# RFID 시스템에서 프라이버시 보호에 관한 연구

박익수° 오병균 *명근홍
목포대학교 정보보호학과
{upark°, obk}@mokpo.ac.kr, *gh6604@naver.com

# A Study of Privacy Protect on RFID System

IK-Su Park° Byeong-Kyun Oh *Kun-Hong Myung
Dept. Information Security, Mokpo National University
*Dept. of Computer Science, Mokpo Science College

요 약

무선 주파수 인식(RFID:Radio Frequency Identification) 시스템은 유비쿼터스 컴퓨팅 환경에서 중요한 기술로 주목 받고 있으나 RFID 시스템이 가지고 있는 특성으로 인하여 시스템의 보안과 프라이버시 침해가 대두되면서 이를 해결하기 위해 많은 프로토콜들이 제안되었다.

본 논문에서는 기존에 제안된 RFID 시스템 프라이버시 보호기법을 해쉬 함수 기반, 재 암호화 기반, XOR 기반으로 분류하여 비교 분석하였다. 향후 유비쿼터스 환경에 적합한 RFID 시스템에서 프라이버시 보호 기법에 관한 연구가 필요하다.

## 1. 서 론

무선 주파수 인식(RFID : Radio Frequency Identification) 시스템은 유비쿼터스 컴퓨팅 환경에서 중요한 기술로 주목 받고 있으나 RFID 시스템이 가지고 있는 특성으로 인하여 시스템의 보안과 프라이버시 침해가 대두되면서 이를 해결하기 위해 많은 프로토콜들이 제안되었다[1-3].

해쉬 함수 기반 기법으로는 해쉬 락, 해쉬 체인, 해쉬 기반 ID 변형, 개선된 해쉬 기반 ID 변형 인증 프로토콜 [1-3] 등이 있으며, 최근 분산 데이터베이스 환경을 고려한 [2]가 제안되었다. [2]는 Challenge-Response 기반으로 리더가 처음 태그에게 질의할 때 난수를 함께 전송하고, 태그는 리더로부터 수신한 난수와 자신이 생성한 난수를 이용하여 응답함으로써 재전송 공격, 스푸핑, 위치 추적에 안전하도록 설계하였으며, 태그에서 3회의 해쉬 연산을 한다.

재 암호화 기법은 해쉬 함수 이외의 암호학적 함수를 사용하는 방법으로 ElGamal 공개키 암호화 시스템에 기반하고 있다. [4]는 태그가 매 세션마다 리더로부터 받은 one-time 랜덤 값들을 사용하여 태그의 비밀정보를 재 암호화하여 전송함으로써 사용자의 프라이버시를 보호하는 기법을 제안하였다. 그러나 재 암호화 방법으로 공개키 암호화 알고리즘을 사용함으로 태그의 제한된 계산 능력으로 인해서 외부의 제 삼자에 의해 시스템 운영되므로 외부 인프라를 형성해야하는 단점이 있으며, 일정 기간 동안 태그의 재 암호화가 수행되지 않는다면 고정된 암호화 값으로 인해 위치 추적이 가능 할 수도 있다[3].

XOR 기반 기법은 태그 인증을 단지 XOR의 연산만을 사용함으로 최저가의 RFID 시스템에 적용이 가능하다. [5]에서 태그는 리더로부터 세션마다 다음 세션에 사용할 랜덤 값들을 받으며, 동일한 랜덤 값들을 가지고 있는지에 대한 확인 과정을 통해 상호 인증한다. 그러나 [5] 기법은 공격자가 정해진 세션만을 도청할 수 있다는 가정 하에서 안전성이 보장된다. 최근 제안된 [3]은 해쉬, 암호화 알고리즘과 같은 암호화 기법을 사용하지 않으며 단지 단순한 비트 연산을 사용하여, 리더와 태그 사이의 모든 통신을 도청할 수 있는 공격자에 대해 안전하도록 설계된 인증 프로토콜이다. 그러나 태그가 처음 생산되고 인증 세션이 한 번도 이루어지지 않은 상태에서 공격자의 공격에 의해 위조된 태그가 인증될 가능성이 있다.

