RFID 인증 프로토콜에 관한 연구

양성훈*, 양진희*, 명근홍**, 서재현*, 오병균*
*목포대학교 정보공학부, **목포과학대학 컴퓨터정보학과
e-mail:{bbs510d, ispecter, jhseo, obk}@mokpo.ac.kr
e-mail:{gh6604}@hanmail.net

A Study on RFID Authentication Protocol

Sung-Hoon Yang*, Jin-Hee Yang*, Keun-Hong Myoung**
Jea-Hyun Seo*, Byeong-Kyun Oh*
*Division of Information Engineering, Mokpo National University.
**Dept. Computer Information, Mokpo Science College

요 약

RFID(Radio Frequency IDentification)란 일정(무선) 주파수 대역을 이용한 자동인식기술로 원거리에서도 대상물을 분석하여 개체의 정보를 읽거나 기록할 수 있는 시스템이다. 현재 RFID기술은 바탕으로 한 유비쿼터스(Ubiquitous)환경 및 물류시스템, 바코드 시스템을 사용하기 힘든 동물 태깅이나 고속도로 요금부과, 도난 방지, 치매환자의 보호관리 등에 사용할 수 있다는 점으로 사회 전반에 걸쳐 그 사용 폭을 넓혀 가고 있다. 그러나 RFID의 낮은 연산능력과 기억능력의 특징상 정보 보안이나 개인의 프라이버시측면에서 여러 문제들을 발생시킨다. 본 논문에서는 기존의 RFID 인증 프로토콜들을 비교 분석하고, 태그와 리더기 사이의 정보 전송 중 공격자에 의한 정보의 변형을 방지하는 RFID 인증 프로토콜을 제안한다.

1. 서론

RFID(Radio Frequency IDentification)란 일정(무선) 주파수 대역을 이용한 자동인식기술로 원거리에서도 대상물을 분석하여 개체의 정보를 읽거나 기록할 수 있는 시스템이다. 현재 RFID 기술을 바탕으로 한 유비쿼터스(Ubiquitous)환경 및 물류시스템, 바코드 시스템을 사용하기 힘든 동물 태깅이나 고속도로 요금부과, 도난 방지, 치매환자의 보호관리 등에 사용할수 있다는 점으로 사회 전반에 걸쳐 그 사용 폭을 넓혀 가고 있다. 그러나 RFID의 낮은 연산능력과 기억능력의 특징상 정보 보안이나 개인의 프라이버시측면에서 여러 문제들을 발생시킨다. 예를 들어 저가의 RFID에 식별 가능한 정보를 그대로 전송하는 경우 태그와 리더기 사이의 전송내용을 쉽게 도청이 가능하며 이러한 정보를 바탕으로 개인의 위치 등을 파악하는 등의 프라이버시 침해로 직결이 가능하다[1].

본 논문에서는 기존의 RFID 인증 프로토콜들을 비교 분석하고, 태그와 리더기 사이의 정보 전송 중 공격자에 의한 정보의 변형을 방지하는 RFID 인증 프로토콜을 제안한다. 논문의 구성은 2장에서는 기존의 RFID 인증 프로토콜들에 관련연구에 대해 기술하고, 3장에서는 태그와 리더기 사이의 정보 전송 중 공격자에 의한 정보의 변형을 방지하는 RFID 인증 프로토콜을 제안한다.

2. 관련연구

2.1 RFID 시스템의 구성

RFID 시스템의 구성요소는 태그, 리더, 백 앤드 데이터베이스로 구성되며 시스템 작동 형태는 그림 1과 같다[1,3,11]. 전방위 영역(Forward ragne)은 리더가 RF 신호를 태그로 전송할 수 있는 영역이며, 후방위 영역(Backward range)는 태그가 리더의 요청에 대하여 자신의 정보를 전송할 수 있는 영역으로 후방위 영역같은 경우 주파수의 종류에 따라 신호의 반경이 달라진다[1,3].

■ 태그(Tag)는 RFID 시스템에서의 리더의 요청에 대해 식별 정보를 송신하는 것으로 무선 통신을 위한 결합장치와 연산을 수행하고 정보를 저장하는 마이크로 칩으로 이루어져 있으며, 전력을 공급받는

형태에 따라 능동형 태그(Active tag)와 수동형 태그(Passive tag)로 나뉘어 진다.

