한국컴퓨터정보학회 동계학술대회 논문집 제21권 제1호 (2013. 1)

RFID 기반 안전한 통신 프로토콜 설계에 관한 연구

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

A Study on Secure Communication Protocol based on RFID Technology

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

● 요 약 ●

우리가 일반적으로 인터넷을 많이 사용하는 디바이스는 컴퓨터가 대표적이었지만 최근에는 스마트 폰을 비롯해서 센서, 자동차, 카메라 등 각종 디바이스를 비롯한 다양한 사물들이 인터넷에 연결되고 있다. 각 구성요소 간의 보안 메커니즘 차이, 시스템의 다양성 문제로 새로운 프로토콜의 필요성이 대두되는 가운데 본 논문은 새로운 IoT환경에서 적용 가능한 통신 프로토콜을 제안한다.

키워드: 통신 프로토콜(Communication Protocol), 공개키(Public Key), RFID

I. 서 론

우리는 현재 주변의 모든 사물이 인터넷에 연결되고 지능적인 서비스를 제공하는 사물인터넷(Internet of things) 세상에 살고 있다[1]. 복합적이고 다양한 사물과 사람의 통신에서는 무선으로 전달되는 정보의 노출과 사생활침해와 같은 보안 문제가 발생할 수 있다. 본 논문에서는 다가오는 미래 인터넷 환경에 맞는 안전한 통신 프로토콜을 제안한다. 제안 프로토콜은 다양한 디바이스들이 통신하는 환경에서 악의적인 디바이스가 서비스를 제공하는 도메인에 들어오거나 도메인 안에 다른 디바이스들과 통신을 요청할 경우 서버를 통한 상호인증으로 악의적인 디바이스의 접근을 예방할 수 있다.

II. 본 론

1. 통신 프로토콜

제안 프로토콜은 키 분배, 디바이스 초기화, 디바이스 간의 통신 세 부분으로 나뉜다. 우선 디바이스의 인증을 위하여 제조사와의 통신을 위해 필요한 키를 획득하기 위한 키 분배 과정이다. 다음은 새로운 디바이스의 접근을 인식한 서버가 디바이스를 초기화하는 과정이다. 마지막으로 디바이스 간의 통신을 위하여 서버를 통한 키 분배가 이루어진다.

1.1 키 분배

그림 1은 제조사가 인증기관에 자신의 공개키와 개인 키 쌍을 인증기관에 등록하고 서버가 인증기관을 통해서 제조사의 공개키를 획득하는 과정이다.

① 제조사가 인증기관에 등록하기 위하여 자신의 공개키와 개인키 쌍을 제조사의 공개키로 암호화해서 전송한다.
② 인증기관은 자신의 개인키로 암호화한 제조사의 공개키와 아이디를 제조사에게 전송한다.
③ 서버가 자신의 아이디와 요청정보를 제조사에게 전송한다.
④ 제조사는 인증기관으로부터 받은 메시지를 서버에게 전송하고 서버는 인증기관의 공개키로 복호화해서 제조사의 공개키를 얻는다.

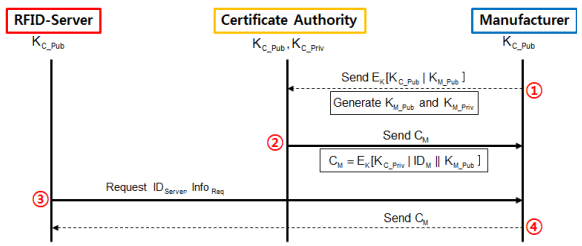

그림 1. 키 분배
Fig. 1. Key Distribution

1.2 디바이스 초기화

그림 2는 디바이스의 인증을 위하여 서버에 요청하는 과정으로 제조사로부터 정당한 디바이스임을 확인받는다.

