자 연구원
- 2002년 3월 ~ 2004년 8월 : 한국전자통신연구원 선임연구원
- 2004년 9월 ~ 현재 : 군산대학교 컴퓨터정보통신공학부 교수

<관심분야> 정보보안, 사물인터넷, 이동컴퓨팅