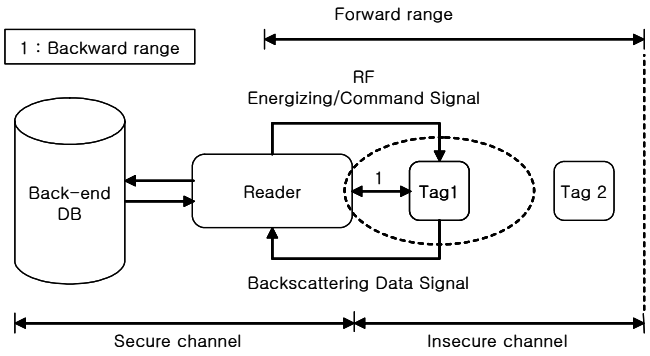

그림 1. RFID 시스템의 구성

■ 리더(Reader)는 태그가 송신한 식별 정보를 수신하여 태그를 인식하는 장치로 트랜시버(Tranceiver)라고도 한다. 리더는 태그에게 RFS(Radio Frequency Signal)를 전송하여 전력을 공급하고, 태그로부터 수신한 정보를 Back and DB로 전송한다.

■ Back and DB는 리더가 수집한 정보를 저장하며 리더기의 연산 능력보다 더 큰 연산을 요구할시 리더를 대신하여 복잡한 연산을 수행한다. 즉, 태그를 식별할 수 있는 정보를 저장하고 리더가 태그로부터 수집한 정보의 진위를 판별할 수 있는 기능을 수행한다.

2.2 RFID 인증 프로토콜 설계 시 고려사항

RFID 시스템은 물리적 접촉 없이 태그의 식별이 가능하다는 특징과 반면 태그와 리더간의 통신이 불안전한 채널 상에서 이루어지므로 공격자에 의한 도청(Eavesdropping), 트래픽 분석(Traffic Analysis), 재전송 공격(Replay Attack), 스푸핑 공격(Spoofing Attack), 서비스 거부(Denial of Service), 메시지 유실등에 대한 보안사항을 유지해야한다[1,3].

RFID 시스템의 보안 문제는 크게 정보 누출(Information Leakage)과 위치 추적(Location Privacy)문제로 나눌 수 있다[4]. 첫째로, 정보 누출은 공격자가 무선을 이용하는 리더와 태그 사이의 정보를 획득할 수가 있으며 DB나 리더 혹은 태그를 속이기 위해 정당하다고 꾸민 거짓 메시지를 이용하여 이들의 정보를 획득할 수가 있는 것이다. 이러한 공격을 막기 위해 블로커 태그, AES를 태그에 탑재한 RFID 시스템, XOR One-Time Pad등이 제시되고 있다. 둘째, 위치 추적에는 태그 자체가 정보가 되는 경우로 해시 기반 인증 프로토콜, 해시 체인, 재 암호화 기법, 상태 기반 인증 프로토콜 등이 제안되었다.

2.3 기존에 제안된 RFID 인증 프로토콜

■ Weis의 해쉬 락 프로토콜은 해쉬 함수를 갖는 태그에 ID와 인증시 이용할 랜덤하게 선택된 Key의 해쉬 값인 metaID(metaID=h(key))를 저장 후 판독기로부터 전송된 key를 이용하여 해쉬한 값이 자신의 metaID와 같다면 그 정보가 타당한 것으로 간주하여 ID를 전송하게 된다. 해쉬 락 프로토콜의 위험성은 ID 노출을 방지하기 위한 고정된 metaID의 이용으로 태그의 추적이 가능하며 재전송 공격에 취약하다[2,3,9,10].

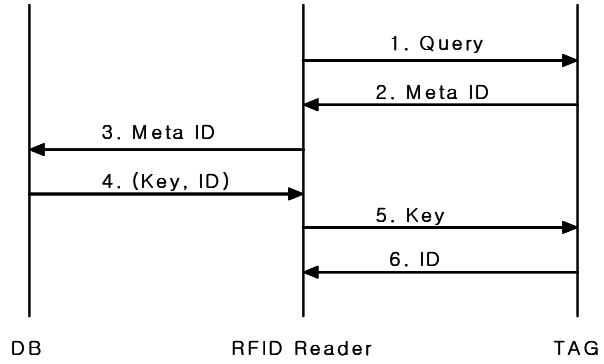

그림 2 해쉬 락 프로토콜

■확장된 해쉬 락 프로토콜은 해쉬 락 프로토콜의 확장기법으로 해쉬 함수와 의사난수 생성기를 갖는 태그는 자신의 ID를 입력값 h(ID || R)을 계산하여 c와 r을 리더에서 전달하고 전달받은 DB는 저장된 모든 IDt와 r로부터 c에 대응하는 식별 정보를 연산 후 IDk를 전달하게 된다. 그러나 IDk가 불안전한 채널을 통해 전송되므로 위치추적이 가능하고 공격자가 도청에의해 R, H(ID,||R)을 획득하여 재전송할 경우 정당한 태그로의 가장이 쉽기 때문에 재전송 공격에도 취약하다.[2,3,6,7]

