JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지(J. Korea Inst. Inf. Commun. Eng.) Vol. 18, No. 7 : 1634~1642 July. 2014

OTP를 이용한 모바일 RFID 상호인증 프로토콜

성종엽 · 이상덕 · 류창주 · 한승조*

Mutual Authentication Protocol using One Time Password for Mobile RFID System

Jong-yeop Sung · Sang-duck Lee · Chang-ju Ryu · Seung-jo Han*

Department of Information and Communication Engineering, Chosun University, Kwangju 501-759, Korea

요 약

모바일 단말기와 RFID(Radio Frequency Identification)통신 기능을 결합한 모바일 RFID는 객체에 대한 정보 확인 및 관련 응용 서비스를 쉽게 이용할 수 있는 기술이다. 모바일 RFID는 기존 RFID와 마찬가지로 보안 기능이 취약해 많은 보안적 위협에 노출되어있다. 본 논문에서는 통신에 참여하는 각 요소들이 생성한 임의의 난수와 대칭키 암호화 알고리즘 OTP(One time Password)를 이용하여 보다 강력한 보안성을 갖는 상호인증 프로토콜을 제안한다. 제안한 프로토콜은 매 인증시 메시지가 변경되기 때문에 기존 프로토콜과 비교하여 스푸핑 공격 및 재전송 공격 등에 안전하다.

ABSTRACT

Mobile RFID system, that consists of the existing RFID reader mounted on the mobile devices such as smartphones, is able to provide the users a variety of services and convenience. But security of mobile RFID system is too weak like the existing RFID system. In this paper, the mobile RFID mutual authentication protocol with high level of security is proposed to overcome the troubles such as cryptographic protocols in the existing RFID system responding with the same value in every authentication procedure and the exposure in the exchange of messages. The proposed protocol exchanges messages unexposed by using the random numbers generated in the mutual authentication between the tag and the reader and making numbers coded with the symmetric key. Besides, the protocol uses the mutual authentication utilizing OTP by considering the characteristics of the reader embedded in mobile devices in the mutual authentication process between the reader and the server. Because changed message in every authentication, which produces safe from spoofing attacks and replay attacks, etc.

키워드 : Mobile RFID, RFID, 상호인증, 프로토콜

Key word : Mobile RFID, RFID, Mutual Authentication, Protocol

접수일자 : 2014. 03. 17 심사완료일자 : 2014. 04. 09 게재확정일자 : 2014. 04. 22

* **Corresponding Author** Seung-jo Han(sjhanb@chosun.ac.kr, Tel:+82-62-230-7247)
Department of Information and Communication Engineering, Chosun University, Gwangju 501-759, Korea

Open Access http://dx.doi.org/10.6109/jkiice.2014.18.7.1634 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

유비쿼터스 환경이 세상에 주목을 받기 시작하면서 많은 기술들이 개발되는 가운데 무선통신 기술을 사용한 RFID는 이미 국가 전반에 걸쳐 정부, 기업, 학계를 통해 많은 연구가 이루어지고 있으며, 이에 따른 개발 및 적용 사례들이 발표되고 있다. 더욱이 초기에 적용된 분야를 넘어서 유통, 물류, 의료, 자동차, 농·축산, 군사 그리고 관광산업에 이르기까지 적용분야가 확대되고 있으며, 서비스업 전체 모든 분야에 있어서 핵심적인 역할을 할 것으로 기대된다[1].

RFID 시스템과 마찬가지로 휴대폰을 비롯한 PDA 및 태블릿 PC 등 모바일 단말기는 다양한 멀티미디어 정보 및 인터넷 서비스를 사용자에게 제공하는 현대 정보 사회의 필수품이라 할 수 있다.

모바일 RFID 기술은 모바일 단말기와 RFID 통신 기능을 결합함으로써 관심 있는 객체에 대한 상세 정보 확인 및 관련 응용 서비스를 쉽게 이용하는 기술이다. 구체적으로는 RFID 통신, 이동통신 및 네트워크 인프라, 그리고 정보처리 기술이 서로 유기적으로 결합되는, 대표적인 IT융합 기술이라 할 수 있다.

모바일 RFID 서비스 환경에서는 사물단위의 정보화가 이루어져 보다 신뢰성 있는 정보 전달이 가능해 질 것이지만, 현재의 모바일 RFID 기술은 기존 RFID 기술과 마찬가지로 보안 기능이 매우 취약해 태그(Tag)의 변조, 위장 리더, 서비스 거부 공격 등 수많은 위협에 노출되어 있다. 또한 기능적으로 가장 중요한 것은 개인 사용자가 제품의 정보를 정확하고 신뢰성 있게 얻는 것이며, 보안 측면에서 가장 중요한 것은 제품의 안전한 제공 및 개인 프라이버시 보호이다.

