이동형 리더를 사용하는 RFID시스템의 보안 프로토콜 설계

장봉임 · 김창수 · 정회경

배재대학교

Design of Security Protocol for RFID System using Mobile Reader

Bong-Im Jang · Chang-Su Kim · Hoe-Kyung Jung

Paichai University

E-mail : jjang@pcu.ac.kr

요 약

최근 모바일 통신장치의 사용이 증가함에 따라 사물에 부착된 태그를 인식하기 위한 이동형 리더기의 사용도 증가하고 있다. 이에 따라 그동안 RFID 시스템의 취약점으로 대두되었던 리더와 태그 사이의 보안 문제점 뿐만 아니라 리더와 백엔드 서버 사이의 보안 문제가 발생한다.따라서 본 논문에서는 이동형 리더와 백엔드 서버 사이의 보안 취약점을 해결하기 위해 해쉬함수를 이용한 효율적인 인증 프로토콜을 제안한다.

ABSTRACT

Recently as increasing the use of mobile communication devices the use of mobile readers for recognition tag attached to objects is also increasing. Accordingly, meantime, that gives rise to the vulnerability of RFID systems between reader and tag security issues, as well as security issues between the reader and the back-end server will occur. In this paper between the reader and the back-end server to security vulnerabilities efficient authentication protocol using the hash function is proposed.

키워드

RFID, Mobile Reader, Hash Function, Authentication Protocol

Ⅰ. 서 론

최근 사물의 인식을 위해 그 사용이 증가되고 있는 RFID 시스템에 대한 많은 연구가 진행되고 있다. 특히 RFID 시스템의 취약점인 프라이버시 침해 등 보안에 대한 연구[1,2]가 활발하다.

또한 최근 모바일 통신장치의 다양화로 휴대전화 등의 이동형 기기에 리더기가 적용되어 태그 정보를 검색하는 이동형 리더의 사용이 증가하고 있다. 이러한 이동형 리더의 사용은 그동안 RFID 시스템의 보안 문제로 인식되지 않던 리더와 백엔드 서버 사이의 보안 취약점을 발생시킨다

그러나 현재까지의 연구는 일반적인 RFID 시스템 구성 환경에서의 보안 문제로 대두되는 태그와 리더 사이의 통신 취약점에 관한 연구가 대다수이다.

따라서 본 논문에서는 리더와 백엔드 서버 사이의 보안에도 안전한 태그 인증 프로토콜을 제안한다.

Ⅱ. 관련연구

현재 여러 산업 분야에서 RFID 시스템의 사용이 증가함에 따라 태그 인증을 위한 다양한 기법들이 제안되고 있다. 특히 수동형 태그 사용을 위한 해쉬 함수[3,4] 및 AES 암호화 기법[5,6] 등의 가벼운 연산기법들이 주로 연구되고 있다

그러나 현재까지의 연구는 고정형 리더를 사용하는 시스템에 대한 연구가 대다수로 이동형 리

더를 사용하는 시스템 환경에서의 보안위협 문제 해결을 위한 개선된 프로토콜이 요구된다

III. 비공개 코드를 이용한 태그 인증

본 논문의 제안시스템에서는 단순히 태그 데이터를 벡엔드 서버로 전달하던 기존의 고정형 리더 기반의 프로토콜을 개선하여 리더에서의 태그 인식 검증 과정을 강화하는 비공개 코드를 이용한 태그 상호 인증 프로토콜을 제안한다.

제안 기법의 태그 인증 세부 실행 과정은 그림 1과 같다.

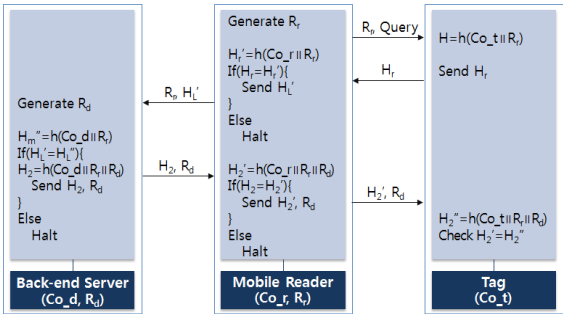

그림 1. 제안 프로토콜의 실행과정

첫째, 태그의 존재가 인식되면 리더는 자신이 생성한 난수 R_r을 태그에게 전송한다.