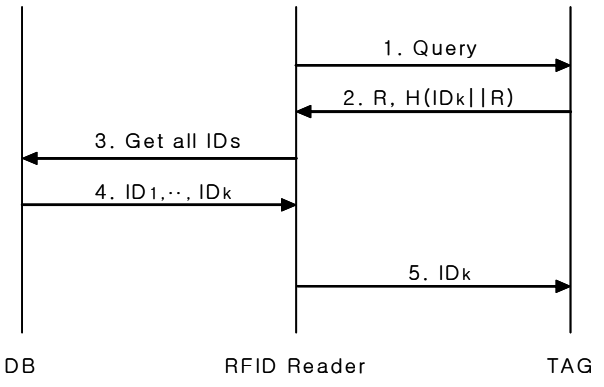

그림 3 확장 해쉬 락 프로토콜

■ 해쉬 기반 ID 변형 프로토콜은 질의를 받은 태그는 TID를 1증가 시킨 후 해쉬를 통해 H(ID), H(TID⊕ID), ΔTID)의 정보를 전달하고 데이터베이스는 이 정보를 이용하여 태그를 인증하고 임의의

랜덤값 R을 생성하여 태그에게 전송한다. 이후 태그는 H(R⊕TID⊕ID)를 생성하여 전달받은 정보와 비교한 후 값이 같으면 기존의 ID를 (ID⊕R)값으로 갱신시킨다. 해쉬 체인 기법과 유사한 ID 변형은 공격자의 재전송 공격으로부터 안전하나 공격자가 정당한 리더로 가장하여 H(ID), H(TID⊕ID), ΔTID를 획득하여 리더의 질의에 대한 응답으로 사용 시 정당한 태그로 인증이 가능하다[1,3,10].

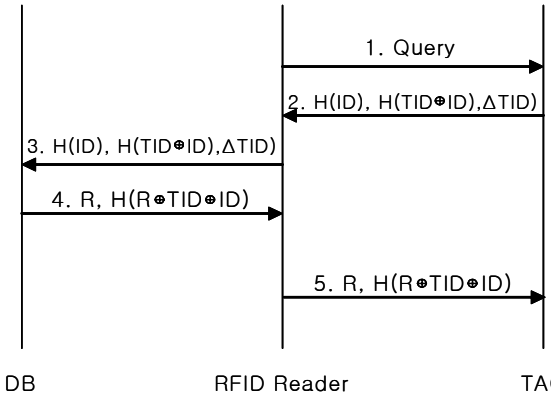

그림 4 해쉬 기반 ID변형 프로토콜

■ 개선된 해쉬 기반 ID 변형 프로토콜은 리더가 의사난수 생성기를 이용하여 랜덤한 S를 생성하여 태그에게 질의를 보내면 태그는 h(ID)와 R=h(ID||S)를 생성 후, R의 왼쪽 반인 L(R)을 리더를 통해 DB에 전송한다.

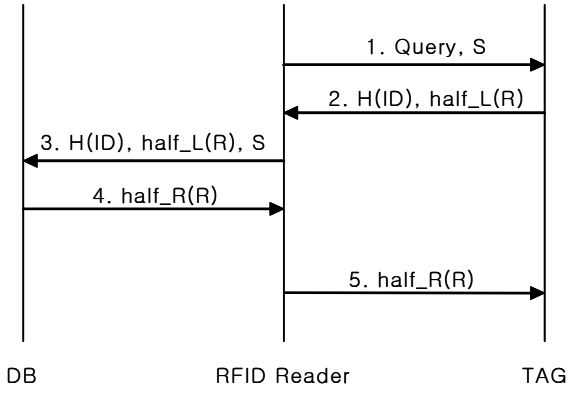

그림 5 개선된 해쉬 기반 ID 변형

DB는 h(ID)를 통해 ID를 검색하여 S와 R′를 생성 후 R′과 L(R′), L(R)을 비교하여 일치할 경우 정당한 태그로 인증하고 ID를 R′로 XOR 연산 후 R′의 오른쪽 반인 R(R′)을 전송한다. 태그는 R(R)과 R(R′)을 비교하여 일치할 경우 ID를 R과 XOR 연산하여 갱신한다. 이 프로토콜의 문제점은 태그가 데이터를 가지는 시스템에 적용될 경우, 공격자는 리더로 가장하여 태그를 속이고 태그 내의 정보를 얻을 수 있는 스푸핑 공격을 가할 수 있다[3,10].

