한국컴퓨터정보학회 동계학술대회 논문집 제21권 제1호 (2013. 1)

모바일 RFID 기반의 안전하고 효율적인 도서대출시스템 설계

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

Design of the Secure and Efficient Library Circulation System based on Moblie RFID

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

● 요 약 ●

현대사회가 언제 어디서나 정보를 주고 받는 유비쿼터스 사회로 변화하면서 센싱기술, 통신기술, 서비스 기술 등을 이용하여 우리가 볼 수 있는 모든 사물을 사람과 통신 가능하게 해주는 IoT기술이 부각되고 있다.
IoT는 일반적으로 사람의 관여 없이 사물 간에 이루어지는 통신을 뜻하는 것으로 국내에선 개념적으로 USN기술과 흡사하다. 본 논문에서는 USN 분야 중 하나인 모바일 RFID 기술을 이용한 도서 대출 시스템을 제안하고 무선으로 정보를 주고 받는 모바일 RFID의 특성을 고려하여 태그와 리더 간의 인증 프로토콜을 제시한다.

키워드: 모바일 RFID(Moblie RFID), 보안 프로토콜(Security Protocol), 도서대출(Library Circulation)

I. 서 론

모바일 RFID(Radio Frequency Identification)는 휴대 가능한 장치에 RFID 리더를 탑재하여 사용자에게 다양하고 편리한 서비스를 제공한다[6]. 현재 국내에서는 주요 이동통신망 사업자인 SKT 및 KTF가 컨소시엄을 구축하여 모바일 RFID 시범사업을 추진해왔다. 구현 사례로는 양주 진품 정보제공 서비스, 관람 영화 정보제공 서비스, 관광 정보제공 서비스 등이 있으며 택시에 RFID 태그를 부착해서 모바일 단말기로 태그를 찍어서 지인에게 문자를 보낼 수 있는 택시 안심 서비스를 시행하기도 했다[8]. 본 논문에서는 모바일 RFID를 이용하여 기존 도서관 시스템에서 발생하는 문제들을 개선하고 다가오는 유비쿼터스 시대에 맞는 서비스를 제공하기 위한 시스템을 제안한다. 또한 개인정보의 악용, 개인의 위치 추적, 사생활 침해 문제 등 무선 통신에서 발생 할 수 있는 보안문제를 해결하기 위하여 사용자 인증 프로토콜을 제시한다. 본 논문 II에서는 모바일 RFID 구성 및 보안 요구사항에 대하여 알아보고 III에서 기존 시스템과 문제점, 제안 시스템의 구조와 프로토콜을 설명한다. 제안 프로토콜을 보안 요구사항에 따라서 분석 후 결론으로 마치겠다.

II. 관련 연구

1. 모바일 RFID 시스템

1.1 구조

모바일 RFID는 고유 식별 정보를 가지고 있는 태그, 태그를 읽어들이는 휴대용 리더기, 데이터를 저장하고 가공하는 RFID 서버로 그림 1과 같이 구성되어 있다. 본 논문에서 제안하는 시스템은 수동형 태그를 이용하는 것으로 태그가 인식가능한 일정거리 안에 들어오면 리더기에서 특정 주파수를 가지는 연속적인 전자파를 송출하게 된다. 태그와 리더기는 이 전자파를 이용하여 통신한다[8].

그림 1. 모바일 RFID 시스템 구조
Fig. 1. System Architecture of Moblie RFID

1.2 보안 요구사항

모바일 RFID의 구성요소인 태그, 리더, 서버에 대한 각각의 보안 위협 요소는 표 1과 같다.

표 1. 보안 위협 요소
Table 1. Security Threats

구성 요소	위협 요소
태그	- 태그 데이터 무단 조작 - 악의적인 리더의 접근
리더	- 불법적인 도청 - 악의적인 태그의 접근
서버	- 서버 공격 - 서버의 내용 획득

III. 본 론

1. 기존 시스템

1.1 시스템의 흐름

기존 도서관 대출 시스템은 아래 그림2와 같다. 우선 도서를 대출하기 위하여 해당 도서관의 홈페이지에서 원하는 도서를 검색한다. 대출 가능 여부를 확인 후 도서관으로 가서 청구기호에 따라 해당 책을 찾는다. 해당 책을 찾은 후 자동대출시스템을 이용하여 책을 대여한다.