본 논문에서는 기존에 제안된 RFID 시스템에서 프라이버시 보호기법을 해쉬 함수 기반, 재 암호화 기반, XOR 기반으로 분류하여 비교 분석하고자 한다. 향후 유비쿼터스 환경에 적합한 RFID 시스템에서 프라이버시 보호 기법에 관한 연구가 필요하다.

## 2. 관련연구

### 2.1 RFID 시스템

RFID 시스템은 물품 등 관리할 사물에 태그를 부착하고 전파를 이용하여 사물의 ID 정보 및 주변 환경 정보를 인식하여 각 사물의 정보를 수집, 저장, 가공 및 추적함으로써 사물에 대한 측위, 원격처리, 관리 및 사물간 정보교환 등 다양한 서비스를 제공한다.

#### 2.1.1 RFID 시스템 동작 원리

RFID 시스템의 기본적인 동작원리는 RFID의 안테나와 리더의 안테나가 전파를 이용, 통신을 하여 데이터를 주고받는 행위를 수행한다. 그림1에서 태그와 리더 사이의 통신 채널은 공격자의 공격에 안전하지 않다고 가정한다. 이 영역에서는 공격자가 시스템에 공격을 가할 수 있다. 또한 리더와 데이터베이스 사이의 통신 채널은 공격자의 공격에 안전하다고 가정한다[6].

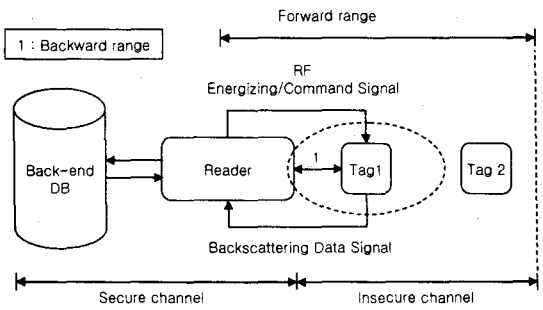


그림 1. RFID 시스템

2.1.2 RFID 시스템의 구성요소[6]

RFID란 마이크로 칩을 내장한 태그, 레이블, 카드 등에 저장된 데이터를 무선주파수를 이용하여 리더에서 자동 인식하는 기술이다. RFID는 비접촉식으로 여러 개의 태그를 동시에 인식할 수 있고, 인식시간이 짧고, 태그에 대용량의 데이터를 저장할 수 있으며, 반영구적인 사용이 가능한 장점이 있다. 그래서 RFID는 기존의 바코드나 자기인식장치의 단점을 보완하고 사용의 편리성을 향상시켜 줄 차세대의 핵심기술이다.

▪ RFID 태그

RFID 태그의 종류는 전원공급 여부에 따라 능동형(Active)과 수동형(Passive)으로 구분한다. 능동형 태그는 배터리를 필요로 하는 타입으로 배터리 사용으로 작동시간의 제한을 받고 수동형에 비해 고가이다. 수동형태그는 내부나 외부로부터 직접적인 배터리의 전원 없이 리더의 전자기장에 의해 작동하며, 능동형 태그에 비해 매우 가볍고 가격도 저렴하면서 반영구적인 반면, 인식거리가 짧고 리더가 더 많은 전력을 소모한다.

▪ 리더

RFID 리더는 태그의 정보를 읽어내기 위해 태그와 송·수신하는 기기이며, 태그에서 수집된 정보를 미들웨어로 전송하는 기능을 한다. RFID 리더는 고정형, 이동형, PC카드형 등 다양한 형태로 되어 있으며 안테나 및 RF회로, 변복조기, 실시간 신호처리 모듈 및 프로토콜 프로세서 등으로 구성된다.

▪ RFID 미들웨어

RFID 미들웨어는 리더에서 계속적으로 발생하는 식별코드 데이터를 수집, 제어, 관리하는 기능을 하며, 모든 구성요소와 연결되어 계층적으로 조직화되고 분산된 구조의 미들웨어 네트워크를 구성하여 서로 통신한다. 미들웨어는 다양한 형태의 리더 인터페이스, 다양한 코드 및 망 연동, 여러 가지 응용 플랫폼에 대해서도 상호 운용성을 보장할 수 있어야 한다.

