유비쿼터스 환경에 적합한 사용자 프라이버시 보호 기능을 제공하는 RFID 시스템

정회원 오 수 현*, 곽 진**

Radio-Frequency Identification systems providing Privacy protection in Ubiquitous Computing

Soo-hyun Oh*, Jin kwak** ***Regular Members***

요 약

RFID 기술은 유비쿼터스 컴퓨팅 환경을 구현하는데 핵심이 되는 주요기술로 최근 들어 활발 연구되고 있다. 그러나 RFID 시스템이 많은 장점을 가지고 있는 반면, 사용자의 프라이버시 침해와 같은 새로운 문제점들 야기시킨다. 본 논문에서는 사용자의 프라이버시를 보호하기 위해 제안된 기존의 방식들과 이들이 가지고 있는 취약점에 대하여 설명하고, 이를 해결할 수 있는 보다 안전한 사용자의 프라이버시 보호 기능을 제공하는 RFID 시스템을 제안한다. 본 논문에서 제안하는 RFID 시스템은 사용자가 원하지 않는 정보의 유출과 공격자에 의한 트래킹이 불가능하며, 필요 시 권한을 가진 관리자에 의해서만 추적이 가능한 안전한 RFID 시스템이다.

Key Words : RFID system, EPC, Privacy, Tracking, Hash function

ABSTRACT

Recently, RFID system have been studied actively in ubiquitous computing as main technology. While RFID systems has much advantages, it may create new problems to the user privacy. In this paper, we present a description of previously proposed mechanisms for protecting user's privacy and problems of these. Then, we propose RFID systems providing privacy protection in ubiquitous computing environment. The proposal system as a way of protecting user's privacy from unwanted scanning and tracking by an adversary, but, it can traceable to the tag by authorized administrator when necessary.

Ⅰ. 서 론

유비쿼터스(Ubiquitous) 컴퓨팅 환경이란 사람과 사물을 포함한 모든 것이 컴퓨팅과 통신 능력을 갖게 되고 서로 네트워크로 연결되는 보다 확장된 미래의 IT 환경이라 할 수 있다. 유비쿼터스 컴퓨팅은 기술, 비즈니스, 산업 분야에 있어 다양한 어플리케이션을 제공할 것으로 기대되며, 특히 단순한 상거래뿐만 아니라 일반적인 기업 경영, 유통 관리, 지식 관리, 자산 관리 등 거의 모든 비즈니스 활동에 혁신적으로 적용될 수 있을 것으로 기대된다.

이러한 유비쿼터스 컴퓨팅 환경의 구현에 있어 핵심이 되는 주요 기술로써, 최근에 활발히 연구되는 분야가 RFID 시스템이다. RFID(Radio Frequency IDentification) 시스템은 식별 정보가 저장된 태그(tag)가 부착된 사물을 물리적인 접촉 없이 RF 신호(RF signal : Radio Frequency signal)를 이용하여 개체의 정보를 읽고 기록하는 기술이다.

* 호서대학교 컴퓨터공학부 정보보호 전공 전임강사(shoh@office.hoseo.ac.kr)
**성균관대학교 정보통신공학부 정보통신보호연구실 박사과정(jkwak@dosan.skku.ac.kr)
논문번호 : KICS2004-07-087, 접수일자 : 2004년 7월 7일
※ 본 논문은 "2004년도 호서대학교 학술연구조성비"에 의하여 연구되었습니다.

RFID는 저 비용의 무선 인식 메모리 태그이며, 인식 속도가 빠르고 바코드(Bar code)에 비해 상대적으로 많은 저장 능력을 가지고 있어 물류 및 유통 시스템에서 바코드를 대체할 수 있는 기술로 기대되고 있다. 그러나 RFID를 이용한 개체 인식 기술은 리더(reader)와 칩(chip)을 내장한 태그 사이에 물리적인 접촉 없이 인식이 가능하고 태그의 정보가 전송될 수 있으므로, 이로 인한 과도한 정보 노출을 포함한 사용자의 프라이버시 침해를 유발시킨다는 문제점을 가지고 있다. 즉, RFID 태그의 사용으로 효율적이고 편리한 재고 관리, 반품 관리, 절도나 모조품 예방 등이 가능하다는 장점이 있지만, 리더를 가진 모든 공격자에 의해 사용자가 모르는 사이에 태그에 저장된 정보가 노출되거나 태그의 유일한 식별 번호를 이용하여 사용자의 위치를 추적하는 등의 프라이버시 침해 문제가 발생할 수도 있다.

따라서, RFID 기술을 물류·유통 시스템을 비롯한 여러 산업분야에 널리 활용하기 위해서는 태그에 저장된 정보를 보호하고 임의의 태그에 대한 트래킹(tracking) 방지 등과 같은 관련 보안 문제를 해결하는 것이 반드시 필요하다.

지금까지 사용자의 프라이버시를 보호할 수 있는 RFID 인증 시스템에 관련된 몇몇 연구 결과가 발표되었으며, 대표적인 것으로 Kill 명령을 이용하는 방식[11][12], 해쉬 락 프로토콜[14], 확장된 해쉬 락 프로토콜[15], re-encryption을 이용하는 방식[5], 그리고 해쉬 체인에 기반한 방식[8] 등이 있다. 그러나 기존에 제안된 방식들은 태그에서 리더로 전송되는 정보가 고정되어 전송되므로 트래킹이 가능하거나 비교적 많은 계산량으로 인해 현실적으로 구현하기 어렵다는 등의 문제점을 가지고 있다.

본 논문에서는 태그에서 리더로 전송되는 정보가 고정되어 있지 않으므로 공격자에 의한 트래킹이 불가능하며, 태그의 실제 시리얼 번호가 노출되지 않으므로 사용자의 프라이버시를 보호할 수 있는 안전한 RFID 시스템을 제안한다.

제안하는 시스템은 태그를 소유한 사용자의 프라이버시를 최대한 보호하기 위해 실제 시리얼 번호를 데이터베이스도 알지 못하며, 실제 태그의 시리얼 번호를 식별하는 것은 인가된 관리자들에 의해서만 가능하다는 장점이 있다. 즉, 사용자의 프라이버시 보호와 함께 특별한 상황에서는 관리자에 의해 실제 태그의 시리얼을 추적할 수 있는 기능을 제공하고 있다.