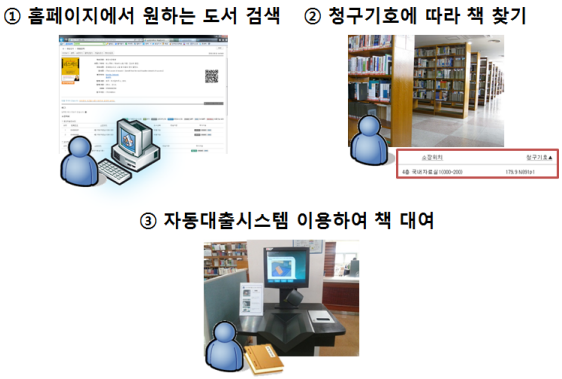

그림 2. 기존 시스템
Fig. 2. Existing System

1.2 문제점

기존 도서대출시스템에서 사용자가 해당 홈페이지에서 도서 검색을 했을 때 대출이 가능하더라도 실제로 도서관에 가서 찾아보면 없는 경우가 있다. 도서를 검색했을 당시에 해당 사용자에게 도서를 빌릴 권한을 줄 필요성이 있다. 또한 자동대출시스템을 이용하여 또 한 번의 절차를 걸쳐야하는 불편함이 발생한다. 모바일 RFID를 이용한다면 충분히 해결 할 수 있는 문제라고 생각한다.

2. 제안 시스템

2.1 시스템의 흐름

제안 시스템은 아래 그림3과 같다. 우선 도서를 대출하기 위하여 해당 도서관의 홈페이지에서 원하는 도서를 검색한다. 도서 대출 가능 여부를 확인하고 대출 가능 상태라면 도서대출 버튼을 클릭한다. 해당 도서는 승인 대기 상태로 바뀌게 된다. 도서관에 가서 청구기호에 따라 해당 도서를 찾는다. 해당 도서를 모바일 리더기로 읽히면 서비스 페이지가 로드되면서 해당 도서가 대출되었다는 메시지가 뜬다. 비로소 해당 도서가 대출된다.

그림 3. 제안 시스템
Fig. 3. Propose System

2.2 보안 프로토콜

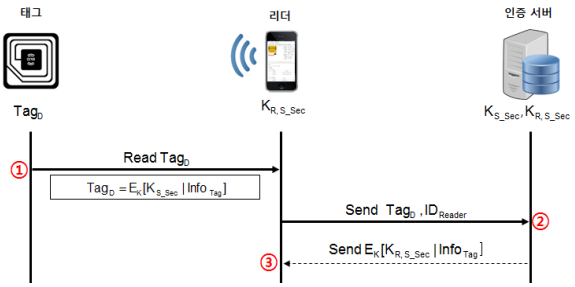

그림 4. 보안 프로토콜
Fig. 4. Security Protocol

사용자가 해당 도서를 대여할 경우 보안적인 측면에서 책에 부착된 태그가 정당한 태그가 맞는지 여부와 사용이 허락된 사용자가 맞는지 리더에 대한 상호인증이 필요하다. 다음 그림 4는 사용자 인증 프로토콜에 대한 내용이다. 제안하는 프로토콜은 리더와 인증서버가 서로 비밀 키를 가지고 있는 상태로 가정한다.

① 태그 – 리더기

$$Tag_D = E_K[K_{S\_Sec} \mid Info_{Tag}]$$

리더기가 태그에 저장된 식별 값을 읽는다. 식별 값에는 인증서버의 비밀 키로 암호화 된 태그의 정보가 저장되어있다. 이 식별 값은 인증 서버만이 풀 수 있는 서버의 비밀 키로 암호화 되어있

다. 악의적인 리더가 접근하여서 해당 태그의 정보를 읽을 수 없도록 하였다.

② 리더 - 인증서버

$$\text{Send } Tag_D, ID_{Reader}$$

리더는 태그로부터 읽어들인 식별 값을 인증서버에게 자신의 ID와 함께 전송한다. 리더가 인증서버에게 전송하는 이유는 해당 태그가 정당한 태그인지 확인받기 위해서이다. 악의적인 태그가 접근해서 잘못된 정보를 리더에게 제공하면 제안한 시스템의 처리 과정에서 문제가 생기게 된다.

③ 인증서버 - 리더

$$\text{Send } E_K[K_{R,S\_Sec} \mid Info_{Tag}]$$

인증서버는 자신의 비밀 키로 복호화해서 정당한 태그임을 확인하고 태그의 정보를 리더와 자신의 비밀 키로 암호화 해서 전송한다. 리더는 자신과 인증서버의 비밀 키로 복호화해서 태그의 값을 확인하고 해당 서비스 페이지로 로드된다. 악의적인 리더일 경우 인증서버와 리더의 비밀 키로 암호화 된 값을 복호화 하지 못하기 때문에 태그에 있는 정보를 읽지 못한다. 이로써 인증서버를 이용하여 태그와 리더가 상호인증 되어서 서로 정당한 구성요소임을 확인하게 된다.

