한국컴퓨터정보학회 동계학술대회 논문집 제21권 제1호 (2013. 1)

IoT 통신 시스템 설계

장선주°, 김규석*
°*성균관대학교 전자전기컴퓨터공학과
e-mail:wkd4861@gmail.com°, tuffever@naver.com*

Design of the Communication System for IoT

Seon-Ju Jang°, Kyu-Seok Kim*
°Dept. of Electronic and Computer Engineering, Sungkyunkwan University
*Dept. of Electronic and Computer Engineering, Sungkyunkwan University

● 요 약 ●

현대사회는 기술의 발전으로 우리가 의식하지 않아도 모든 사물과 사람이 통신을 하는 시대로 바뀌고 있다. 이런 기술을 Internet of things 줄여서 IoT라고 부른다. IoT기술의 핵심은 인간의 개입 없이 모든 사물들이 상호 협력적으로 센싱, 정보 처리 등을 수행한다는 점이다. 본 논문은 IoT기술의 지속적인 발전과 함께 기술의 실현을 위해서 필요한 시스템을 제안한다.

키워드: 사물 인터넷(Internet of Things), 통신 시스템(Communication System), RFID

I. 서 론

IoT는 USN(Ubiquitous Sensor Network), M2M(Machine to Machine)과 비슷한 개념으로 2005년 ITU의 SPU(Strategic Planning Unit)의 보고서를 통해서 처음으로 소개되었다[1]. 일반적으로 사람의 관여 없이 사물 간에 이루어지는 통신을 뜻하는 것으로 IoT의 실현을 위해서는 모든 사물이 각각의 Identity를 가지고 있고 이를 네트워크를 통해 데이터를 수신하여 처리하는 컴퓨팅 능력을 지니고 있어야 한다[2]. 센서 기술을 이용하여 주변의 정보를 감지하고 이를 통해 주변 정보의 변화를 감지하고 네트워크에 연결되어 다양한 정보를 주고받는 네트워크를 형성하게 될 것이다. IoT의 실현을 위해서는 관련 기술의 발전과 더불어 새로운 환경에 맞는 프로토콜과 시스템의 연구가 필요하다. 본 논문에서는 IoT기술을 위한 시스템을 제안한다.

II. 관련 연구

1. IoT 기술

1.1 구성 요소

IoT 기술의 3대 구성요소는 인간, 사물, 서비스이다[1]. 인간은 사람 그 자체를 의미하며 사물은 휴대용기기, 컴퓨터, 전구 등의 유형의 사물과 특정 서비스를 담당하는 함수 등이 있으며 서비스는 어떤 목적을 위해서 제공되는 프로세스나 작업 명세를 의미한다.

1.2 주요 기술

IoT의 주요기술은 센싱 기술, 유무선 통신 및 네트워크 인프라 기술, 서비스 인터페이스 기술이 있다[1]. 센싱 기술은 센서나 RFID를 이용하여 온도나 습도 주변 환경에서 감지하는 정보를 감지하는 기능이고 통신 및 네트워크 인프라 기술은 WiFi, Bluetooth, 인터넷 등 인간, 사물, 서비스를 연결하는 모든 네트워크를 말한다[3]. 서비스 인터페이스 기술은 보안, 프로세스 관리, 센싱 데이터를 필요한 데이터만을 추출하여 가공, 처리하거나 저장하는 기술로 특정한 목적을 위한 응용 서비스를 제공하기위한 중개자 역할을 수행한다.

III. 본 론

1. 제안 시스템

1.1 시스템의 구조

제안 시스템은 그림 1과 같은 구조로 되어있다. 우선 각 디바이스들이 RFID칩을 가지고 있다고 가정한다. 디바이스를 관리하는 RFID 서버가 일정한 범위의 도메인 각각에 존재하고 새로운 디바이스가 도메인 안에 들어왔을 경우 RFID 서버를 통해서 인증절차를 거치게 된다. 인증 절차를 거친 디바이스는 도메인 안의 또 다른 디바이스들과 통신을 할 수 있다.