▪ 백-엔드 데이터베이스

백-엔드 데이터베이스는 리더가 수집한 정보를 저장하며, 연산 능력이 낮은 태그 또는 리더를 대신하여 복잡한 연산을 수행한다. 또한 태그를 식별 할 수 있는 정보를 저장하고 있으므로 리더가 태그로부터 수집한 정보의 진위를 판별하는 기능을 수행한다.

2.2 RFID 시스템에서 프라이버시 보안 요구 사항

2.2.1 RFID 개인정보 침해[6]

기존 인터넷 환경에서는 개인신상정보, 부가정보, 관리정보 등 정보가 생성 시부터 거의 변하지 않는 정보이며, 보안기술 또한 이러한 정보 자체를 보호하는 데 초점을 맞추고 있다. 반면에 RFID 시스템에서 정보는 개인 혹은 기업과 직접적 연관을 가지기보다는 RFID 태그를 활용하면서 생성되는 자료가 정보의 효력을 발휘하여 개인화되거나 기업 자료화되는 시점에서의 데이터가 정보보호의 대상이 된다.

RFID에서 리더와 태그 사이의 통신은 무선 주파수를 사용하므로 제 삼자에 의해 도청이 가능하며 도청된 내용을 이용한 태그의 위조 및 변조, 위치 추적 등은 개인의 프라이버시를 침해하는 문제와 직결된다.

2.2.2 RFID 시스템의 공격 방법

RFID 네트워크를 공격하는 유형으로는 악의적인 공격자가 태그의 정보를 얻고자 시도하는 공격, 정상적인 리더와 태그 사이의 데이터를 공격자가 엿듣는 경우, 공격자가 정상적인 데이터를 위조하여 리더 또는 태그를 혼란시키는 공격, 태그와 관련된 데이터를 입수하기 위하여 정보 서버에 불법적으로 접근해 해킹하는 경우, 인증되지 않은 DoS 트래픽으로 공격하는 경우이다. RFID 시스템에 공격자가 행할 수 있는 공격의 방법은 다음과 같다.

▪ 재전송 공격 (Replay Attack) : RFID 시스템에서 태그, 리더, DB간 통신 중에 획득한 메시지를 그대로 재사용하여 정당한 정보로 위장할 수 있다.
▪ 위치 추적 : 추적자는 트래픽 분석이 가능한 공격자로서 언제, 어디로, 어느 정도의 정보가 전송되었는지를 알 수 있다. 이러한 정보를 이용하여 추적자는 사용자의 위치를 추적할 수 있다.
▪ 스푸핑 (Spoofing Attack) : 공격자는 임의의 태그에게 판독기인 것처럼 위장하여 정당한 태그의 정보를 얻어내고, 정당한 판독기에게 태그로부터 얻은 정보를 보여줌으로써 정당한 태그인 것처럼 가장할 수 있다.
▪ 트래픽 분석 (Traffic Analysis) : 도청 가능한 공격자는 도청된 내용을 가지고 임의의 정보를 분석해 낼 수 있다.
▪ 서비스 거부 (Denial of Service) : 공격자는 자신이 RFID 시스템으로부터 유용한 정보를 얻지 못하더라도 태그와 리더기간의 RF통신에 잡음을 넣거나 통신 내용을 왜곡 시킬 수 있다.

▪ 메시지 유실 : 공격자에 의한 서비스 거부나 무선 통신에 방해가 되는 잡음 등의 문제로 전송되는 데이터가 훼손, 유실될 수 있다.
▪ 물리적인 공격 : 태그를 훔치는 등 물리적인 공격이 가능하다. 이 공격은 태그와의 물리적인 접촉이 요구되어 공개적으로 수행될 수 없으며, 감지 없이 넓게 수행되지

못하므로 본 논문에서는 고려하지 않는다.

### 3. 기존에 제안된 RFID 기반 인증 프로토콜

본 장에서는 기존에 제안된 RFID 시스템에서 프라이버시 보호기법들을 해쉬 함수 기반 기법, 재 암호화 기반 기법, XOR 기반 기법 등으로 분류하여 분석하였다.