본 논문의 구성은 다음과 같다. 2장에서는 RFID 시스템에 대해 간략히 설명하고, 기존에 제안된 프라이버시 보호를 위한 RFID 인증 메커니즘들에 대하여 기술한다. 다음으로 3장에서는 RFID 시스템에서의 보안 요구사항에 대해 설명하고, 4장에서 제안하는 RFID 시스템의 동작 과정을 기술한다. 그리고 5장에서는 제안하는 RFID 시스템의 특징 및 안전성을 분석하고, 마지막으로 6장에서 결론을 맺는다.

Ⅱ. 관련 연구

1. RFID 시스템의 개요

RFID 시스템은 그림 1과 같이 태그, 리더, Back-end 데이터베이스로 구성되며 각각의 기능은 다음과 같다.

- *태그(tag)* : 리더의 요청에 응답하는 트랜스폰더(transponder). 태그는 각각의 고유한 시리얼 번호(serial number)를 저장하고 있다.
- *리더(reader)* : 태그에 정보를 요청하고 수신한 데이터를 판독하고 태그를 인식하는 트랜시버(transceiver). 리더는 태그에게 RF 신호를 통해 태그의 전원을 공급하는 역할을 한다.
- ***Back-end 데이터베이스*** : 리더가 수집한 정보를 저장하거나 리더 또는 태그 대신 복잡한 연산을 수행하는 안전한 서버. 리더에서 수집된 정보의 진위 여부를 판별해주는 역할을 수행한다.

그림 1에서 forward range는 리더가 RF 신호를 전송할 수 있는 범위를 의미하며, backward range는 태그가 응답 정보를 전송할 수 있는 범위를 말한다. 리더가 태그를 인식하기 위해 보내는 신호를 forward range안에 포함된 tag1과 tag2 모두 수신할 수 있지만, backward range 안에 있는 tag1만 응답 신호를 전송할 수 있게 되는 것이다. 그리고 태그와 리더간의 통신은 RF 신호를 이용하므로 공격자에 의한 도청이 가능하므로 안전하지 않은 통신로를 이용하는 것이고, 리더와 데이터베이스 사이의 통신은 안전한 통신로를 이용하게 된다.

태그는 IC 칩과 안테나로 구성되어 있으며, 그 모양과 크기는 다양하게 존재한다. IC 칩의 데이터를 저장하는 메모리의 크기는 25bit에서 512 KB 이상 등 여러 종류가 있으며, 메모리의 형태 또한 읽기 전용, 읽고 쓰기 가능한 형, 한번만 쓰고 여러 번 읽기 가능한 형태 가 있다. 그리고 전력을 공급받는 방법에 따라 능동형 태그와 수동형 태그로 나눌 수 있으며, 각각의 특징은 다음과 같다.

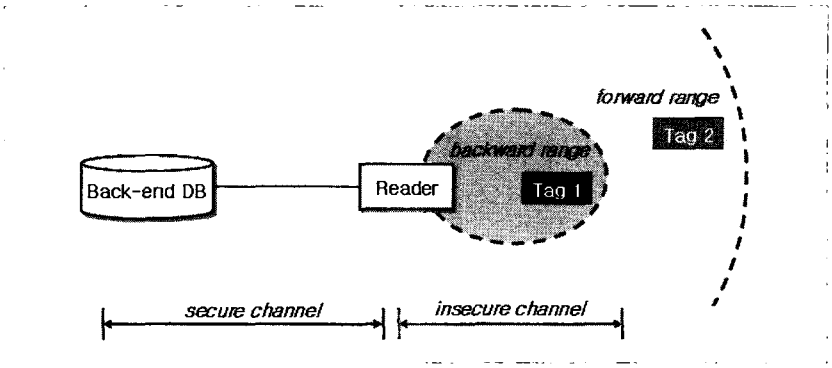


그림 1. RFID 시스템

- *능동형 태그(Active Tag)* : 태그 내부에 전원이 포함되어 있으며, 장거리 데이터 전송 및 인식이 가능하다. 일반적으로 읽기/쓰기 형으로 사용되고 배터리로 인해 가격이 고가이다. 토목·건축 분야, 의료 분야 등에 응용이 가능하다.
- *수동형 태그(Passive Tag)* : 리더의 유도 전류에 의해 전원을 공급받으며, 비교적 간단한 구조이고 단거리 인식에 사용된다. 일반적으로 읽기 전용으로 사용되며, 소형이고 비용이 저렴하여 물류관리, 전자 상거래, 교통 분야 등에 응용할 수 있다.

2. 기존의 RFID 인증 프로토콜

RFID를 이용하여 개체를 인식하기 위해서는 리더가 RF 신호를 이용하여 태그에게 정보를 요청하면 태그가 저장된 정보를 전송하여 응답하고, 이를 수신한 리더는 *back-end DB* 와의 통신을 통해 태그를 식별하게 된다. 이 경우에, 리더를 소유한 공격자는 물리적인 접촉 없이 태그의 정보를 읽는 것이 가능하므로, 사용자가 알지 못하는 사이에 태그에 저장된 정보가 노출되거나 태그의 시리얼 번호를 이용한 사용자의 위치 추적 등이 가능하게 된다.

이러한 문제점을 해결하기 위해 사용자의 프라이버시를 보호할 수 있는 RFID 인증 프로토콜이 제안되었다. 본 절에서는 지금까지 제안된 사용자의 프라이버시 보호가 가능한 RFID 인증 시스템의 특징 및 장·단점에 대해 간략히 살펴보고자 한다.

2.1 "Kill" 명령을 이용하는 방식

Kill 명령을 이용하는 방식은 사용자가 *"kill command"*를 이용하여 RFID 태그의 실행을 중단할 수 있도록 하는 것으로, MIT의 Auto-ID 센터에서 제안한 방식이다.[11][12] 리더는 태그의 정보를 수신하기 위한 쿼리(query)와 kill 명령을 보내고, 메시지를 수신한 태그는 쿼리에 대한 응답을 한 후 *kill* 명령을 수행한다. *kill* 명령을 수행한 태그는 재사용할 수 없게 된다. 그러나 이 방식은 *kill* 명령을 받은 태그를 다시 활성화시킬 수 있는 방법이 없고, *kill* 명령이 제대로 완료되었는지를 확인하기 어렵다는 문제점을 가지고 있다.