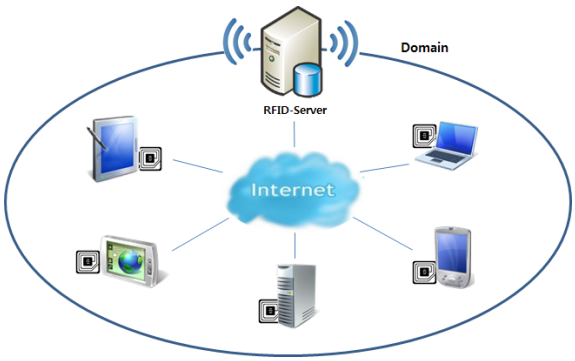

그림 1. 시스템 구조
Fig. 1. System architecture

1.2 시스템의 흐름

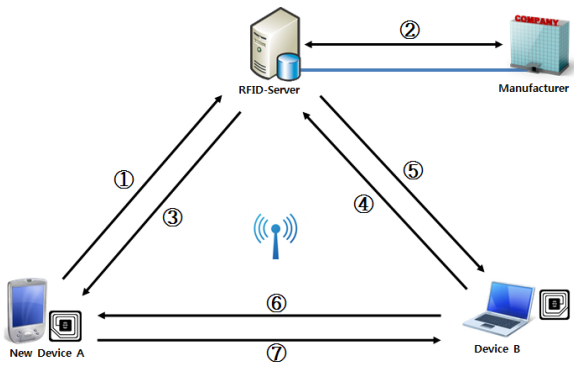

그림 2. 시스템 흐름
Fig. 2. Flow of the System

① 새로운 디바이스 A가 도메인 안에 들어오면 RFID 서버는 디바이스 A의 Tag안에 저장되어있는 데이터를 읽는다.

② RFID 서버가 디바이스 A의 Tag 데이터를 제조사에게 전송하면 제조사에서 정당한 디바이스인지 판단 후 RFID 서버의 공개키로 암호화한 디바이스 A의 Tag정보와 공개키를 RFID 서버에게 전송한다. RFID 서버는 디바이스 간의 통신을 위한 공개키를 관리하고 각 디바이스에 매칭되는 Tag의 정보를 저장한다.

③ RFID서버는 디바이스 A에게 인증확인 메시지를 전송한다.

④ 디바이스 B가 디바이스 A와의 통신을 위해서 RFID 서버에게 디바이스 A의 공개키를 요청한다.

⑤ RFID서버는 데이터베이스에서 인증된 목록 정보를 검색하여 디바이스 A의 공개키를 디바이스 B의 공개키로 암호화하여 전송한다.

⑥ 디바이스 B는 디바이스 A와 자신의 비밀 키를 생성하여 디바이스 A의 공개키로 암호화해서 전송한다.

⑦ 디바이스 A는 자신의 개인키로 복호화해서 비밀 키를 확인하고 통신을 위한 ACK메시지를 전송한다.

Ⅳ. 결 론

본 논문은 새로운 패러다임을 제시하는 IoT기술에 대하여 알아보고 IoT기술의 구현을 위해서 필요한 통신 시스템을 제안하였다. 최근 정보기술이 모든 사물과 통신할 수 있는 환경으로 바뀌면서 각 통신 방식과 프로토콜에 따라 적용할 수 있는 적절한 보안 기술의 연구가 시급하다. 우리는 본 논문을 바탕으로 제안 시스템에 적합한 보안 프로토콜을 설계하는 방향으로 연구를 진행할 것이다.

참고문헌

[1] Ho-won Kim, Dong-gyu Kim “Technology and Security of IoT” The Korea Institute of Information Security and Cryptology Vol. 22 No.1 pp.7-13, 2012.

[2] Sandra Dominikus and Jorn-Marc Schmidt. “Connecting Passive RFID Tags to the Internet of Things” IAIK, Graz University of Technology, 2011

[3] S. Dominikus, M. J. Aigner, and S. Kraxberger. Passive RFID Technology for the Internet of Things. In Workshop on RFID / USN Security and Cryptography, 2010.

[4] M. Hutter, M. Feldhofer, and T. Plos. An ECDSA Processor for RFID Authentication. In Workshop on RFID Security (RFIDsec 2010), June 2010.