3. 분석 및 평가

3.1 보안 프로토콜

제안한 프로토콜을 관련연구의 모바일 RFID 보안 요구사항에 따라서 분석한다.

① 태그

제안 프로토콜에서는 태그의 식별 정보 값을 인증서버의 비밀 키로 암호화 함으로써 정당한 리더기가 해당 정보를 읽을 수 있도록 하였으며 해당 태그의 정보를 임으로 조작하고 수정 할 수 없도록 보안 문제점을 개선하였다.

② 리더

제안 프로토콜에서는 악의적인 사용자가 가짜 태그를 만들어서 리더기로 접근하는 것을 방지하기 위하여 인증서버에게 인증을 받는 과정을 넣었으며 인증서버와 리더의 비밀 키로 암호화 된 태그의 정보를 전송함으로써 불법적인 도청을 방지할 수 있다.

③ 서버

해킹을 통하여 해당 서버를 공격해서 내용을 획득하거나 변조할 수 있다. 본 제안 방식에서는 태그와 리더 간 통신에서 서로를 인증하는 과정에 대하여 서술하였으므로 서버 보안을 위한 별도의 방법을 제시하지 않았다.

3.2 제안 시스템

제안 시스템은 기존의 도서대출시스템을 개선하여 불편한 점을 개선하였다. 또한 대출과정에서의 보안적인 문제를 해결하고자 보안 프로토콜을 제안하여 보다 안전하고 효율적인 시스템을 설계하였다. 하지만 프로토콜 상에서 인증서버와 리더가 같은 비밀 키를 가지고 있어야 하다는 한계점이 있다. 이 점을 개선하기 위해서는 리더와 인증서버 사이의 키 분배 프로토콜 설계를 고려해야 할 것이다.

Ⅳ. 결 론

본 논문에서는 수동형 태그와 모바일 RFID를 이용한 도서대출 시스템을 소개하였다. 제안 시스템은 인증 서버를 이용하여 태그와 리더 간의 상호 인증을 제공하는 프로토콜 설계를 통해서 사용자 위주의 도서대출 서비스를 제공하면서 동시에 안전하게 이용할 수 있는 시스템을 제안하였다. 우리는 앞으로 본 논문을 바탕으로 키 분배의 한계점과 서버 공격에 대한 보안 사항을 개선하는 프로토콜에 대한 연구와 제한된 시스템이 아닌 넓은 분야에 적용 할 수 있는 시스템의 설계에 대한 연구를 진행할 것이다. 현대 사회의 사람들은 점점 더 편리한 서비스 제공을 필요로 한다. 수요자 니즈에 따라 기술이 발달하면서 언제 어디서나 정보를 주고받는 유비쿼터스 사회로 변화하고 있다. 점점 현실로 다가오는 유비쿼터스 사회에 맞추어 사용자의 편리성과 효율성을 고려한 응용서비스을 발전시키고 여기에 맞는 보안 기술의 연구가 시급하다.

참고문헌

[1] Feldhofer, etcs, “Strong authentication for RFID systems using the AES algorithm,” Cryptographic hardware and embedded systems”, CHES 2004, v.31, n.56, pp.357-370, 2004

[2] Maier, M.W., and Rechtin E. The Art of Systems Architecting, 2nd Edition. CRC Press, London, 2000

[3] Jun Zhou; Yongjun Xu; Xiaowei Li; Inst. “Reconfigurable and scalable security module of active RFID for security-sensitive applications” Information Management and Engineering (ICIME), 2010 The 2nd IEEE International Conference, pp.135-140, April 2010

[4] Gildas Avoine and Philippe Oechslin "RFID Traceability : A Multilayer Problem", Financial Cryptography, March 2005.

[5] Boyeon Song, and Chris J Mitchell, “RFID Authentication Protocol for Low-cost Tags,” ACM Conference on Wireless Network Secrity(WiSec ‘08), March, 2008.

[6] Taeyang Eom, Jeong-Hyun Yi “Performance Evaluation of Authentication Protocol for Moblie RFID Privacy” The Korean Institute of Communications and Information Sciences 11-6 Vol. 36 No.6 pp.618-630, 2011.

[7] T. Li, G. Wang. “Security Analysis of Two Ultra-Lightweight RFID Authentication Protocols,” Proceeding of IFIP SEC 2007, May 2007.

[8] Kim Hyung Jun “Mobile Plus RFID” The Korean Institute of Communications and Information Sciences 103-108 Vol. 24 No.6 pp.46-53, 2007.