2.2 Faraday cage를 이용하는 방식

Faraday cage란 RF 신호가 통과할 수 없는 금속으로 만들어진 케이스를 말하며, 그물망이나 컨테이너 형태로 구성된다. 이 방식은 태그를 Faraday cage안에 넣어 태그와 리더간의 통신을 불가능하게 함으로써 사용자의 프라이버시를 보호하는 방식이다. 그러나 Faraday cage의 크기와 모양, 그리고 이동성 등이 제한적이므로 다양한 환경에 적용하기에는 어렵다는 단점이 있다.

2.3 Active jamming

Active jamming은 Faraday cage와 유사한 방식으로 사용자가 RF 신호를 브로드 캐스팅하는 장비를 이용하여 리더의 동작을 방해하는 방식이다. 태그의 사용자는 RF 신호를 발생시킬 수 있는 디바이스를 소유하여야 하며, 이 디바이스에서 리더의 RF 신호를 방해할 수 있는 다른 RF 신호를 발생하게 된다. 이는 사용자의 프라이버시와 관련 없는 합법적인 리더들의 동작까지 방해할 수 있으므로 합법적이지는 않다는 문제점이 있다.

2.4 Blocker 태그를 이용하는 방식

A. Juels 등은 *tree-walking singulation* 프로토콜을 이용하여 *blocker* 태그를 이용한 사용자 프라이버시

보호 방법을 제안하였다[6]. 이 방식은 슈퍼마켓 등과 같은 곳에서 태그가 부착된 물건을 구입할 경우, 프라이버시 보호를 위해 태그의 특정 "bit"를 바꿔주는 구조로 되어 있다. 예를 들어 첫 번째 비트가 0으로 시작하는 시리얼 번호를 가진 태그들이 슈퍼마켓에 진열되어 있고 사용자가 이중 하나의 물건을 구입하고 프라이버시를 보호하고자 할 경우 첫 번째 비트를 "1"로 바꾸어 프라이버시 존으로 설정을 해주는 방식이다.

2.5 해쉬 락(Hash lock) 프로토콜

해쉬 락 프로토콜은 *"locked"* 상태에서는 태그가 자신의 실제 *ID* 값이 아닌 *metaID* 값을 전송하고, *"unlocked"* 상태에서만 실제 *ID*를 전송함으로써 사용자의 프라이버시를 보호하는 방식이다[14]. 이 방식에서 *metaID = hash(key)*이며, 데이터베이스는 각 태그에 대해 키(key) 값과 *metaID*를 저장해야 한다. 태그는 리더로부터 자신의 키 값을 정확히 전송받은 경우에만 정당한 쿼리로 간주하여 자신의 *ID* 값을 전송하며, 공격자의 공격을 방지하기 위해 *"unlocked"* 상태는 아주 짧은 순간에 이루어지도록 해야 한다.
그러나, RFID 시스템에서 태그와 리더간의 통신은 불안전한 통신로를 이용하므로 누구나 도청이 가능하다. 따라서, 이 방식에서 공격자는 리더와 태그간의 통신을 도청하여 태그의 *ID*를 얻는 것이 가능하고, 또한 *metaID*가 항상 동일한 정보이므로 리더나 공격자에 의한 트래킹이 가능하다는 문제점이 있다.

2.6 확장된 해쉬 락 프로토콜

이 방식은 해쉬 락 프로토콜을 개선한 방식으로 랜덤화 된(randomized) 해쉬 락 프로토콜[15]이라고도 한다. 이 방식에서 태그는 해쉬 함수를 이용하며 매 세션마다 전송되는 값을 변형하며 공격자나 리더를 포함한 허가받지 않은 개체에 의한 트래킹을 방지할 수 있다는 장점이 있다. 그러나 이 방식은 리더에 의한 트래킹은 불가능 하지만 *back-end DB*에는 실제 시리얼 번호가 저장되어 있으므로 *DB*에서의 트래킹이 가능하고, 스푸핑 공격이 가능하며 태그가 수행해야 하는 계산량이 다소 많다는 단점이 있다.

2.7 Re-encryption을 이용하는 방식

이 방식은 EURO banknote에 RFID 시스템을 이용하여 합법적인 트래킹이 가능하도록 하기 위해 제안된 방식이다[5]. 이 방식에서 태그의 메모리는 optical contact area와 RF contact area로 나누어지며, 리더에 의해 태그가 인식된 후에 재 암호화를 이용하여 태그에 저장된 정보를 재 기록하는 방법이다. 이 방식은 사용자가 인식하지 못하는 사이에 물리적인 접촉 없이 리더가 태그의 정보를 읽거나 쓰는 것을 방지할 수 있으며, 필요한 경우에 법 집행기관 같은 합법적인 기관에 의한 트래킹은 가능하다는 장점이 있다. 그러나 공개키 암호 방식과 디지털 서명 방식을 이용하므로 재 암호화에 많은 양의 계산을 요구하므로 현실적으로 구현하는데 많은 어려움이 있다.

2.8 해쉬 체인(Hash-chain)을 이용하는 방식

해쉬 체인을 이용하는 방식은 두 개의 해쉬 함수를 이용하여 리더의 query에 대해 태그가 매 세션마다 서로 다른 응답을 전송하고, 이를 이용하여 태그를 인증하는 방식이다[8]. 이 방식에서 동일한 태그라 할지라도 매번 다른 값을 전송하여 인증을 받으므로, 공격자가 태그의 응답들을 이용하여 동일한 태그인지 아닌지를 구별하는 것이 불가능하다. 그러나 *back-end DB*에는 각 태그의 실제 *ID*가 저장되므로 *DB*의 트래킹은 가능하다.

Ⅲ. RFID 시스템의 보안 요구 사항

RFID 인증 시스템에서 리더와 태그간의 통신은 RF 신호를 이용한 불안전한 채널을 통해 이루어지므로 공격자에 의한 도청이 항상 가능할 뿐만 아니라, 물리적인 접촉없이 태그에 저장된 정보를 판독하는 것이 가능하므로 다음과 같은 보안 요구사항을 만족하도록 시스템을 설계하여야 한다.