모바일 RFID는 특성상 태그와 리더(Reader), 서버(Server)가 무선통신을 이용하여 데이터를 교환하기 때문에 각종 공격을 받을 수 있다. 안전한 데이터 교환을 위하여 무선 네트워크에서 사용되는 보안 프로토콜을 적용시키는 것을 고려해볼 수 있으나, RFID의 제한적인 환경에 적용하기 힘든 것이 현실이다.

본 논문에서는 각 통신 요소들이 생성한 임의의 난수와 대칭키 암호화 알고리즘, OTP를 이용하여 보다 강력한 보안성을 갖는 상호인증 프로토콜을 제안한다.

Ⅱ. 모바일 RFID 시스템

모바일 RFID 시스템은 모바일 휴대 단말기에 RIFD 태그를 인식 할 수 있는 리더를 내장하거나 장착한 것을 말하며, 모바일 단말기를 가진 사람은 언제, 어디서나 RFID 태그가 부착된 물품의 RFID 식별코드를 획득할 수 있는 기술이다[2].

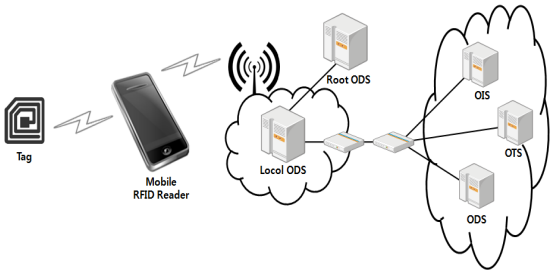

그림 1. 모바일 RFID 시스템
Fig. 1 Mobile RFID System

모바일 RFID 시스템은 식별코드를 가지고 있는 태그, 휴대용 단말기에 내장되거나 장착된 리더, 그리고 리더로부터 전송 받아 태그의 정보를 처리하는 응용서비스를 갖춘 서버로 구성된다. RFID 시스템은 기존 바코드 시스템과 비교했을 때 원거리에서 직접적인 접촉 없이 동작 할 수 있으며 시야가림 상태에서도 통신이 가능하다는 장점을 가진다. 또한 빠른 판독 속도는 동시에 많은 상품의 처리를 가능하게 하며 태그별 고유번호를 통한 인식으로 많은 개체들 속에서도 원하는 개체의 식별을 가능하게 한다.

모바일 RFID는 무선네트워크를 이용하여 정보를 전송한다는 편리함을 가지고 있지만 정보나 보안에 대해 취약한 점을 가지고 있다. 여러 가지 공격들에 대한 취약점들은 개인이나 기업의 심각한 보안 문제를 발생시킨다. 또한 RFID 시스템에서 태그는 개인정보가 포함된 경우가 아니라도 어떤 시스템과 결합 하느냐에 따라 개인정보와 연계될 수 있는 점에서도 프라이버시 침해 가능성이 제기 될 수 있다. 이러한 문제점은 기존 RFID 시스템에서 태그와 리더 사이의 무선통신을 이용한 데이터 교환에 있었으며, 모바일 RFID 시스템에서는 리더의 특성상 태그와 리더, 서버의 데이터 교환이 모두 무선으로 이루어져 있기 때문에 통신에 참여하는 모든 요소들이 정당한 사용자에 의한 것인지 검증 할 필요가 있다.

Ⅲ. 관련연구

3.1. 기존 RFID 시스템 보호 기법

기존의 RIFD 시스템의 보호 기법으로는 물리적 보호 기법과 암호학적 인증 기법으로 나눌 수 있으며, 물리적 보호 기법으로는 태그의 기능을 정지시켜버리는 Kill 태그[3] 기법, 태그 자체에 그물(Cage)이나 박막을 입혀 무선주파수가 침투하지 못하도록 하는 Faraday Cage 기법, 방해 신호 발생장치를 이용한 Active Jamming 기법[4] 등이 있다. 암호학적 인증 기법으로는 공개키, 대칭키, 해시함수를 이용하여 각 노드간 통신 과정에서 노출되는 정보를 암호화함으로써 악의적인 공격자로부터 시스템을 보호하는 방식으로 해시기반 인증기법에는 해시락, 변형된 해시락, 해시체인, 해시기반 ID 변형 기법 등이 있으며, 대칭키 기반 인증기법으로 Feldhofer의 프로토콜[5], Gen2기반 경량화 프로토콜에는 Duc의 프로토콜[6]과 Chien-Chen의 프로토콜[7] 등이 있다.