■ 해쉬 체인 프로토콜은 서로 다른 두개의 해쉬 함수를 이용하여 리더의 질의에 응답하여 At, I, G(Si) 정보를 전달하고 DB에서 G(Si)에 대한 i번의 인증 연산을 거친 후 ID를 전달하게 된다. 그러나 해쉬 체인은 리더이 질의에 대해 항상 다른 응답을 하므로 공격자가 태그의 응답 αt,i를 알고 있으며 αt,i를 재전송 하는 경우 정당한 태그로 가장할 수 있으므로 재전송과 스푸핑 공격에 취약하다[1,2,3].

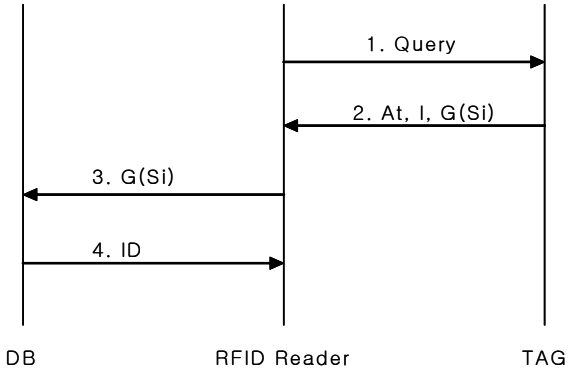

그림 6 해쉬 체인 프로토콜

■ One time Pad 프로토콜은 리더가 태그에게 질의를 요청하면 태그는 K∈{α}∪{β}∪{γ}를 구성하는 값중 어떠한 d가 결정 되었을때 αd를 전송하고 검증자는 αd와 같은 정보가 있는지 검색하여 이에 해당하는 βd를 태그에게 전송한다. 이때 βd가 일치하는 값이면 태그는 γd를 검증자에게 전송하여 서로를 인증하고 필요시 One-Time pad를 태그에게 전송하여 패드에 k를 덧붙여 k′를 구성하고 k를 XOR 연산한 결과를 알려주게 된다[2,11].

■ 재 암호화 프로토콜에서 태그는 비밀키 xt와 공개키 yt 값을 생성하고 DB에 각 태그의 (xt, IDt)를 저장하게 된다. 리더는 각 태그의 암호문 C와 난수 R값을 사용해서 one-time pad를 생성하고 초기 one-time 값과 C값은 태그에 저장되고 다음부터 이 값을 갱신한다. 리더가 태그로부터 C를 받으면 리더는 해당 ID를 식별하기위해 DB의 모든 태그의 비밀키를 이용하여 복호화를 수행하고 태그가 리더로 다시 신호를 보낼때 one-time pad에서 2개의 값을 선택해서 암호화를 수행하게 된다[2,11].

3. RFID 기반 인증 프로토콜 설계

제안하는 프로토콜은 그림7 에 간략히 묘사 되어 있다.

3.1 사전준비단계

① 랜덤값인 y_1를 선택하고, $y_1 \odot y_2 = P$인 y_2를 결정한다.(⊙는 연산자)

② y_1^2 mod N, y_2^2 mod N으로 하여 ID에 저장한다.

③ 태그에는 ID, h(ID)를 저장한다.
④ DB서버에는 ID, y_1, y_2를 저장한다.
③ 리더의 질의 시 마다 매번 값이 증가하는 C, 초기값을 0으로 갖는 flag를 태그에 저장한다.

3.2 인증단계

① 최초 리더는 Request 메시지를 태그에게 보낸다.
② 태그는 h(ID)를 DB서버에게 전달한다.
③ DB서버는 저장된 ID를 이용 태그로부터 전송받은 h(ID)와 비교하여 같으면 y_2^2 mod N을 태그에 전송하고, 다르면 통신을 중단한다.
④ 태그는 DB에서 전송된 y_2^2 mod N을 이용하여 $y_1 \odot y_2 = P$를 계산하여 같으면 y_1^2 mod N을 전송하고 다르면 세션을 중단한다.
⑤ DB는 태그에서 전송된 y_1^2 mod N을 이용하여 $y_1 \odot y_2 = P$를 계산하여 인증을 완료한다.