(1) *도청 공격에 대한 안전성* : 공격자가 리더와 태그간의 통신을 도청 가능하더라도 태그에 저장된 비밀 정보를 알아내는 것은 불가능해야 한다.
(2) *재 전송 공격에 대한 안전성* : 공격자가 이전 세션의 모든 리더와 태그간의 통신 내용을 도청하여 저장하더라도, 이를 이용하여 리더가 정당한 태그로 인증할 수 있는 새로운 값을 생성하는 것은 불가능해야 한다.
(3) *리더로 위장하는 공격에 대한 안전성* : 공격자가 정당한 리더로 위장하여 태그에게 쿼리를 전송하는 경우, 태그의 응답 정보를 이용하여 태그안의 비밀 정보나 실제 시리얼 번호와 같은 정보를 알아내는 것은 불가능해야 한다.
(4) *트래킹에 대한 안전성* : 공격자가 태그와 리더들 간의 모든 통신 내용을 도청하더라도, 서로 다른

두 개의 응답이 동일한 태그에서 나온 것 인지 아닌지를 구별하는 것은 불가능해야 한다.

(5) *사용자의 프라이버시 보호* : 사용자가 인식하지 못하는 사이에 리더와 태그 간의 통신을 통해 사용자가 소유한 상품이나 구매 패턴 등 사용자의 프라이버시와 관련된 정보가 노출되는 것을 방지해야 한다.

(6) ***Unlinkability*** : 데이터베이스간의 공모를 통해 태그로부터 전송된 응답 정보들의 상관관계를 판별하는 것은 불가능해야 한다.

(7) *추적 가능성* : 필요한 경우에는 각 태그의 실제 시리얼 번호를 추적할 수 있는 방법을 제공해야 한다.

Ⅳ. 제안하는 RFID 시스템

MIT Auto-ID 센터[7]는 효율적인 RFID 태그의 상업화를 위해 EPC(Electronic Product Code)를 제안하였다[1][2][3]. EPC는 크게 헤더(Header), EPC Manager, Object Class, 그리고 시리얼 번호로 구성되어 있다. 헤더는 태그의 버전 등을 나타내는 것이고 EPC Manager는 상품의 제조사, Object Class는 제조사에서 생산한 제품, 그리고 시리얼 번호는 제품을 개별적으로 관리할 수 있도록 유일한 식별번호로 구성되어 있다. 각 제품 하나하나에 부여되는 시리얼 번호가 유일하게 저장이 되므로 프라이버시 문제를 야기한다.

그러므로 본 논문에서는 제품을 유일하게 구별할 수 있는 시리얼 번호를 이용하여 *seed* 값을 생성하여 프라이버시를 보호할 수 있는 시스템을 제안한다. 본 논문에서는 태그를 인증할 수 있는 데이터베이스와 리더를 각각 3개씩이라 가정하고 데이터베이스를 관리하는 마스터 데이터베이스를 고려하여 설명한다.

1. 제안하는 RFID 시스템의 구성

본 절에서는 제안하는 시스템에서 사용하는 *seed* 값의 생성 과정 및 시스템 구성에 대해 설명한다. 먼저, 본 논문에서 제안하는 시스템에서는 사용자의 프라이버시를 보호하기 위해 실제 시리얼 번호 대신 이를 이용하여 *seed* 값을 생성하여 사용한다. 음 그림 2는 본 논문에서 사용하는 *seed* 값의 생성 과정을 나타낸 것이다.

$seed_{ij}$는 i번째 태그의 j번째 *seed* 값을 나타낸다. 예를 들어, $seed_{11}$은 첫 번째 태그의 첫 번째 *seed* 값을 나타낸다. 본 논문에서 제안하는 시스템의 구성은

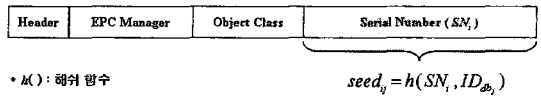


그림 2. $seed_{ij}$ 값 생성

앞에서 설명한 기본적인 RFID 시스템과 동일하며, 각 구성요소는 다음과 같다.

- *마스터 데이터베이스(MasterDB)* : 마스터 데이터베이스는 실제 시리얼 번호(*SN*)를 저장하고 있으며, 실제 시리얼 번호에 해당하는 *seed* 값과 이것이 저장되어 있는 각 데이터베이스(*DB*)의 식별자(*ID*)와 함께 마스터키(*K*)로 암호화되어 저장되어 있다. 필요시 복호화 하여 실제 시리얼 번호를 복구할 수 있다. 그림 3은 본 논문에서 제안하는 마스터 데이터베이스에 저장된 정보들을 나타낸 것이다.

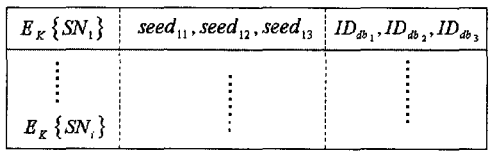


그림 3. 마스터 데이터베이스의 저장 정보

- *데이터베이스(Database, DB_i)* : 데이터베이스는 태그를 식별할 수 있는 *seed* 값을 저장하고 있으며, 리더가 전송해 주는 태그의 정보를 자신이 저장하고 있는 정보와 비교하여 태그의 인증을 수행하고, 리더에게 인증정보를 전송해 준다. 그림 4는 본 논문에서 제안하는 데이터베이스에 저장된 정보들을 나타낸 것이다.
- *리더(Reader, R)* : 리더는 별도의 저장 능력과 계