3.1.1. Feldhofer의 프로토콜

M. Feldhofer은 32비트 대칭키 암호 알고리즘인 AES를 RFID에 적합하면서 효율적인 저전력 AES로 설계하고 안전한 상호 인증을 위한 프로토콜을 제안하였다.

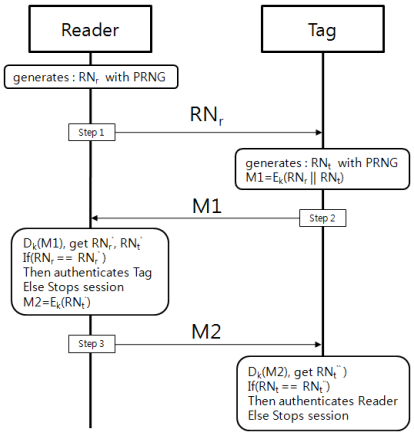

그림 2. Feldhofer's 프로토콜의 3-way 인증 방식
Fig. 2 3-way authentication method of Feldhofer's Protocol

Feldhofer의 프로토콜은 태그와 리더간 통신 메시지를 AES 대칭키 암호 알고리즘을 사용하여 정보 노출을 방지하는 기법으로 해시함수나 공개키 기반의 큰 문제인 게이트 제약사항을 해결하였다. 또한 태그와 리더가 서로 공유한 비밀키에 의해 메시지를 암호화하고 서버의 동작 없이 상호 인증을 수행한다.

각종 공격에 대해서는 태그와 리더간 메시지 전달에 있어서 태그와 리더가 각각 난수를 사용하며, 이를 비밀키 K를 이용하여 암호화 하여 전송하기 때문에 도청 공격과 재전송 공격에 안전하다. 하지만, 첫 번째 단계에서 리더가 태그에게 전송하는 메시지 RN_r은 아무런 암호화과정 없이 전송되므로 공격자는 이를 통해 재전송공격을 시도 할 수 있다. 공격자는 첫 번째 단계에서 리더가 태그에게 RN_r을 도청하여 이를 정당한 리더로 위장하여 태그에게 RN_r을 전송, 태그로부터 메시지를 받아 암호문의 분석이 가능하다. 첫 번째 단계에서 RN_r을 주고받으며 리더에서 태그를 인증하지만 공격자가 특정 태그에 대하여 일정한 메시지를 계속 전송하게 된다면 태그의 메시지가 암호화 되어 있더라도 같은 메시지를 계속 전송하므로 위치 추적 공격에 취약하다.

3.1.2. Duc의 프로토콜

Duc은 Gen2에서 제공하는 PRNG 함수와 CRC만을 사용하여 상호 인증을 수행하는 동기화 기반의 프로토콜을 제안하였다. 태그와 서버는 동일한 PRNG 함수를 사용하여 세션키를 생성하게 된다.

Duc 프로토콜은 EPC Class-1 Gen 2에서 제공하는 PRNG와 오류검사 함수인 CRC만을 사용하여 상호인증을 하는 기법이다. 리더의 Query 요청에 대한 응답으로 태그 난수 r을 생성하여 도청공격에 의한 프라이버시를 방지한다. 또한 통신 데이터에 대한 무결성 검사를 위해 해시함수를 대신하여 CRC를 사용한다.

메시지 M_1, M_2를 전송함에 있어서 세션키 K_i를 사용하여 XOR 연산을 하기 때문에 CRC 함수의 일방향성 약점을 해결하고 도청을 방지한다. 하지만 마지막 단계의 “End Session” 명령어를 획득하여 서버와 태그에게 재전송공격을 시도 할 수 있다. 또한 정당한 리더로 위장하여 서버와 태그에게 스푸핑 공격을 시도 할 수 있다. 태그와 서버에서 사용되는 비밀 정보인 EPC, PIN 키 값들은 고정되어 있기 때문에 이전에 이루어졌던 통신들에 대한 정보 역시 노출 가능성이 있다. 공격자가 태그의 현재 정보 M_1, M_2, r을 알게 되었을 때 이를 이용하여 이전 정보 EPC, PIN, K_i의 획득이 가능하므로

이동 경로를 추측할 수 있다. 따라서 이 기법에서는 전방향 안전성을 만족하지 못하는 문제가 있다.

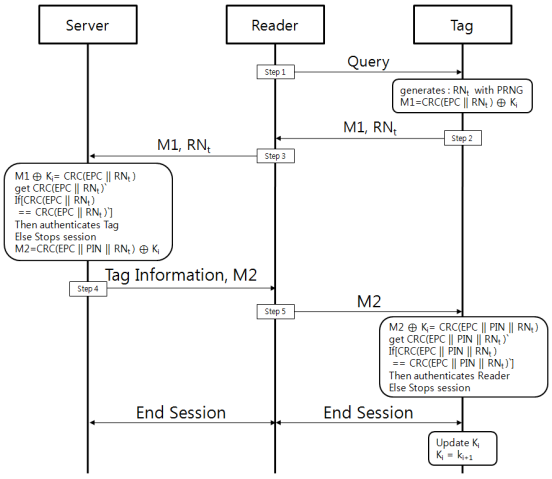

그림 3. duc의 프로토콜
Fig. 3 duc's Protocol

마지막 단계의 “End Session” 명령어는 세션에서의 동기화를 유지하기 위해 태그와 서버의 세션키를 업데이트하여 동일한 세션키를 생성하게 되는데, 이때 서비스 거부공격을 시도한다면, 태그와 서버 간에 비동기화 문제가 발생하게 되고 이로 인해 인증이 실패한다.