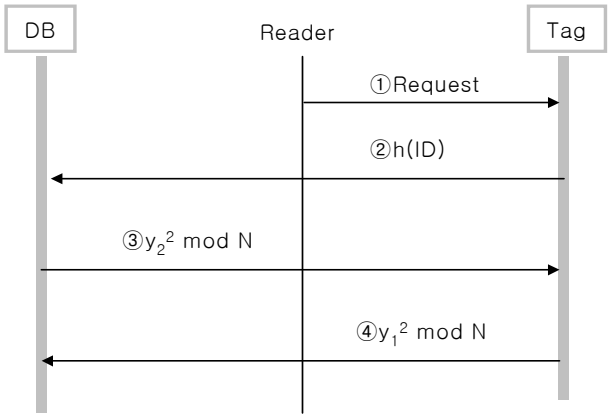

그림 7 RFID 인증 프로토콜 제안

3.3 안전성 분석

■ Replay : 공격자는 도청으로부터 획득한 h(ID), y_1^2 mod N, y_2^2 mod N을 이용하여 재전송공격을 시도할 수 있다. 그러나 질의 시 마다 C값이 매번 증가하므로 재전송 공격에 안전하다.

■ 위조 : 만약 공격자가 태그나 DB서버를 위조할 때, 공격자는 h(ID), y_1^2 mod N, y_2^2 mod N을 도청하여 y_1, y_2를 올바르게 생성해야만 한다. 그런데, y_1이 P보다 큰 정수에서 랜덤에서 선택한다. 그러므로 공격자가 y_1, y_2를 결정하기 위한 공간은 계산상 불가능하다.

■ 위치추적 : 공격자가 정당한 리더로 가장하여 지속적으로 Request를 요청하면서 h(ID)를 획득하여도 DB에 태그의 실질적인 개인 정보 y_1, y_2를 보관하므로 개인 정보 프라이버시를 보장하며, 태그에 저장된 ID값이 변하지 않더라도 공격자가 y_1, y_2를 결정하기 위한 공간은 계산상 불가능하므로, 위치 프라이버시를 만족한다.

4. 결론

본 논문에서는 기존에 제안된 RFID 인증 프로토콜들에 관한 인증 및 프라이버시에 관하여 논의하였고, 재전송 공격, 위조, 위치추적 공격에 안전한 RFID 인증 프로토콜을 제안하였다. 현재 태그와 리더가 공유하는 키 값을 줄이는 여러 방법이 제안되고 있으나 강력한 암호를 사용하지 않는 한 안전성에 문제가 있다. 따라서 RFID의 자원 제약성에 따른 특성으로 암호 모듈에 대한 경량화 기술 개발이 필요하다.

참 고 문 헌

[1] 유성호, 김기현, 황용호, 이필중, “상태기반 RFID 인증 프로토콜”, 한국정보보호학회논문지 14권 6호
[2] 양정규, 김광조, 표철실, “저가의 RFID에 관한 정보보호 기법 연구”, 한국정보보호학회논문지 14권 1호
[3] 이근우, 오동규, 곽진, 오수현, 김승주, 원동호, “분산 데이터베이스 환경에 적합한 Challenge-Response 기반의 안전한 RFID 인증 프로토콜”, 정보처리학회논문지 C 제12-C권 3호 2005. 6
[4] 정교일, “유비쿼터스 정보보호 기술동향-RFID 정보보호 기술과 소비전력 중심으로”, 지역정보화·KALY 2005. 9 Vol. 34
[5] 강전일, 양대헌, “위치 추적과 서비스 거부 공격에 강한 RFID 인증 프로토콜”, 한국정보보호학회논문지 15권 4호 2005. 8
[6] Weis, S. et al. Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems, First International Conference on Security in Pervasive Computing (SPC), 2003
[7] Weis, S. et al. Security and Privacy in Radio Frequency Identification Devices, Massachusetts Institute of Technology, 2003
[8] Henrici, D. Müller, P. : Hash-based Enhancement of Location Privacy for Radio Frequency Identification Devices using Varying Identifiers, PerSec'04 at IEEE PerCom, 2004
[9] S. E. Sarma, S. A. Weis, and D.W. Engels. Radio frequency identification systems. In Burton S. Kaliski Jr., C, etin Kaya Ko.c, and Christof Paar, editors, CHES '02, pages 454-469. Springer-Verlag, 2002. LNCS no. 2523
[10] 황영주, 이수미, 이동훈, “An Authentication Protocol for Low-Cost RFID in Ubiquitous”, CISC'504 pp.120-122. Jun 2004
[11] 강전일, 박주성, 양대헌, “RFID 시스템에서의 프라이버시 보호기술”, 한국정보보호학회지 14권 6호 2004. 12