▪ 해쉬 함수 기반 기법

해쉬 함수 기반 기법으로는 해쉬 락, 해쉬 체인, 해쉬 기반 ID 변형, 개선된 해쉬 기반 ID 변형 인증 프로토콜 [1-3] 등이 있으며, 최근 분산 데이터베이스 환경을 고려한 [2]가 제안되었다.

황영주 등이 제안한 "유비쿼터스 환경의 Low-Cost RFID 인증 프로토콜"은 스푸핑 공격에 취약한 해쉬 기반 ID 변형 기법을 개선한 RFID 인증 기법을 제안하였다. 그러나 해쉬 기반 ID 변형 기법과 동일하게 인증 세션이 완전하게 종료된 이후에나 ID가 갱신되기 때문에 여러 개의 리더를 곳곳에 설치해놓은 공격자가 정당한 리더로 가장하여 태그의 위치를 추적 할 수 있다[2].

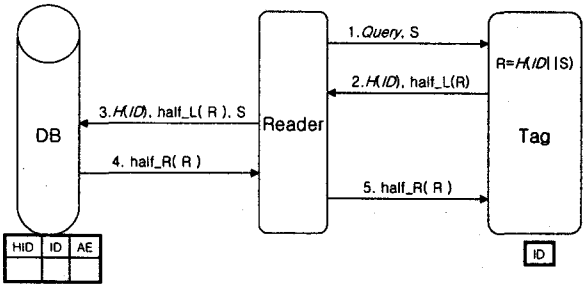


그림 2 개선된 해쉬 기반 ID 변형 기법

이근우 등이 제안한 "분산 데이터베이스 환경에 적합한 Challenge-Response 기반의 안전한 RFID 인증 프로토콜" 일 방향 해쉬 함수와 난수를 이용한 challenge-Response 방식에 RFID 인증 프로토콜을 제안하였다. 이 프로토콜은 태그가 리더로부터 수신한 난수를 이용하여 세션마다 다른 응답을 하기 때문에 재전송 공격과 스푸핑 공격에 대하여 안전하며, 공격자에 의한 추적도 방지 할 수 있다[2]. 그러나 태그에서 해쉬 연산이 3회 이상이다.

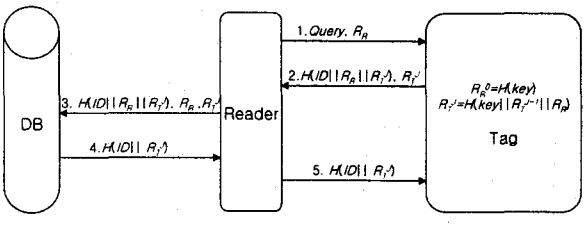


그림 3 Challenge-Response[2]

▪ 외부 재 암호화 기반 기법

재 암호화 기법은 해쉬 함수 이외의 암호학적 함수를 사용하는 방법으로 ElGamal 공개키 암호화 시스템에 기반하고 있다.

Saito 등이 제안한 "Enhancing Privacy of Universal Re-encryption scheme for RFID Tags"는 태그가 매 세션마다 리더로부터 받은 one-time 랜덤 값들을 사용하여 태그의 비밀정보를 재 암호화하여 전송함으로써 사용자의 프라이버시를 보호하는 기법을 제안하였다[4]. 그러나 공개키 암호화 알고리즘을 사용하므로 태그의 제한된 계산 능력으로 인해서 외부의 제 삼자에 의해 이러한 동작이 수행되어야 한다. 이점은 재 암호화 기법을 사용하기 위해 외부 인프라를 형성하여야 한다는 단점을 가진다. 또한 일정 기간 동안 태그의 재 암호화가 수행되지 않는다면 고정된 암호화 값으로 인해 위치 추적이 가능 할 수도 있다[3].