3.1.3. Chien-Chen의 프로토콜

Duc가 제안한 기법들을 향상 시킨 Gen2 기반에서 보다 강력한 프라이버시 보호 기법으로 서비스 거부 공격을 통한 비 동기화 문제를 개선하였다. Chien-Chen의 프로토콜은 Duc의 프로토콜과 같이 PRNG와 CRC를 통해 상호 인증을 수행하며 서버는 태그와 상호인증을 위한 많은 데이터를 소유하고 있다.

Chien-Chen의 프로토콜은 Duc의 프로토콜을 개선하여 각각 K_{old}, K_{new} 2개의 인증키와 접근키를 사용한다. K_{new}는 현재의 갱신된 키로서 태그를 인증하는데 사용하지만 비동기화 문제로 인증이 실패하는 것을 방지하기 위해 K_{old}를 사용한다. 따라서 두 개의 키는 서비스 거부 공격을 통한 비동기화 문제를 방지한다. 하지만 비동기화 문제를 완전히 해결하고 있지는 못하고 있으며, 효율적인 측면에서 서버는 특정 태그를 인증하기 위해 많은 데이터를 소유하고 있으므로 모든 태그에 대하여 전수조사를 해야 한다. 따라서 오버헤드로 인해서 비효율적이다.

Chien-Chen의 프로토콜에서 메시지 M_1, M_2는 세션키 K_i와의 XOR 연산을 하기 때문에 CRC 함수의 값이 숨겨져 있어 도청 공격으로부터 안전하다. 공격자는 i번째 세션에서 메모리에 저장된 K_i, P_i, ECP_x 값을 알아낼 경우, 이전 i번째 세션에서 1, 2단계에서 도청한 M_1, N_R, N_T 값들과 함께 $M_1 \oplus CRC(EPC_x \| N_R \| N_T)$을 계산하여 인증키 K_i를 알 수 있다. 또한 N_R, N_T값을 획득한다면, 새로운 태그를 통해 거짓 M_1을 생성하여 재전송 공격을 시도 할 수 있다.

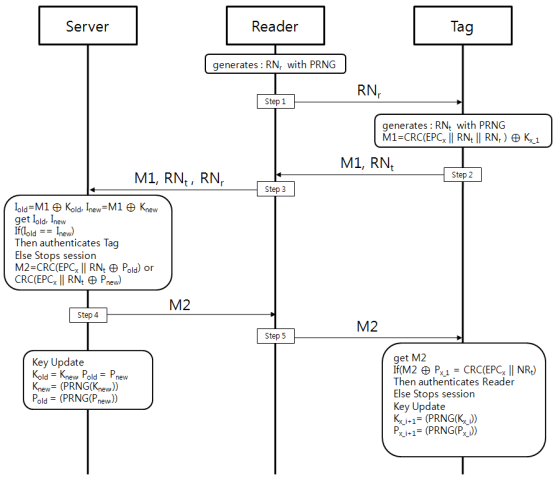

그림 4. Chien-Chen의 프로토콜
Fig. 4 Chien-Chen's Protocol

재전송공격과 마찬가지로 인증키 K_i와 N_R, N_T값을 통해 정당한 태그인 것처럼 위장하여 스푸핑 공격을 시도할 수 있다. Chien-Chen의 프로토콜은 1, 2, 4 단계에서 메시지는 태그와 리더에서 생성한 난수 N_T, N_R로 인해 태그 및 리더의 출력 값이 일정하지 않으므로 기본적으로 위치 추적에 안전하다고 분석하였다. 하지만 공격자가 K_i-PRNG(K_{i-1})을 계산할 수 있고 그 결과 i번째 세션의 인증키와 이전 i번째 세션의 인증키의 연계성을 찾을 수 있다. 이는 전방향 안정성을 만족하지 못하며 위치추적도 가능하다.

Ⅳ. 제안하는 프로토콜

본 장에서는 기존의 RFID 시스템을 분석한 취약점으로 인해 발생하는 문제점들로부터 안전하고 효율적인 기법을 프로토콜로 제안한다. 대칭키 암호화를 이용하여 메시지의 직접 노출을 막고, 난수를 사용하여 매 세션 다른 값을 사용하였다.