둘째, 태그는 리더의 난수와 자신의 비공개 코드값 Co_t를 연접 해쉬 함수 처리한 값 H의 오른쪽 n비트 값 H_r을 리더에게 전송한다.

셋째, 리더는 자신이 저장하고 있던 비공개 코드값 Co_r을 자신의 난수 R_r과 연접 해쉬 함수 처리한 연산 값 H_r'와 H_r을 비교 검증한 후, 값이 일치하면 H'의 왼쪽 n비트값 H_l과 R_r을 벡엔드 서버로 전송한다.

넷째, 벡엔드 서버는 난수 R_d를 생성한 후, 자신이 저장하고 있던 비공개 코드값 Co_d를 R_r과 연접 해쉬 함수 처리하여, 전송 값의 정당성을 확인한다. 그 결과, 값이 일치하면 리더로부터 전송받은 R_r과 자신이 저장하고 있던 비공개 코드값 Co_d, 자신의 난수 R_d를 연접 해쉬 함수 처리한 연산 값 H_2와 R_d를 리더에게 전송한다.

다섯째, 리더는 앞에서와의 동일한 방법으로 전송 값의 정당성을 확인한 후, H_2'와 R_d를 태그에게 전송한다.

마지막으로 태그는 H_2'와 H_2''값을 비교 검증한 후 인증절차를 마친다.

IV. 성능분석

본 논문에서 제안한 이동형 리더 사용을 위한 태그 상호 인증 프로토콜의 보안성 분석결과, 제안 기법은 매회 리더와 벡엔드 서버에서 난수를 발생시키고, 난수와 비공개 코드값을 해쉬 함수 처리 한 값만 전송 데이터로 이용함으로써 도청의 위협이나 재전송 공격, 스푸핑 공격으로부터 안전하다.

특히 이전 기법에서는 제시되지 않았던 리더에서의 데이터 검증 절차를 추가하여 이동형 리더 사용의 보안 안정성을 확보한다.

V. 결 론

최근 RFID 시스템의 사용에 있어 이동형 리더기의 사용이 증가되면서, 기존에는 안전한 통신 채널로 인식되던 리더와 벡엔드 서버 사이의 보안 위협 문제가 대두된다. 따라서 본 논문에서는 이동형 리더 사용 환경에서 발생될 수 있는 보안 위협을 해결하기 위하여 비공개 코드를 해쉬 함수 처리하는 방법을 기반으로 한 리더에서의 전송 데이터 검증 절차 강화 기법을 제안하였다.

분석결과, 제안 시스템은 이동형 리더 사용의 취약점인 프라이버시 침해 및 보안상의 위협으로부터 안전성을 확보하였다.

참고문헌

[1] Hung-Yu Chien, Chen-Wei Huang, "A Light weight Authentication Protocol for Low-Cost RFID", Journal of Signal Processing Systems, 59, pp.95-102, 2010.

[2] Woo-Sik Bae, Shin-Hyeong Choi, Kun Hee Han "RFID Security Authentication Protocol for the Ubiquitous Environment", Korea Society of Computer Information, 12(4), pp.69-75, 2007.

[3] Stephen A. Weis, Sanjay E. Sarma, R. L. Rivest, and D. W. Engels, "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems", *Security in Pervasive Computing 2003*, LNCS 2802, pp.201-212, 2004.

[4] 오세진, 윤태진, 이창희, 이재강, 정경호, 안광선 "개선된 해시함수와 CRC 코드 기반의 RFID 상호인증 프로토콜", 한국통신학회논문지, 37C(02), pp.132-139, 2012.

[5] B. Toiruul, K. Lee, "An Advanced Mutual-Authentication Algorithm Using AES for RFID Systems," IJCSNS, Sep. 2006.

[6] 이남기, 장태민, 전병찬, 전진오, 유수봉, 강민섭, "AES 암호 프로세서를 이용한 강인한RFID 인증 프로토콜 설계", 한국정보처리학회 논문집, 15(2), pp.1473-1476, 2008.