RFID 시스템에서 리더 ID를 이용한 인증 프로토콜

김태은 주소진° 이재식 이승민 전문석
숭실대학교 대학원 컴퓨터학과
{eunii31, yetiblow°, j30231, cowaboonga}@ssu.ac.kr
mjun@computing.ssu.ac.kr

Authentication Protocol Using Reader ID In RFID System

Taeeun Kim, Sojin Ju°, Jaesik Lee, Seungmin Lee, MoonSeog Jun
Department of Computing, Soongsil University

요 약

RFID는 IC칩에 내장된 정보를 무선주파수를 이용하여 비접촉방식으로 읽는 기술로서 유비쿼터스 시대를 맞이하여 주목받는 기술이다. 그러나 사용자도 알지 못하는 사이에 리더가 요구하는 질의에 자동으로 응답하는 RFID 태그의 특성은 사용자의 개인 정보 노출의 위험이 있다.

본 논문에서는 이러한 RFID 시스템의 문제점을 해결하기 위한 기존의 방법을 알아보고, 문제점을 분석한다. 또한 해쉬 함수를 이용하여 암호화하고, 리더 ID를 사용하여 데이터베이스와 리더간의 인증을 보완한 안전한 RFID 인증 프로토콜을 제안하고 설명한다.

1. 서 론

RFID(Radio Frequency Identification)는 IC칩에 내장된 정보를 무선주파수를 이용, 비 접촉방식으로 읽어내는 기술로서 상품, 화물, 자재, 유가증권 등 모든 물건과 동식물 등에 부착하여 생산, 유통, 판매 등에 있어 관리 효율 및 고객만족도 향상을 통해 획기적인 비용절감을 가능하게 하는 기술이다[1].

그러나 사용자도 알지 못하는 사이에 모든 리더에게 자동으로 응답하는 RFID 태그의 특성은 개인의 정보 노출, 위치 추적 등의 프라이버시 침해 문제를 발생시킬 수 있다. 게다가 물리적 접촉 없이도 인식이 가능한 RFID*시스템은 태그와 리더사이의 통신내용이 3자에 의해 쉽게 도청이 가능하므로 이는 사용자의 프라이버시 침해로 직결된다. 따라서 RFID 시스템에 대한 여러 응용에 대한 연구와 더불어 RFID 통신에서 일어날 수 있는 여러 보안, 프라이버시 문제를 해결하는 것에도 많은 연구가 행해져야 할 것이다.

본 논문에서는 RFID의 프라이버시 문제를 해결하기 위한 기존의 방식들을 살펴보고, 이들의 문제점 분석을 통해 보다 안전한 인증 방식을 제안하고자 한다. 본 논문의 구성은 다음과 같다. 먼저 2장에서는 RFID 시스템과 RFID 프라이버시에 관련된 기존 방식을 알아보고, 이를 분석한다. 3장에서는 제안하는 프로토콜을 소개하고, 마지막으로 4장에서 결론을 내리고자 한다.

2. 관련연구

2.1 RFID 시스템

RFID 시스템은 라디오 주파수를 이용하여 물리적 접촉 없이 개체에 대한 정보를 읽거나 기록하는 자동데이터식별 시스템이다[2]. RFID 시스템은 고유의 정보를 저장하는 태그, 판독 및 해독 기능을 수행하는 리더, 태그로부터 읽어 들인 데이터를 처리할 수 있는 데이터베이스를 포함한 호스트 컴퓨터로 구성되어 있다 [3].

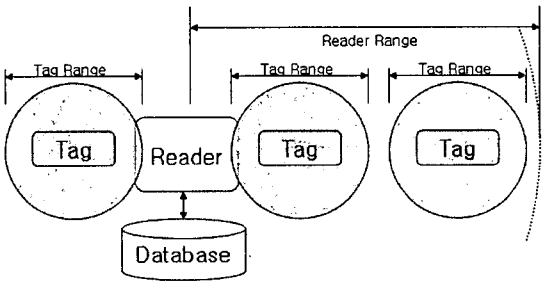

그림 1 RFID 시스템

2.1.1 태그(Tag)

태그의 구성은 연산을 수행하고 데이터를 저장하는 칩과 송수신을 위한 안테나로 구성되어 있는 장치로 트랜스폰더(Transponder)라고도 한다. 태그는 전력 유무에 따라 능동형 태그와 수동형 태그로 분류된다.