표 1. 용어 정리
Table. 1 Term List

용어	내용
$Query_T$	태그 응답 요청 질의
R_R	리더에서 생성한 임의의 난수
TagID	태그 고유의 ID
SK	대칭키
PRNG	난수 발생기
CRC	CRC 전송코드
$E_{SK}(*)$	대칭키를 이용한 암호화 연산
$D_{SK}(*)$	대칭키를 이용한 복호화 연산
⊕	eXclusive OR
‖	연접 연산자

R_R은 64bit로 리더에서 생성성한 임의의 난수이며, TagID는 RFID 태그의 고유의 식별 값으로 서버의 데이터베이스에 저장된 태그 ID를 의미한다. 태그와 리더는 64bit의 동일한 CRC 발생코드를 생성하며, OTP는 S/KEY 알고리즘[8]을 사용한다. 제안하는 프로토콜은 다음과 같은 전제조건과 가정에서 동작이 가능하다.

① 태그는 리더로부터 전원을 공급받는 수동형 태그이다.
② 태그와 리더는 난수를 생성할 수 있는 난수 발생기를 가지고 있으며 동일한 CRC 발생코드를 사용한다.
③ 태그와 리더, 서버는 AES 암호화 알고리즘 연산이 가능하며, 사전에 대칭키 SK를 안전한 방법으로 공유하고 있다.
④ 리더와 서버는 S/KEY 알고리즘의 연산이 가능하다.

4.1. 태그-리더 인증 과정

Step 1에서는 초기 질의 단계로 리더가 태그에게 $Query_T$, M_1을 전송한다. 이 때 M_1은 리더에서 생성한 임의의 난수 R_R에 CRC발생코드를 연접한 메시지를 대칭키 암호화하였다. 태그와 리더는 무선으로 서로 메시지를 교환하기 때문에 난수 R_R를 직접 전송하지 않고 대칭키 암호화 하여 전송함으로써 도청공격으로부터 노출을 방지할 수 있고, 매 인증 요청 시 랜덤한 값을 갖기 때문에 완전 암호계 판정법을 만족한다.

Step 2에서 태그는 리더로부터 전달받은 메시지 M_1을 복호화 하여 $R_R \| CRC$를 획득하고, CRC 발생코드로 나눠 획득한 메시지가 정당한 리더로부터 전송된 것인지 판별한다. 나머지가 0이 아니면 세션이 종료되며, 나머지가 0이면 태그는 리더를 인증한다. 리더를 인증한 태그는 자신의 고유 식별 정보인 TagID와 리더로부터 전달받은 R_R을 XOR 하고 CRC 발생코드와 연접하여 대칭키 암호화한 메시지 M_2를 리더로 전송한다.

Step 3에서 리더는 태그로부터 전송 받은 메시지 M_2를 복호화 하여 $TagID \oplus R_R \| CRC$를 획득하고, $TagID \oplus R_R$을 CRC 발생코드로 나눠 획득한 메시지가 정당한 태그로부터 전송된 것인지 판별한다. 나머지가 0이 아니면 세션이 종료되며, 나머지가 0이면 리더는 태그를 인증한다. 리더가 태그를 인증함으로써 리더와 태그는 상호인증이 이루어진다.

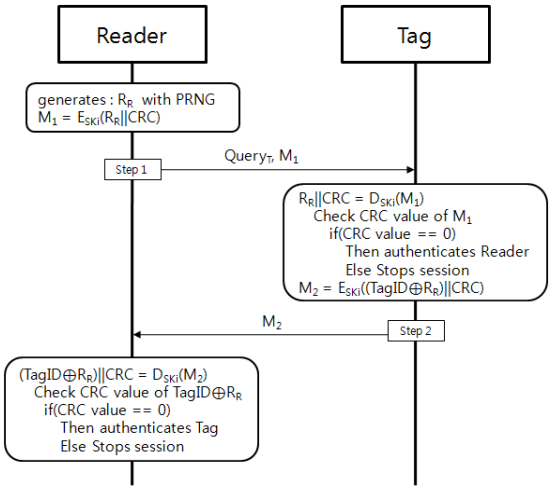

그림 5. 태그 리더간 인증 과정
Fig. 5 Authentication Process between Tag and Reader

그림 5는 제안하는 프로토콜의 태그 리더간 상호 인증 과정이며 Step 1부터 Step 3까지의 과정을 설명한 것이다. Step 2의 과정을 통해 태그는 리더를 정당한 사용자인지 CRC 발생코드를 이용하여 판별하고, CRC 판별코드로 나누었을 때 나머지가 0이 아니면 인증이 비정

상 종료된다. Step 3의 과정에서는 리더가 동일한 방식으로 태그를 정당한 태그인지 판별한다. 교환되는 메시지는 각각 리더에서 임의로 생성한 난수를 포함하고 있어 불구분성을 만족하고, 대칭키 암호화 되어있어 기밀성을 만족한다. 또한 CRC 발생코드를 이용하여 리더의 난수를 판별하기 때문에 전송되는 메시지의 무결성을 만족한다.