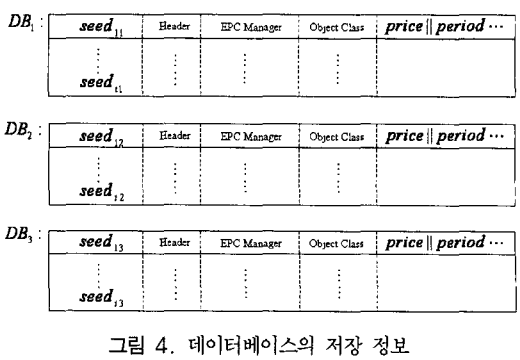


그림 4. 데이터베이스의 저장 정보

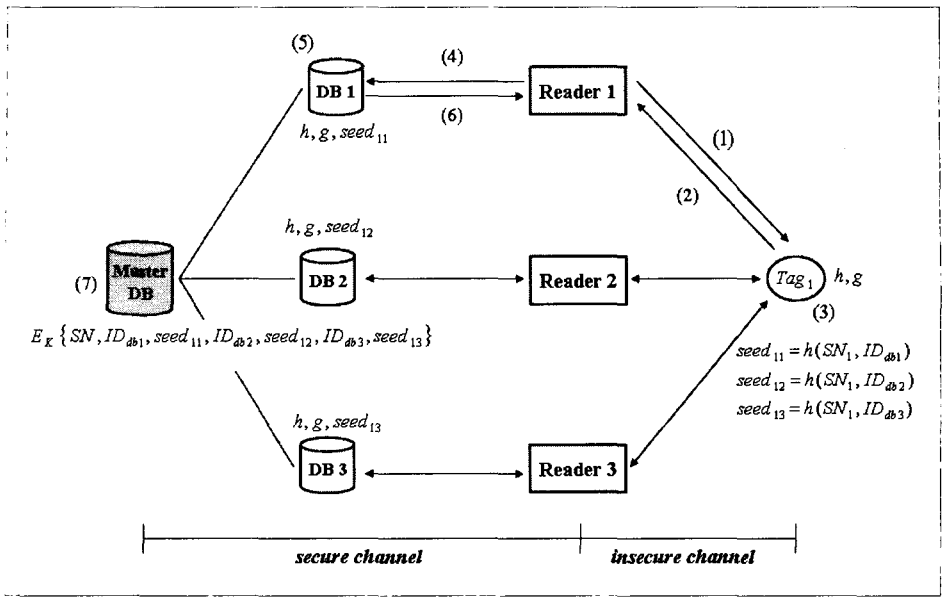


그림 5. 제안하는 RFID 시스템

산 능력을 필요로 하지 않으며, 태그로부터 수신한 정보를 데이터베이스에 전송하고, 데이터베이스에 의해 수행된 인증 정보를 수신하여 태그의 정당성을 판별한다.

- *태그(Tag, T)* : 본 논문에서 제안하는 태그는 기존의 방식과는 달리 실제 시리얼 번호 대신 이에 해당하는 *seed* 값을 저장하고 있다. 태그에는 실제 시리얼 번호가 저장되어 있지 않으므로 사용자의 프라이버시를 제공할 수 있으며, 리더의 요청에 대해 매번 다른 값을 전송하게 되므로 트래킹이 불가능하다.

2. 동작 과정

제안하는 RFID 시스템의 동작 과정은 다음과 같다.(그림 5 참조)

(1) R_1은 T_1에게 자신의 *ID*와 자신이 연결되어 있는 *DB*의 *ID*를 포함하는 query를 보내고 T_1의 응답을 기다린다.

$$R_1 \rightarrow T_1 : query = \{ID_{R1} \,||\, ID_{db1}\}$$

(2) R_1의 query를 수신한 T_1은 *DB*의 *ID*를 확인한 후, 이에 해당하는 $seed_{11}$의 해쉬 값을 R_1에게 전송한다. (여기서, $g()$, $h()$는 일방향 해쉬 함수이다.)

$$T_1 \rightarrow R_1 : g(seed_{11}) = g(h(SN_1, ID_{db1}))$$

(3) T_1은 해쉬 함수 h를 사용하여 $seed_{11}$ 값을 다음과 같이 갱신한다.

$$seed_{11} \rightarrow seed_{11}' : h(seed_{11}) = h(h(SN_1, ID_{db1}))$$

R_1의 query에 의한 T_1의 첫 번째 응답이 완료된 후, T_1에 저장되는 정보는 다음과 같다.

$$seed_{11}' = h(h(SN_1, ID_{db1}))$$
$$seed_{12} = h(SN_1, ID_{db2})$$
$$seed_{13} = h(SN_1, ID_{db3}))$$

(4) R_1은 T_1으로부터 수신한 데이터를 자신과 연결되어 있는 DB_1에게 자신의 *ID*와 함께 전송하고 응답을 기다린다.

$$R_1 \rightarrow DB_1 : \{ID_{R1} \,||\, g(seed_{11})\}$$

(5) DB_1은 저장되어 있는 모든 $seed_{i1}$값에 대해 $g(seed_{i1})$ 값을 구하고 수신한 값과 동일한 값을 찾는다.

$$computed\ g(seed_{i1}) \stackrel{?}{=} received\ g(seed_{11})$$

(6) DB_1은 위의 (5)번 과정에서 일치하는 값을 찾으면 T_1을 인증하고, T_1에 해당하는 정보를 R_1에게 전송한다.

$$DB_1 \rightarrow R_1 : \{ID_{db1} \,||\, price \,||\, valid\ period \ ...\}$$

R_1은 위의 값을 수신하여 T_1이 정당한 태그임을 인증하고, 수신한 정보를 사용하여 과금 등을 수행하게 된다.

(7) 필요한 경우, DB의 요청에 의해 마스터 데이터베이스는 소유하고 있는 마스터키 K를 이용하여 T_1의 실제 시리얼 번호를 복구 할 수 있다.

3. Examples

[Example 1] R_1과 T_1의 재 통신

T_1이 R_1과 첫 번째 통신을 완료한 후, R_1과 T_1의 두 번째 통신이 필요한 경우를 예를 들어 살펴보면 다음과 같다. 먼저 T_1에 저장되어 있는 정보는 다음과 같으며, R_1의 요청에 대해 다음과 같은 순서로 응답한다.