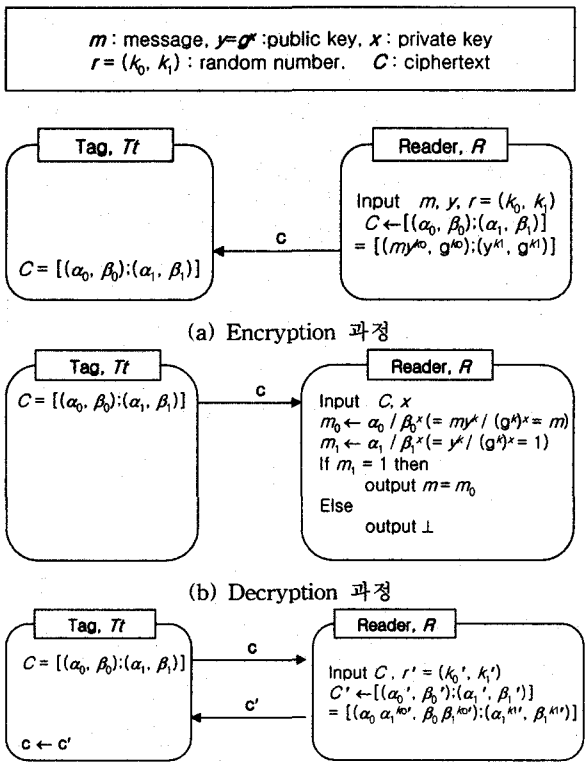


그림 4 Universal Re-encryption 기법

▪ XOR 기반 기법

XOR 기반 기법은 태그 인증을 단지 XOR의 연산만을 사용함으로 최저가의 RFID 시스템에 적용이 가능하다. 최근 저가형의 RFID 태그를 위한 최소한의 암호화 기법을 사용하는 "Minimalist cryptography for Low-cost RFID Tags"가 제안되었다[5]. 이 기법은 단지 XOR (exclusive-or) 연산을 사용하기 때문에 최저가의 RFID 시스템 적용이 가능하다. 이 기법에서 태그는 리더로부터 세션마다 다음 세션에 사용할 랜덤 값들을 받으며,

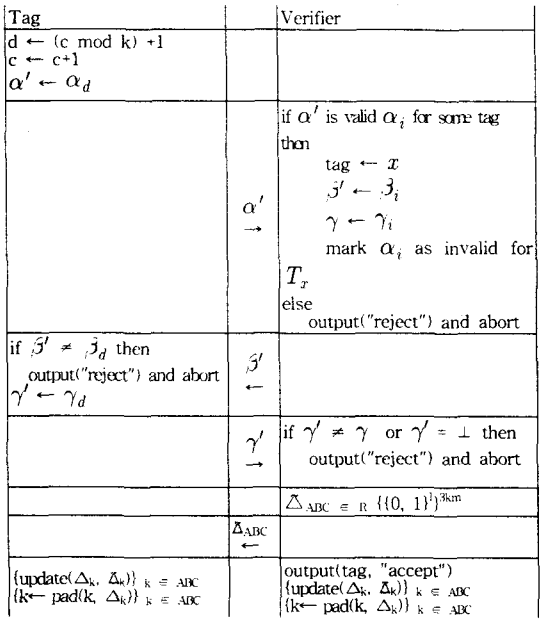


그림 5 Full RFID-tag authentication protocol

동일한 랜덤 값들을 가지고 있는지에 대한 확인 과정을 통해 상호인증을 한다. 이와 같이 매 세션마다 랜덤한 값을 사용하여 태그에서 리더로 전송하는 값을 변경하기 때문에 공격자에 의한 태그의 위치 추적이 불가능하다. 그러나 제안된 기법은 공격자가 정해진 세션만을 도청할 수 있다는 가정 하에서 안정성이 보장된다. 만약 공격자가 가정 이상의 세션을 도청 하게 된다면 도청한 값들을 사용하여 태그의 비밀 정보를 알아 낼 수 있다[3].