4.2. 리더-서버 인증과정

리더 서버간 인증과정은 리더가 모바일 기능을 갖춘 단말의 특성을 고려하였으며, 사용자 인증을 위한 OTP 시스템은 S/KEY 방식을 기반으로 구현 한다.

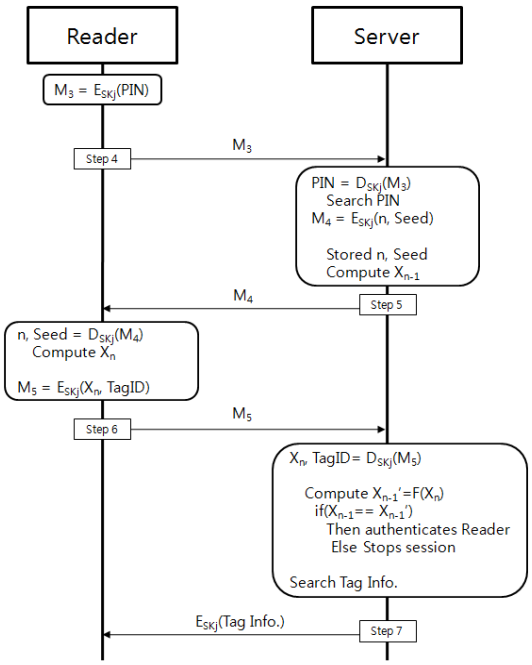

그림 6. 리더 서버간 인증 과정
Fig. 6 Authentication Process between Reader and Server

Step 4에서 태그와 상호인증을 마친 리더는 모바일 단말의 고유 식별정보인 PIN을 암호화한 메시지 M3를 서버에게 전송한다.

Step 5에서 서버는 리더로부터 전송받은 메시지 M_3를 복호화 하여 PIN을 획득하고, PIN에 해당하는 n과 seed 값을 암호화 하여 M_4로 하는 메시지를 리더에게 전송한다. 또한 n과 seed 값을 자신의 시스템에 저장하고, X_{n-1}값을 계산한다.

Step 6에서 리더는 서버로부터 전송받은 M_4를 복호화하여 n과 seed값을 획득하고, 획득한 정보를 바탕으로 새로운 OTP 번호 X_n을 산출한다. 리더는 X_n과 TagID를 서버에게 암호화 하여 전송한다.

Step 7에서 서버는 리더로부터 전송받은 메시지 M_5를 복호화 하여 X_n, TagID을 획득하고, 획득한 X_n을 단방향 해시 함수에 n-1번 수행한 값과, 다섯 번째 단계에서 수행한 값과 비교하여 일치하면 인증하여 태그의 정보를 검색해 리더에게 전달한다.

그림 6은 제안하는 프로토콜의 리더 서버간 인증 과정이며, S/KEY방식을 이용한 OTP 인증 과정을 통해 리더와 서버가 상호 인증한다. 인증을 마치면 서버는 Step 6에서 전달받은 TagID를 통해 리더에게 태그의 정보를 전송한다.

Ⅴ. 안전성 분석

제안한 프로토콜의 보안 요구사항과 공격유형에 대한 안전성을 분석하고, 기존에 연구되었던 기법들과 제안 프로토콜의 안전성을 비교 분석한다.

5.1. 보안 요구사항에 대한 분석

5.1.1. 기밀성과 무결성

인증 과정에서 이루어지는 모든 통신 구성요소들 간 전달되는 어떠한 메시지라도 도청되어 이용되지 않도록 암호화 및 직접노출을 피해야 한다. 제안하는 프로토콜의 경우 전송되는 메시지가 난수로 이루어져 있으며, 또한 대칭키 암호화하여 직접노출을 피하였다. 만약 공격자가 메시지를 도청하더라도 대칭키로 암호화되어있고, 다수의 세션을 도청 및 수집하여 복호화했다 하더라도 난수의 값이기 때문에 무의미한 정보로 기밀성이 유지된다. 또한 리더 서버간 인증과정에서는 OTP를 이용하여 인증하기 때문에 자신이 알고 있는 것, 자신이 가지고 있는것의 이중 인증 방식을 취하게 되므로 기밀성이 유지된다.