- T_1의 저장정보 : $seed_{11}' = h(h(SN_1, ID_{db1}))$
  $seed_{12} = h(SN_1, ID_{db2})$
  $seed_{13} = h(SN_1, ID_{db3}))$

① R_1은 T_1에게 query를 보내고 응답을 기다린다.

$$R_1 \rightarrow T_1 : query = \{ID_{R1} \parallel ID_{db1}\}$$

② R_1의 query를 수신한 T_1은 DB의 ID를 확인한 후, $seed_{11}'$을 R_1에게 전송한다.

$$T_1 \rightarrow R_1 : g(seed_{11}') = g(h(h(SN_1, ID_{db1})))$$

③ T_1은 해쉬 함수 h를 사용하여 $seed_{11}'$값을 다음과 같이 갱신한다.

$$seed_{11}' \rightarrow seed_{11}'' : h(seed_{11}') = h(h(h(SN_1, ID_{db1})))$$

두 번째 응답 후, T_1에 저장되는 정보는 다음과 같다.

$$seed_{11}'' = h(h(h(SN_1, ID_{db1})))$$
$$seed_{12} = h(SN_1, ID_{db2})$$
$$seed_{13} = h(SN_1, ID_{db3}))$$

④ R_1은 수신한 데이터를 DB_1에게 전송하고 응답을 기다린다.

$$R_1 \rightarrow DB_1 : \{ID_{R1} \parallel g(seed_{11}')\}$$

⑤ R_1으로부터 데이터를 수신 한 후, DB_1은 저장되어 있는 모든 $seed_{i1}$값에 대해 해쉬 값을 구하고 수신한 값과 동일한 값을 찾는다.

$$computed\ g(h(seed_{i1})) \stackrel{?}{=} received\ g(seed_{11}')$$

⑥ DB_1은 일치하는 값을 찾아 T_1을 인증하고, T_1에 해당하는 정보를 R_1에게 전송한다.

$$DB_1 \rightarrow R_1 : \{ID_{db1} \parallel price \parallel valid\ period\ ...\}$$

R_1은 위의 값을 수신하여 T_1이 정당한 태그임을 인증하고, 수신한 정보를 사용하여 과금 등을 수행하게 된다.

[Example 2] R_2와 T_1의 통신

T_1이 R_2와 첫 번째 통신을 수행하는 경우, T_1에 저장되어 있는 정보는 다음과 같으며 R_2의 요청에 대해 다음과 같은 순서로 응답한다.

- T_1의 저장정보 : $seed_{11} = h(SN_1, ID_{db1})$
  $seed_{12} = h(SN_1, ID_{db2})$
  $seed_{13} = h(SN_1, ID_{db3}))$

① R_2는 T_1에게 query를 보내고 응답을 기다린다.

$$R_2 \rightarrow T_1 : query = \{ID_{R2} \parallel ID_{db2}\}$$

② R_2의 query를 수신한 T_1은 DB의 ID를 확인한 후, $seed_{12}$을 R_2에게 전송한다.

$$T_1 \rightarrow R_2 : g(seed_{12}) = g(h(SN_1, ID_{db2}))$$

③ T_1은 해쉬 함수 h를 사용하여 $seed_{12}$ 값을 다음과 같이 갱신한다.

$$seed_{12} \rightarrow seed_{12}' : h(seed_{12}) = h(h(SN_1, ID_{db2}))$$

두 번째 응답 후, T_1에 저장되는 정보는 다음과 같다.

$$seed_{11} = h(SN_1, ID_{db1})$$
$$seed_{12}' = h(h(SN_1, ID_{db2}))$$
$$seed_{13} = h(SN_1, ID_{db3}))$$

④ R_2는 수신한 데이터를 DB_2에게 전송하고 응답을 기다린다.

$$R_2 \rightarrow DB_2 : \{ID_{R2} \parallel g(seed_{12})\}$$

⑤ R_2로부터 데이터를 수신 한 후, DB_2는 저장되어 있는 모든 $seed_{i2}$값에 대해서 해쉬 값을 구하고, 수신한 값과 동일한 값을 찾는다.

$$computed\ g(h(seed_{i2})) \stackrel{?}{=} received\ g(seed_{12})$$

⑥ DB_2는 일치하는 값을 찾아 T_1을 인증하고, T_1에 해당하는 정보를 R_2에게 전송한다.

$$DB_2 \rightarrow R_2 : \{ID_{db2} \parallel price \parallel valid\ period\ ...\}$$

R_2는 위의 값을 수신하여 T_1이 정당한 태그임을 인증하고, 수신한 정보를 사용하여 과금 등을 수행하게 된다.

V. 제안하는 RFID 시스템의 안전성

기존의 RFID 시스템에서 리더의 query에 대해 태그는 시리얼 번호와 같은 고정된 정보를 응답으로 전송하므로, 공격자에 의한 트래킹이 가능하고 이를 이용한 사용자의 프라이버시 침해 문제가 발생하게 되었다. 그러나 제안하는 RFID 시스템에서는 태그가 자신의 실제 시리얼 번호가 아닌 이를 이용하여 생성된 *seed* 값을 응답으로 전송하며, 태그의 응답은 동일한 리더에 대해서도 매 세션마다 서로 다른 값이 생성된다. 따라서, 공격자에 의한 트래킹이 불가능하며 사용자의 프라이버시를 효율적으로 보호할 수 있다는 장점이 있다. 또한, 태그가 응답 정보를 생성하기 위해서는 해쉬 값의 계산만을 필요로 하므로 비교적 적은 양의 연산을 요구한다.

본 절에서는 제안하는 RFID 시스템이 3장에서 설명한 보안 요구사항을 만족하는 지에 대해 설명한다.

(1) *도청 공격에 대한 안전성* : 제안하는 시스템에서 태그가 리더에게 전송하는 응답은 해쉬 값 $g(seed_{11})$과 같은 형태이다. 따라서, *SHA-1*이나 *MD5*와 같이 안전한 일방향 해쉬 함수를 이용한다면, 공격자가 태그와 리더의 통신 내용을 도청하더라도 전송정보로부터 실제 $seed_{ij}$ 값이나 시리얼 번호(SN_i)를 알아내는 것은 계산상 불가능하다.