- 능동형 태그(Active tag) : 태그가 전력을 가지고 있어서 자체 전력을 이용하여 데이터를 송수신한다. 원거리 데이터 송수신이 가능하지만 수동형 태그에 비해 가격이 비싸고, 배터리의 수명이 다하면 작동이 멈추는 단점이 있다.
- 수동형 태그(Passive tag) : 태그가 전력을 가지고 있지 않고, 리더로부터 수신한 전자기파에 의한 유도를 통하여 전력을 공급받는다. 능동형 태그에 비해 가격이 저렴하고, 반영구적으로 사용이 가능하나 태그의 전송 전력이 능동형보다 낮기 때문에 근거리 정보 전송에 주로 이용된다.

2.1.2 리더(Reader)

리더는 태그로부터 송신된 정보를 식별하는 장치로 트

랜시버(Tranceiver)라고도 한다. 태그로 부터 얻은 정보는 데이터베이스로 전송되어 데이터베이스에 저장된 태그의 상세한 정보를 얻는데 이용될 수 있다.

2.1.3 호스트 컴퓨터(Host Computer)

데이터베이스(Database)를 포함한 호스트 컴퓨터는 태그의 정보를 저장하고 있다. 리더의 요청을 받은 호스트 컴퓨터는 데이터베이스에 저장되어 있는 태그의 정보를 리더에게 전송해주는 역할을 한다. 리더와 호스트 컴퓨터 사이에는 SSL과 같은 안전한 통신채널을 사용한다.

2.2 RFID 시스템의 보안 요구사항

RFID 시스템은 무선을 통해 불안전한 채널에서 통신이 이루어지기 때문에, 정보가 소유자의 의도과 상관없이 노출되는 위험이 발생할 수 있다. 그러므로 RFID 시스템은 도청, 통신내용분석, 위치트래킹, 스푸핑, 재전송 공격, 메시지 유실, 서비스 거부, 물리적 공격 등에 안전하도록 설계되어야 한다.

2.3 해쉬-락 기법

해쉬-락 기법의 경우 실제 ID의 노출을 방지하기 위하여 metaID를 이용하고, DB에서 metaID를 이용하여 획득한 Key값을 Tag에 전송하여 ID값을 얻는다. 하지만 Key와 ID값이 도청가능하고 스푸핑 및 재전송 공격이 가능하며 위치트래킹이 가능한 단점이 있다[4].

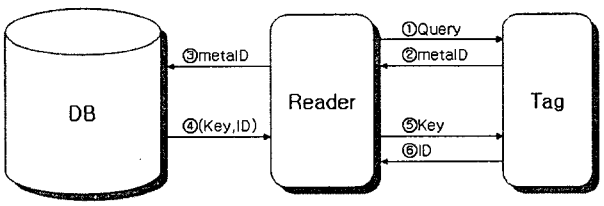

그림 2 해쉬-락 기법

2.4 해쉬-체인 기법

서로 다른 두 개의 해쉬함수를 사용하는 해쉬-체인 기법은 세션마다 다른 A_i값을 전송하므로 위치트래킹 공격에 안전하다. 하지만 최악의 경우 데이터베이스에서는 모든 S_i에 대하여 H와 G를 i번 수행해야 한다. 또한 잘못된 응답이 왔을 경우, 데이터베이스는 보유한 모든 ID에 대해 ∞번의 해쉬를 수행할 가능성이 있다[5].

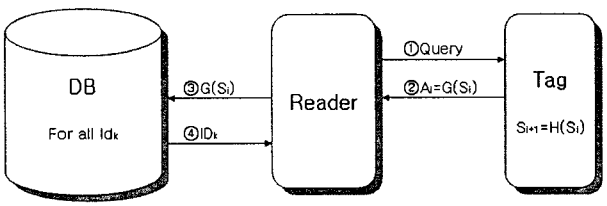

그림 3 해쉬-체인 기법

3. 제안 프로토콜

본 논문에서 제안하는 프로토콜은 리더가 고유의 ID를 갖고 난수 R을 생성하는 방법을 이용하여 XOR와 해쉬함수를 거침으로써 ID와 Key가 평문형태로 전달되는 것을 방지한다. 태그는 데이터베이스와 인증을 거친 ID를 갖는 리더를 인식하고 리더가 생성한 R값을 이용하여 리더에게 자신의 정보를 전송하므로 기존 인증 프로토콜과는 다르게, 보다 안전하게 할 수 있도록 설계하였다.