5.1.2. 익명성과 불구분성

태그가 리더에게 송신하는 유일한 식별 정보가 매 인증 요청마다 동일하거나 예측 가능해서는 안 되며, 태

그 ID가 노출되지 않더라도 태그를 구별할 수 있는 정보를 얻게 되면 위치추적의 보안 문제가 발생한다. 제안하는 프로토콜의 경우 태그는 태그 고유 식별 정보인 TagID를 대칭키 암호화 하여 리더에게 전송한다. 이때 상호 인증에 사용되었던 메시지는 리더가 생성한 임의의 난수 R_R을 XOR 한 값으로 메시지를 암호화하기 때문에 매 인증 요청 시 리더는 새로운 임의의 난수를 생성하고 TagID $\oplus$ R_R 의 값도 항상 새로운 값으로 전송되어 익명성 및 불구분성을 만족한다.

5.1.3. 전방향 안전성

태그가 리더, 서버에서 전송하는 유일한 식별 정보, 메시지를 도청하여 이전에 전송했던 정보를 이용해 태그를 추적할 수 없어야 한다. 태그가 리더에 제공되는 응답이 예측 가능한 경우 보안 문제가 발생한다. 제안하는 프로토콜의 경우 태그가 제공하는 메시지는 $E_{SK}((TagID \oplus R_R) \| CRC)$이므로 난수를 포함하고 있고, 매 인증 마다 다른 값으로 바뀌기 때문에 도청 공격으로 수집한 정보를 분석하여 태그의 위치 추적을 할 수 없다.

5.1.4. 상호인증

RFID 시스템에서 통신 요소들 간의 상호인증을 거치지 않으면 프로토콜을 통해 전송되는 정보들이 공격자에게 쉽게 노출되고 위·변조가 될 수 있다. 제안하는 프로토콜은 상호 인증을 위해 리더가 생성한 난수를 대칭키 암호화한 메시지를 전송한다. 전송받은 메시지를 사전에 안전하게 공유한 키 값으로 복호화하고 또한 복호화한 임의의 난수 값을 CRC 순환중복검사하여 정당한 사용자로부터 전달 받았음을 알 수 있다.

5.2. 공격 유형에 대한 분석

5.2.1. 스푸핑 공격

공격자의 태그나 리더가 마치 정당한 것처럼 속여 거짓 정보로 응답하고, 인증을 통과하는 공격법이다. 상호 인증을 하지 않고 메시지 정보를 전달할 경우, 스푸핑 공격에 취약할 수 있다. 제안한 프로토콜은 대칭키 암호화된 메시지 정보를 가지고 인증을 참여하기 때문에 공격자는 암호화된 메시지를 복호화 할 수 없어 상호 인증 과정에서 비 정상 종료된다.

5.2.2. 도청공격

모바일 RFID 시스템에서 메시지 교환은 무선 채널상에서 이루어지기 때문에 공격자에게 도청공격을 받을 수 있다. 제안한 프로토콜은 기밀성 및 무결성의 보안 요구사항을 만족하며 난수를 사용하고, 대칭키 암호화한 메시지를 전송하기 때문에 비밀키가 없는 공격자는 해독할 수 없다.

5.2.3. 재전송 공격

재전송 공격은 무선 채널상 메시지를 도청공격으로 획득하여 이후 정당한 태그나 리더에게 획득한 메시지를 다시 전송하여 인증과정을 통과하고 태그의 정보를 획득하는 것을 말한다. 제안한 프로토콜의 경우 상호 인증과정에서 매 세션 마다 각각의 구성 요소들이 생성한 난수가 포함되어있어 재전송 공격에 안전하다.

5.2.4. 위치추적 공격

위치 추적은 공격자가 태그에게 동일한 요청을 하여 동일한 응답 값이 전송되는 것을 이용한 공격법이다. 이는 태그의 응답 값을 매 세션마다 다른 값으로 전송하여 방어 할 수 있다. 공격자의 리더가 태그에게 식별정도 요청 질의를 보내더라도 태그는 항상 자신이 생성한 임의의 난수를 대칭키 암호화 하여 보내기 때문에 매 인증 시 동일한 응답 값이 전송되지 않아 위치추적 공격에 안전하다.

표 2. 안전성 분석
Table. 2 Safety analysis

구분	Feldhofer	duc	chien-chen	제안 프로토콜
기밀성	○	○	○	○
불구분성	×	×	×	○
전방향안전성	×	×	×	○
상호인증	○	○	○	○
스푸핑공격	×	×	×	○
도청공격	○	○	○	○
재전송공격	×	×	×	○
위치추적공격	×	×	×	○