최은영 등이 제안한 "저가형 RFID 시스템을 위한 효율적인 인증 프로토콜"은 XOR 연산만을 이용하여 안전하고 효율성이 좋은 저가형 프로토콜이다. 그러나 태그가 생산된 후 인증 세션이 한 번도 이루어지지 않은 상태를 가정하면 불법적인 태그 인증이 가능하다

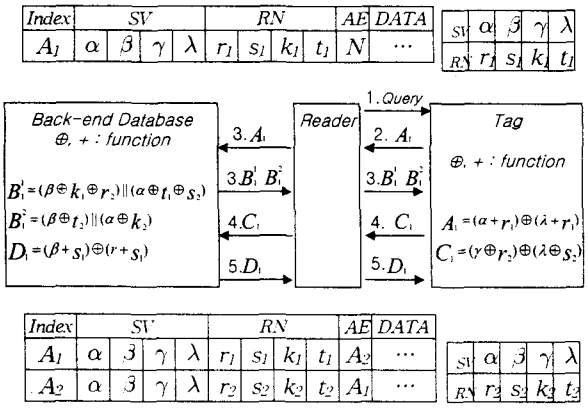


그림 6 XOR 기반 저가형 RFID 시스템[3]

현재까지 RFID 프라이버시 보호 기법은 현재 구현가능한 모델과 유비쿼터스 환경에 활용 가능한 모델을 제안하고 있으며, 특히 저가형의 RFID 시스템 구축을 위한 연구가 활발히 진행되고 있다. 저가의 RFID 시스템은 저전력 소비, 연산 처리 시간, 저장, 게이트 수와 같은 부분에서 많은 제약을 갖는다. 표1은 기존에 제안된 프로토콜을 비교분석 하였다.

표 1 제안 프로토콜 비교분석

| 기반 | 기법 | 재전송 | 스푸핑 | Traffic Analysis | 위치 추적 | 연산 횟수 |
|---|---|---|---|---|---|---|
| 해쉬 함수 기반 | [1] | o | o | o | o | 2 |
| | [2] | o | o | o | o | 3 |
| 재 암호화 | [4] | o | x | - | x | 1 |
| XOR 기반 | [5] | o | x | - | - | 0 |

## 4. 결 론

무선 주파수 인식(RFID:Radio Frequency Identification) 시스템은 유비쿼터스 컴퓨팅 환경에서 중요한 기술로 주목 받고 있으나 RFID 시스템이 가지고 있는 특성으로 인하여 시스템의 보안과 프라이버시 침해가 대두되면서 이를 해결하기 위해 많은 프로토콜들이 제안되었다.

본 논문에서는 기존에 제안된 RFID 시스템에서 프라이버시 보호기법을 해쉬 함수 기반, 재 암호화 기반, XOR 기반으로 분류하여 비교 분석하였다.

RFID 시스템은 전력 소비, 연산 처리 시간, 저장, 게이트 수와 같은 부분에서 많은 제약이 있다. 그러므로 [3] 등에서 제안된 XOR 기반 기법은 저가형 RFID 시스템을 구축하는데 적합하였다. 향후 유비쿼터스 환경에 적합한 RFID 시스템에서 프라이버시 보호 기법에 관한 연구가 필요하다.

### [참고 문헌]

[1] 황영주, 이수미, 이동훈, 임종인, "유비쿼터스 환경의 Low-Cost RFID 인증 프로토콜", 한국정보보호학회 하계정보보호학술대회 논문집 Vol.14, No.1 2004.

[2] 이근우, 오동규, 곽진, 오수현, 김승주, 원동호, "분산 데이터베이스 환경에 적합한 Challenge-Response 기반의 안전한 RFID 인증 프로토콜", 정보처리학회논문지 C 제12-C권 3호 2005.

[3] 최은영, 최동희, 임종인, 이동훈, "저가형 RFID 시스템을 위한 효율적인 인증 프로토콜", 한국정보보호학회 논문지 제15권 제5호 2005.

[4] S. Junichiro, R. Jae-Cheol and S. Kouichi, "Enhancing privacy of Universal Re-encryption scheme for RFID Tags", EUC 2004, vol. 3207 LNCS, pp.879-890, Springer-Verlag, 12, 2004

[5] A. Juels, "Minimalist Cryptography for Low-cost RFID Tags", In the Fourth International Conference on Security in communication networks-SCN2004, vol 3352 LNCS, pp.149-164, Springer-Verlag, 2004.

[6] 유승화, " 유비쿼터스 사회의 RFID", 전자신문사