3.1 프로토콜 구조

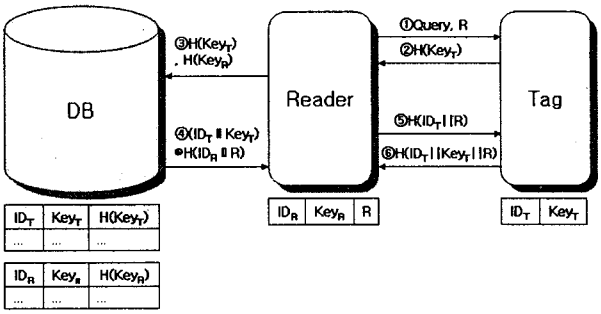

그림 4 제안 프로토콜

[파라미터]

- Query : 질의, 태그의 응답을 요청
- ID_T : 태그 고유의 은닉 정보
- Key_T : 태그 고유의 키 값
- ID_R : 리더 고유의 은닉 정보
- Key_R : 리더 고유의 키 값
- R : 리더가 생성하는 난수(Pseudo Random Number)

[연산]

- H( ) : One-way 해쉬함수
- ‖ : 문자열 연접 연산(Concatenate function)
- ⊕ : exclusive OR

[그림 4] 에서 태그는 고유의 정보인 ID_T와 Key_T를 갖고 있고 해쉬함수와 리더에서 생성된 난수 R을 저장할 수 있는 임시 저장소를 갖는다. 리더는 해쉬함수, 난수 발생을 할 수 있으며 리더도 태그와 같이 리더만의 고유 ID와 Key값을 각각 갖는다. 데이터베이스는 이런 태그와 리더를 인증하기 위하여 태그에 대한 정보를 담아둔 필드와 리더에 대한 정보를 담아둔 필드를 갖는다.

3.2 인증 과정

- 단계 1 : 리더

  리더는 Query와 R을 생성하여 태그에 전송한다. 태그들과의 세션이 종료될 때까지 리더는 R 값을 임시 기억장소에 기억한다.

- 단계 2 : 태그

  태그는 새로운 Query가 들어오거나 세션이 종료될 때까지 R값을 임시 기억장소에 기억하고, Key_T와 해쉬함수를 사용하여 $H(Key_T)$를 생성하고 그 값을 리더에게 전송한다.

- 단계 3 : 리더

리더는 태그로부터 받은 $H(Key_T)$값과 리더 자신의 Key_R를 해쉬한 $H(Key_R)$를 데이터베이스로 전송한다.

- 단계 4 : 데이터베이스

  리더로부터 $H(Key_T)$와 $H(Key_R)$를 수신한 데이터베이스는 저장된 태그의 $H(Key_T)$와 리더의 $H(Key_R)$를 비교하여 태그의 ID_T와 리더의 ID_R를 얻어내 태그와 리더를 인증한다. 인증이 성공하면, 데이터베이스는 태그의 ID_T와 Key_T를 연접한 값과 인증된 리더의 ID_R와 난수R을 연접한 후 해쉬한 값을 XOR 연산하여 리더로 전송한다.

- 단계 5 : 리더

  리더는 데이터베이스로부터 수신한 $(ID_T \| Key_T) \oplus H(ID_R \| R)$를 ID_R과 단계 1에서 생성했던 R값을 연접한 후 해쉬한 $H(ID_R \| R)$을 생성하여 수신한 값을 XOR하여 마지막 태그의 인증을 위한 ID_T와 Key_T를 얻어 임시저장소에 저장한 뒤 태그에게 인증 받기 위해 태그의 ID_T와 난수 R을 연접한 후 해쉬한 값인 $H(ID_T \| R)$을 태그에게 전송한다.

- 단계 6 : 태그

  태그 ID_T와 임시기억장소에 저장된 R값을 해쉬하여 리더로부터 전송한 $H(ID_T \| R)$값과 비교하여 리더를 인증한다. 인증이 성공하면, 태그는 ID_T, Key_T, R를 해쉬하여 리더에게 전송한다. 리더는 임시기억장소에 있던 ID_T, Key_T, R를 해쉬하여 태그로부터 전송된 $H(ID_T \| Key_T \| R)$값과 비교하여 태그를 인증한다.

3.3 제안 프로토콜의 안전성

2.2절에서 설명된 공격 유형에 대하여 제안하는 프로토콜의 안전성을 분석한다.