① 서버가 태그를 읽고 태그 안에는 제조사의 비밀 키로 암호화된 태그 정보가 저장되어있다.
② 서버가 제조사와 자신의 비밀 키로 암호화한 자신의 공개키와 태그 정보를 전송한다.
③ 제조사는 서버의 공개키로 암호화한 태그의 정보를 전송한다.
④ 서버는 자신의 공개키로 암호화한 디바이스의 공개키를 태그에 저장한다.

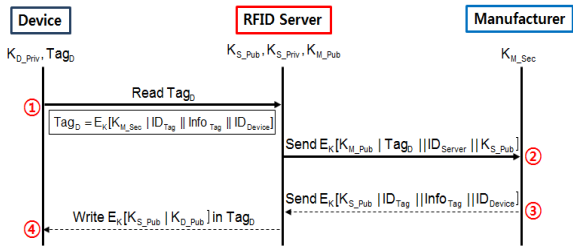

그림 2. 디바이스 초기화
Fig. 2. Device Initialization

1.3 디바이스 간의 통신

그림 3은 도메인 안의 디바이스 간의 통신을 위한 공개키 분배 과정이다. 서버로부터 받은 공개키를 이용해서 디바이스 간의 통신을 위한 비밀 키 분배를 위해서 사용한다.

① 디바이스B가 디바이스A와의 통신을 위해서 서버에게 자신의 아이디와 함께 요청메시지를 보낸다. 서버는 B의 태그의 정보를 읽어서 정당한 태그인지 확인 후 자신의 공개키를 전송한다.
② 디바이스B가 서버의 공개키로 디바이스A의 공개키를 요청하는 메시지를 전송한다. 서버는 디바이스 A의 태그를 읽어서 공개키를 디바이스B에게 전송하고 디바이스B는 통신을 위한 비밀키를 디바이스A의 공개키로 암호화해서 전송한다.
③ 디바이스A는 디바이스B의 공개키를 서버에 요청하고 서버는 디바이스A가 정당한 디바이스인지 확인 후 디바이스B의 공개키를 디바이스A에게 전송한다.
④ 디바이스B의 공개키를 받은 디바이스A는 자신의 개인키로 암호화한 승낙 메시지를 전송하고 디바이스B는 자신과 A의 비밀키로 암호화한 데이터를 전송한다.

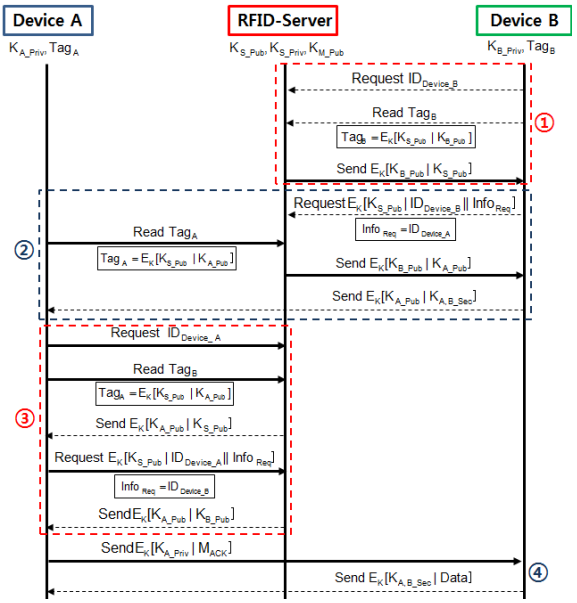

그림 3. 디바이스 간의 통신
Fig. 3. Communication between Device

III. 결 론

본 논문은 앞으로 다가올 미래 인터넷 환경에 필요한 통신 프로토콜을 제안했다. 미래 인터넷 세상에서는 무선을 이용한 데이터 통신이 지금보다 더 활성화 되는 만큼 본 논문을 바탕으로 다가오는 미래에 필요한 프로토콜과 보안에 대한 연구가 활발하게 이루어져야 할 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] Chatmon, Christy, Tri van Le, and Mike Burmester. Secure Anonymous RFID Authentication Protocols. Florida State University Technical Report, 2006.
[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.