사물 인터넷망을 이용한 스마트 홈에서의 기기 인증 메카니즘

김정태
목원대학교

Authentication Mechanism of Devices in Smart Home Using Internet of Things

Jung Tae Kim
Mokwon University
E-mail : jtkim3050@mokwon.ac.kr

요 약

최근 들어 과학기술의 발전으로 인하여 유무선 통신 환경이 통합되는 형태로 발전되고 있다. 인터넷의 발전으로 인하여 사물들이 서로 상호 연결하여 융합하는 사물인터넷 환경으로 발전되고 있다. 이러한 사물인터넷 환경 하에서의 대표적인 응용 시스템으로 홈 네트워크가 그 실 예이다. 사물인터넷을 이용한 센서 노드에서의 통신 환경은 작은 메모리 용량, 낮은 컴퓨팅 파워 등과 같은 제한적인 자원으로 인하여 기존의 암호 알고리즘을 사용을 할 수 없다. 따라서 본 논문에서는 이러한 IoT 환경 기반의 홈 네트워크 하에서의 보안을 위한 기기간의 인증을 분석하였다.

ABSTRACT

Recently, as science and technology is very growing, wire and wireless communication is merged and interconnected. Therefore, advanced internet technology allow all kinds of communication to integrate with heterogeneous device and sensors. The representative example is smart home network based on internet of things. Communication surroundings under IoT services are more complex. Conventional encryption techniques can't provide to IoT application because of its limited resources such as small memory capacity and low computing power. In this paper, we analyzed authentication procedure between home gateway and node in sensor under smart home network.

키워드

Encryption, Internet of things, IoT, Authentication

Ⅰ. 서 론

최근 들어 반도체 제조 공정의 발전으로 인하여 많은 소자들이 경박단소하게 제작됨으로 인해 소형화 및 가격이 낮아지고 있다. 특히 기존의 유무선 망이 통합되어 지고 사물인터넷에 연결된 수많은 이기종의 소자, 기기, 단말기, 센서들이 상호 연결하여 운용되어지고 있다. 특히 IoT 기기들은 임베디드 형태의 시스템으로 구현이 되어 현재 시장에 많은 제품을 출시하고 있다. 사물인터넷망에 연결된 소자 및 센서들의 정보보호를 위하여 보안 메카니즘을 반드시 충족을 시켜야 한다. 그러나 기존의 관용 보안 알고리즘을 활용하기 위해서는 IoT 센서, 기기 등에서의 제한된 메모리, 컴퓨팅 파워 등의 문제로 인하여 기존의 알고리즘을 사용할 수 없게 되었다. 따라서 현재는

많은 연구자들이 이러한 보안적인 문제점을 해결하기 위하여 초경량화된 알고리즘을 개발 중에 있으나 고비도 수준의 알고리즘을 현재까지 개발 중에 있다. 따라서 본 논문에서는 대표적인 IoT 응용 시스템인 홈 네트워크 한경하에서의 보안적인 문제점을 분석하였다.

II. 시스템 구성

본 논문에서 구성하는 시스템의 구성은 그림 1과 같으며, 오부망은 인터넷으로 연결이 되어지고 홈 네트워크을 연결하기 위하여 홈게이트웨이를 통하여 상호 연결하는 구조로 되어 있다. 따라서 보안적인 고려 사항으로 외부 망과 홈 게이트웨이는 기존의 알고리즘을 통하여 보아적인 취약성을 극복할 수 있으나, 홈 네트워크 망에서는 통신 연결을 위하여 블루투스, 지그비, 와이파이 등을 0주로 사용하여 보안 취약성이 많이 발생한다. IoT 응용 시스템에서의 보안적인 이슈는 주로 시스템의 종단간의 디바이스 연결상 에서 문제가 주로 발생을 한다. 여기에서 홈게이트웨이는 외부 시스템의 점근 제어 및 홈 네트워크 시스템에서의 모니터링과 인증 관련 사항을 주로 담당한다. 이러한 게이트웨이는 서로 다른 IoT 표준사이의 접속을 변환하는 역할을 주로 한다.

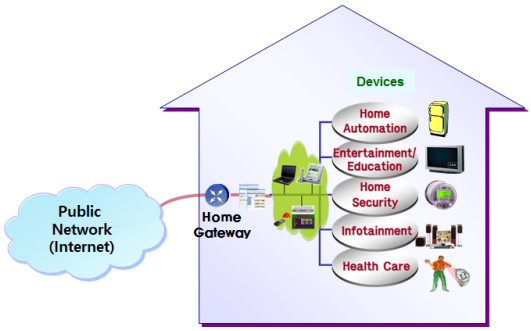

그림 1. 스마트 홈 네트워크의 구성도

각각의 디바이스가 서로 연결하기 위해서는 중간의 홈 게이트웨이를 경유하여 프로토콜을 연결하여 정보를 서로 전달하는 구조로 되어 있다.

III. 인증 프로세서

인증 문제는 IoT 시스템에서의 센서 노드 혹은 각각의 기기 상에서는 상당한 중요한 문제이다. 이러한 인증 절차를 위해서는 기존의 공개키 기반의 상호 인증 프로토콜을 주로 사용하여 문제를 해결하고 있다. 이러한 프로토콜은 ECC 기반의 상호 인증을 위하여 사용하고, 인증 과정이 연결되면 ECDH(Elliptic Curve DiffiHellman) 알고리즘을 사용하여 연산 과정을 거쳐 상호 인증하는 구조로 되어 있다. 다음의 그림 2는 상호 인증하는 프로토콜의 절차를 보여 주고 있다. 홈 게이트웨이와 연결하고자 하는 디바이스 간의 인증을 위한 절차를 가진다. 각각의 디바이스 간의 통신은 UDP 프로토콜을 사용하여 대표적인 표준 블록 알고리즘인 AES 를 사용한다.

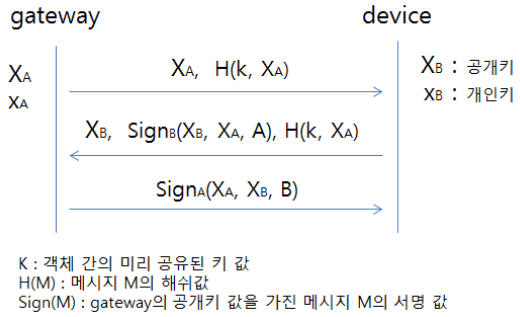

그림 2. 인증 메카니즘의 프로토콜

IV. 결 론

본 논문에서는 사물인터넷 환경 하에서의 유무선 통신이 상호 초연결성을 이루고 있으며, 이기종의 디바이스들의 연결로 인하여 보안상에 취약성을 내포하고 있다.

ACKNOWLEDGMENTS

This research was supported by Basic Science Research Program through the National Re-search Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (Number: 2015R1D1A09061435)

참고문헌

[1] Young-Jae Park and Young-Beom, Kim, “On the accuracy of RFID tag estimation functions, Journal of Information and Communication Convergence Engineering, vol.10, no.1, pp.33-39, 2012.

[2] Ioannis Andrea, Chrysostomos Chrysostomou and George Hadjjichristofi, “Internet of Things: Security Vulnerabilities and Challenges,” The 3rd IEEE ISCC 2015 International Workshop on Smart City and Ubiquitous Computing Applications, pp.180-186.

[3] Freddy K Santoso and Nicholas C H Vun, “Securing IoT for Smart Home System”, 2015 IEEE International Symposium on Consumer Electronics, pp.11-12.