- 도청 및 통신내용분석 : RFID 시스템은 리더와 태그 간의 통신방식이 무선이므로 도청 공격은 불가피하나 ①Query, R, ②$H(Key_T)$, ⑤$H(ID_T \| R)$, ⑥$H(ID_T \| Key_T \| R)$ 의 값이 도청되어도 ID_T와 Key_T를 유출하기 어렵다.
- 스푸핑 및 재전송공격 : 매 세션마다 리더에서는 랜덤한 R값이 생성되므로 ⑤$H(ID_T \| R)$, ⑥$H(ID_T \| Key_T \| R)$ 의 값이 매번 다르기 때문에 스푸핑 및 재전송 공격을 하기 어렵다.
- 위치트래킹 (Location Tracking) : 리더에서 전송하는 ①Query, R에 대한 태그의 ②$H(Key_T)$값이 일정하고, 같은 세션에서 ⑤$H(ID_T \| R)$에 대한 ⑥$H(ID_T \| Key_T \| R)$값이 일정하여 위치트래킹 공격에 취약한 단점이 있다. 위치트래킹 공격을 막기 위해서는 태그는 매 Query마다 리더가 예상할 수 없는 결과 값을 리더에 전송해주어야 하며, 이를 위해서는 DB나 리더에 많은 부하가 전해질 것으로 예상된다.
- 메시지 유실 (Message loss) : 메시지가 유실되어 인증세션이 비정상적으로 종료되어도 리더는 새로운 R값을 생성하여 다시 세션을 생성할 수 있다.
- 서비스 거부 (Denial of Service) : 악의적인 리더가 지속적으로 ①Query, R값을 전송하면 태그는 R값을 계속 갱신하므로, 서비스 거부 공격에 취약한 단점이 있다. 단점을 보안하기 위해서는 태그는 R값을 매 세션마다 일정시간 유지하도록 설계할 수 있다.
- 물리적 공격 : 프로브공격이나, TEMPEST공격 등에 취약하나 이를 보안하기 위해서는 태그에 고가의 메모리나 칩을 사용해야 하므로 저가의 RFID칩에는 적합하지 않다.

4. 결 론

지금까지 사용자의 프라이버시를 보호하기 위한 기존 RFID 인증 프로토콜과 그 단점에 대해 알아보고, 그것을 보완하여 좀 더 안전한 RFID 통신을 할 수 있도록 하는 프로토콜을 제안하고 설명하였다.

본 논문에서 제안한 프로토콜은 기존에 제안된 프로토콜들이 가지는 취약점인 도청 및 통신내용분석, 스푸핑 및 재전송 공격, 메시지 유실 등의 문제를 해결하였다. 또한 태그가 난수 R을 생성하지 않도록 설계하여 태그의 연산횟수를 줄여 통신 속도를 높였다. 리더가 고유의 ID와 Key를 가지기 때문에 기존에는 이루어지지 않았던 데이터베이스와 리더간의 인증이 가능하도록 하였다. 기존의 프로토콜보다 많은 파라미터를 사용하지만 데이터베이스가 해쉬 모듈을 사용하지 않고 Key값을 이용해서 ID를 확인하므로 서버의 오버헤드를 줄였다.

RFID 시스템은 유비쿼터스 컴퓨팅 환경을 실현시킬 수 있는 기술로 많은 연구가 이루어지고 있지만 그에 따른 문제점도 하나둘씩 드러나고 있다. 그 중에 하나인 사용자 프라이버시 노출에 대한 문제는 시급히 해결되어야할 과제 중 하나이다. 제안하는 프로토콜은 이러한 문제 해결의 한 방안이 될 수 있다.

참 고 문 헌

[1] Klaus Finkenzeller, "유비쿼터스 컴퓨팅의 핵심 RFID Handbook(Second Edition)," 영진.COM, 2004.

[2] 유성호, 김기현, 황용호, 이필중, "상태기반 RFID 인증 프로토콜," 정보보호학회논문지 제14권 6호, pp.57-68, 2003.

[3] 장재득, 장운수, 최송인, "무선 주파수 인식 RFID 시스템 기술 분석," ETRI 전자통신동향분석 제19권 2호, 2004.

[4] Stephen A. Weis, "Security and Privacy in Radio- Frequency Identification Devices," Maters thesis, MIT. May, 2003.

[5] M. Ohkubo, K. Suzuki and S. Kinoshita, "Hash-Chain Based Forward-Secure Privacy Protection Scheme for Low-Cost RFID," Proceedings of the SCIS 2004, pp.719-724, 2004.