○ : 안전, × : 취약

Ⅵ. 결 론

기존 RFID 기술이 주로 기업간 비즈니스 영역에서 유통 및 물류 개선을 위해 사물 식별 및 데이터 수집 효율화에 기여하고 있는 반면 모바일 RFID 기술은 일반 개인 사용자의 영역으로 그 활용 영역을 확대할 것으로 예상된다. RFID 시스템의 핵심은 무선통신으로 이루어진 각 요소들 사이의 데이터 교환이며, 외부의 공격을 받을 수 있는 여지가 있는 부분이다. 안전한 데이터 교환을 위하여 무선 네트워크에서 사용되는 보안 프로토콜을 적용시키는 것을 고려해 볼 수 있겠으나, 이는 저가의 수동형 태그의 제한적인 환경에 적용하기 힘든 것이 현실이다. 본 논문에서는 기존의 RFID 시스템에서 연구되었던 암호학적 프로토콜들이 매 인증 시 동일한 값으로 응답하는 것과 메시지 교환 시 노출되는 등의 문제점을 고려하여 높은 보안성을 갖는 모바일 RFID 상호인증 프로토콜을 제안하였다.

제안한 프로토콜은 태그와 리더간 상호 인증 시 리더가 생성한 임의의 난수를 사용하고 대칭키로 암호화하여 노출되지 않은 상태로 메시지 교환이 이루어진다. 또한 리더 서버간 상호 인증 시 모바일 단말에 내장된 리더의 특성을 고려하여 OTP를 활용한 상호 인증 방식을 이용하였다. 이러한 고려사항을 바탕으로 제안한 프로토콜은 임의의 난수와 OTP가 활용되어 매 인증 마다 메시지가 변경되어 스푸핑 공격, 재전송공격 및 위치 추적 및 트래픽 분석 공격 등에 안전하다.

감사의 글

본 연구는 2013년도 조선대학교 학술연구비의 지원을 받아 연구되었음

성종엽(Jong-yeop Sung)

2009년 조선대학교 정보통신공학과(학사)
2011년 조선대학교 정보통신공학과(공학석사)
현재 조선대학교 정보통신공학과 박사과정
※관심분야 : 컴퓨터네트워크, 정보보안

REFERENCES

[1] Deborah Platt Majoras, "Radio Frequency Identification : Applications and Implications for Consumers," *Workshop Report from the staff of the Federal Trade Commission*, Mar. 2005.

[2] S. M. Lee, E. H. Kim, M. S. Jun, "Design of RFID Mutual Authentication Protocol for Mobile," *Journal of the Institute of Communication and Information Sciences of Korea*, Vol.33, no.2, pp183-190, Feb. 2010.

[3] Hung-Yu Chien and Che-Hao Chen, "Mutual Authentication Protocol for RFID Conforming to EPC Class 1 Generation 2 Standards," *Computer Standards & Interfaces*, Vol 29 No 2, pp.254-259, Feb. 2007.

[4] H. Y. Chien, "Secure Access Control Schemes for RFID System with Anonymity," *In Proceedings of 1005 national Workshop on Future Mobile and Ubiquitous Information Technologies*. 2006.

[5] Martin Feldhofer, Sandra Dominikus and Johannes Wolkerstorfer. "Strong authentication for RFID systems using the AES algorithm," *Workshop on Cryptographic Hardware and Embedded Systems, Lecture Notes in Computer Science*, pp. 357-370, 2004.

[6] D.N. Duc, J.M. Park, H.R. Lee and K.J. Kim, "Enhancing Security of EPCglobal GEN-2 RFID Tag against Traceability and Cloning," *Symposium on Cryptography and Information Security*, 2006.

[7] H. C. Yoon, J. K. Kim, J. Y. Park, J. U. Bum, "Passive RFID Sensor Tag," *The Journal of Korean Institute of Electromagnetic Engineering and Science*, Vol.16, no.3, pp. 16-25, 2005.

[8] IETF RFC 1760, "The S/KEY One-Time Password System," Feb. 1995.

이상덕(Sang-duck Lee)

1997년 조선대학교 전자공학과(학사)
1999년 조선대학교 전자공학과(공학 석사)
2008년 조선대학교 전자공학과(공학 박사)
현재 ㈜ 그린정보시스템 연구원
※관심분야 : 컴퓨터 네트워크, 정보보안, 임베디드 시스템

류창주(Chang-ju Ryu)

2012년 조선대학교 정보통신공학과(학사)
2014년 조선대학교 정보통신공학과(공학 석사)
※관심분야 : 네트워크 보안, 정보보호

한승조(Seung-jo Han)

1980년 조선대학교 전자공학과(학사)
1982년 조선대학교 전자공학과(공학 석사)
1994년 충북대학교 전자계산학과 (공학 박사)
1986년 6월 ~ 1987년 3월 뉴올리언즈대학 객원교수
1995년 2월 ~ 1996년 1월 텍사스대학 객원교수
2000년 12월 ~ 2002년 3월 버클리대학 객원교수
1998년 3월 ~ 현재 조선대학교 전자정보통신공학부 교수
※관심분야 : 통신보안시스템설계, S/W 불법복제 방지시스템, ASIC 설계