(2) *재 전송 공격에 대한 안전성* : 제안하는 시스템에서 재 전송 공격은 두 가지 경우로 나누어 생각할 수 있다. 먼저, 첫 번째는 공격자가 T_1과 R_1의 첫 번째 통신을 도청하고, 이를 이용하여 R_1에게 정당한 T_1으로 위장할 수 있는 두 번째 응답을 생성하는 것이다. 즉, 공격자는 $g(seed_{11})$을 도청하고, 이 정보를 이용하여 자신을 정당한 T_1으로 인증받을 수 있는 새로운 응답을 생성하여 리더에게 전송하려 한다고 가정하자. 이 경우에, T_1과 R_1의 두 번째 통신에서 정당한 태그로 인증받기 위해서는 $g(seed_{11}')$ 값을 계산해야 하며, $seed_{11}' = h(seed_{11})$이다. 이 경우, 제안하는 시스템에서 안전한 일방향 해쉬 함수를 사용한다면 공격자가 $g(seed_{11})$으로부터 $seed_{11}$을 구하는 것은 계산상 불가능하므로 공격자가 $g(seed_{11}')$ 값을 계산하는 것은 불가능하다.

두 번째 경우는 공격자가 T_1과 R_1의 통신을 도청하고, 이를 이용하여 R_2에게 정당한 태그로 인증 받을 수 있는 응답을 생성하려는 경우이다. 즉, 이 경우에 공격자는 도청한 $g(seed_{11})$을 이용하여, $g(seed_{12})$ 값을 생성해야 한다. 제안하는 시스템에서 $seed_{11} = h(SN_1, ID_{db1})$이고 $seed_{12} = h(SN_1, ID_{db2})$ 이므로, 안전한 해쉬 함수를 사용하고 태그의 실제 시리얼 번호 SN_1이 노출되지 않는 한 재 전송 공격은 불가능하다.

(3) *리더로 위장하는 공격에 대한 안전성* : 제안하는 시스템에서 리더는 태그에게 query를 전송한 후 태그의 응답을 받아 이를 데이터베이스에 전달하고, 데이터베이스로부터 정당한 태그인지 아닌지 결과를 받는 역할만을 수행한다. 즉, 리더는 정보의 저장이나 생성 등에 관여하지 않는다. 따라서, 공격자가 정당한 리더로 위장하여 태그에게 query를 전송하더라도 공격자가 태그안의 저장된 데이터와 관련된 유용한 정보를 알아내는 것은 불가능하다.

(4) *트래킹에 대한 안전성* : 제안하는 시스템에서 동일한 태그와 리더간의 통신이라 할지라도, 태그의 응답 정보가 세션마다 변하므로 임의의 공격자가 태그의 응답 정보간의 상관관계를 알아내는 것은 불가능하다. 즉, 공격자가 T_1과 R_1의 첫 번째 통신에서 전송되는 $g(seed_{11})$과 T_1과 R_1의 두 번째 통신 $g(seed_{11}')$ 값을 얻게 되더라도, 이 정보들이 동일한 시리얼 번호 SN_1로부터 생성된 값인지를 알아내는 것은 계산상 불가능하다. 따라서 제안하는 시스템에서는 공격자에 의한 트래킹이 불가능하며, 태그의 응답 정보들의 상관관계를 판별하여 동일한 태그를 소유한 사용자의 위치 정보를 트래킹하는 것은 불가능하다. 즉, 태그를 소유한 사용자의 위치 정보에 대한 프라이버시를 제공한다.

(5) *사용자의 프라이버시 보호* : 제안하는 시스템에서 태그와 리더간의 통신 과정 중에 태그의 실제 시리얼 번호가 전송되지 않으므로, 리더는 태그가 정당한 태그인지 여부만을 판별할 수 있다. 따라서, 사용자가 인식하지 못하는 사이에 리더와 태그 간의 통신을 통해 사용자가 소유한 상품들의 실제 시리얼 번호가 노출됨으로써 이를 통해 소유한 상품이나 구매 패턴 등 사용자의 프라이버시와 관련된 정보가 노출되는 것을 방지할 수 있다.

(6) ***Unlinkability*** : 제안하는 시스템에서는 동일한 태그라 할지라도, 쿼리를 보낸 리더와 연결된 데이터베이스에 따라 서로 다른 응답을 전송한다. 즉, T_1은 DB_1과 연결된 R_1의 쿼리를 받는 경우에는 $g(seed_{11})$을 응답하고, DB_2와 연결된 R_2의 쿼리에 대해서는 $g(seed_{12})$을 응답한다. 이러한 경우에, 데이터베이스 간의 공모를 통해 수신된 응답 정보가

표 1. 기존 시스템과 제안하는 RFID 시스템의 안전성 비교

	해쉬 락 프로토콜	확장된 해쉬 락	해쉬 체인 방식	제안하는 시스템
도청	안전하지 않음	안전	안전	안전
재 전송 공격	안전하지 않음	안전	안전	안전
트래킹	안전하지 않음	안전	안전	안전
Unlinkability	제공하지 않음	제공하지 않음	제공하지 않음	제공
추적 가능성	-	-	-	제공

동일한 태그로부터 나온 것인지를 판별할 수 있다면, 데이터베이스간의 공모를 통해 태그를 소유한 사용자의 위치 정보 등을 알아낼 수 있게 된다. 그러나 제안하는 시스템에서는 데이터베이스들도 각 태그의 실제 시리얼 번호를 알지 못하므로, 안전한 해쉬 함수를 사용하고 태그의 마스터 데이터베이스에 암호화되어 저장되어 있는 실제 시리얼 번호 SN_i가 노출되지 않는 한 데이터베이스 간의 공모를 통해 태그의 응답들의 상관관계를 알아내는 것은 불가능하다.

(7) *추적 가능성* : 제안하는 시스템에서 실제 태그의 시리얼 번호는 마스터 데이터베이스에 암호화되어 저장되어 있다. 따라서 태그의 실제 시리얼 번호를 추적할 필요가 있는 경우에는, 비밀키를 알고 있는 인가된 관리자의 접근에 의해 각 태그의 시리얼 번호를 획득할 수 있는 방법을 제공한다.

표 1은 사용자의 프라이버시를 보호하기 위해 제안된 기존의 RFID 인증 시스템과 본 논문에서 제안하는 시스템의 안전성을 비교한 것이다.

VI. 결 론

RFID 기술은 저 비용의 무선 인식 메모리 태그로 인식 속도가 빠르고 바코드에 비해 상대적으로 많은 저장 능력을 가지고 있어, 물류 및 유통 시스템에서 바코드를 대체할 수 있는 차세대 기술로 기대되고 있다. 그러나 RFID를 이용한 개체 인식 기술은 리더와 태그 사이에 물리적인 접촉 없이 인식이 가능하고 태그의 정보가 전송될 수 있으므로, 이로 인한 사용자의 프라이버시 침해를 야기시킨다는 문제점을 가지고 있다. 지금까지 사용자의 프라이버시를 보호할 수 있는 RFID 시스템에 관한 몇몇 연구 결과가 발표되었으나 제안된 방식들은 각각 안전성과 효율성 면에서 몇 가지 문제점을 가지고 있다.

본 논문에서는 태그에서 리더로 전송되는 정보가 매 세션마다 변경되므로 공격자에 의한 트래킹이 불가능하고, 태그의 실제 시리얼 번호가 노출되지 않으므로 사용자의 프라이버시를 안전하게 보호할 수 있는 안전한 RFID 시스템을 제안하였다.

제안하는 RFID 시스템은 공격자가 리더와 태그간의 정보를 도청함으로써 태그안의 실제 시리얼 번호와 같은 비밀 정보를 알아내는 것이 불가능하고, 이전 세션에 도청한 정보를 재 전송하여 정당한 태그로 인증 받는 재 전송 공격이 불가능하다. 또한, 동일한 리더가 동일한 태그를 인증하는 경우에도 전송하는 정보가 매 세션마다 변경되므로 공격자의 트래킹이 불가능하며, 사용자의 위치 정보나 소유한 상품에 대한 정보 노출 등 사용자의 프라이버시 침해 문제를 해결할 수 있다. 그리고 각 데이터베이스에도 태그의 실제 시리얼 번호가 저장되어 있지 않으므로, 데이터베이스 간의 연동을 통해 태그의 응답 정보들 간의 상관관계를 알아내는 것이 불가능하므로 unlinkability를 제공한다. 그러나, 마스터 데이터베이스에 태그의 실제 시리얼 번호를 암호화하여 보관하므로, 필요한 경우에는 허가된 관리자에 의해 태그의 실제 시리얼 번호를 식별할 수 있는 방법을 제공한다.

제안하는 사용자의 프라이버시 보호가 가능한 RFID 시스템은 기존의 바코드 시스템을 대체할 수 있는 효율적인 물류 관리 시스템에 적용가능 할 것으로 기대한다.

참 고 문 헌

[1] D. L. Brock, "The electronic product code (EPC): A naming scheme for objects", *Technical Report MIT-AUTOID-WH-002*, MIT Auto ID Center, 2001.

[2] D. L. Brock, "EPC Tag Data Specification", *Technical Report, MIT-AUTOID-WH-025*, MIT Auto ID Center, 2003.

[3] D. Engels, "EPC-256 : The 256-bit Electronic Product Code Representation", *Technical Report MIT-AUTOID-WH-010*, MIT Auto ID Center,

2003.

[4] K. Finkenzeller. *RFID Handbook*, John Wiley and Sons. 1999.

[5] A. Juels and R. Pappu, "Squealing Euros : Privacy protection in RFID-enabled banknotes", *Financial Cryptography'03*, LNCS 2742, pp. 103-121, Springer-Verlag, 2003.

[6] A. Juels, R. L. Rivest and M. Szydlo, "The Blocker Tag : Selective Blocking of RFID Tags for Consumer Privacy", *10th ACM Conference on Computer and Communications Security*, CCS 2003, pp. 103-111, 2003.

[7] MIT Auto-ID Center, http://www.autoidcenter.org.

[8] M. Ohkubo, K. Suzuki, and S. Kinoshita, "A Cryptographic Approach to "Privacy-Friendly" tag", *RFID Privacy Workshop*, Nov 2003.

[9] S. E. Sarma, "Towards the five-cent tag", Technical Report, *MIT-AUTOID-WH-006*, MIT Auto ID Center, 2001.

[10] S. E. Sarma, S. A. Weis, and D. W. Engels, "RFID systems, security and privacy implications", *Technical Report MIT-AUTOID-WH-014*, AutoID Center, MIT, 2002.

[11] S. E. Sarma, S. A. Weis, and D. W. Engels, "Radio-frequency identification systems". *Workshop on Cryptographic Hardware and Embedded Systems*, CHES'02, LNCS 2523, pp. 454-469, Springer-Verlag, 2002.

[12] S. E. Sarma, S. A. Weis, and D. W. Engels, "Radio-frequency-identification security risks and challenges", *CryptoBytes*, 6(1), 2003.

[13] T. Scharfeld, "An Analysis of the Fundamental Constraints on Low Cost Passive Radio-Frequency Identification System Design", MS Thesis, Department of Mechanical Engineering, Massachusetts Institute of Technology, Cambridge, MA 02139, 2001.

[14] S. A. Weis, "Radio-frequency identification security and privacy", Master's thesis, M.I.T. May 2003.

[15] S. A. Weis, S. Sarma, R. Rivest, and D. Engels, "Security and privacy aspects of low-cost radio frequency identification systems", In *First International Conference on Security in Pervasive Computing 2003*, LNCS 2802, pp. 201-212, Springer-Verlag, 2004.

오 수 현 (Soo-hyun Oh) 정회원

1998년 2월 : 성균관대학교 정보공학과 졸업

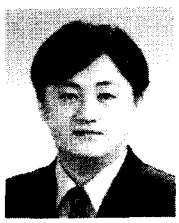
2000년 2월 : 성균관대학교 전기전자및컴퓨터공학부 대학원 졸업(공학석사)

2003년 8월 : 성균관대학교 전기전자및컴퓨터공 학부 대학원 졸업(공학박사)

2004년 3월 ~ 현재 : 호서대학교 컴퓨터공학부 정보보호 전공 전임강사

<관심분야> 암호 알고리즘/프로토콜, 유비쿼터스 보안

곽 진 (Jin-Kwak) 정회원



2000년 8월 : 성균관대학교 생물기전공학과 졸업

2003년 2월 : 성균관대학교 전기전자및컴퓨터공학부 대학원 졸업(공학석사)

2003년 3월~현재 : 성균관대학교 정보통신공학부 박사 과정

<관심분야> 암호 알고리즘/프로토콜, 유비쿼터스 보안