RFID 프라이버시 보호를 위한 향상된 모바일 에이전트 기법

정회원 김 수 철*, 여 상 수**, 김 성 권*

Enhanced Mobile Agent Scheme for RFID Privacy Protection

Soo-Cheol Kim*, Sang-Soo Yeo**, Sung Kwon Kim* ***Regular Members***

요 약

우리는 RFID(Radio Frequency Identification) 시스템이 여러 가지 장점과 응용으로 인하여 널리 사용되는 자동 인식기술이 될 것으로 전망한다. 그러나 프라이버시 침해 문제가 RFID 시스템의 대중화에 걸림돌이 되고 있다. 이와 같은 문제점을 해결하기 위해 많은 연구가 발표되었는데 대부분 암호학적 기법에 중점을 두고 있다. 그 외 모바일 장치를 프록시 에이전트로 사용하는 보안 기법이 있다. 일반적으로 에이전트는 고성능 CPU와 전원을 사용하는 높은 수준의 암호화 모듈을 가지며, 사용자 보안을 보장한다. 본 논문에서는 RFID 프라이버시 보호를 위한 향상된 모바일 에이전트 기법을 제안한다. 제안 기법은 이전 기법에 비해 도청 가능성을 줄이고 태그의 프로토콜 참여를 낮추었다. 그리고 서버도 공개키 암호를 사용하여 쉽게 에이전트를 인증할 수 있다. 또한 다른 에이전트 기법에서 문제시 된 에이전트 자체에 의한 위변조를 방지할 수 있는 장점을 가지고 있다.

Key Words : RFID Security, Privacy, Mobile Agent

ABSTRACT

We are sure that RFID system should be a widely used automatic identification system because of its various advantages and applications. However, many people know that invasions of privacy in RFID system is still critical problem that makes it difficult to be used. Many works for solving this problem have focused on light-weight cryptographic functioning in the RFID tag. An agent scheme is another approach that an agent device controls communications between the tag and the reader for protecting privacy. Generally an agent device has strong security modules and enough capability to process high-level cryptographic protocols and can guarantees consumer privacy. In this paper, we present an enhanced mobile agent for RFID privacy protection. In enhanced MARP, we modified some phases of the original MARP to reduce the probability of successful eavesdropping and to reduce the number of tag's protocol participation. And back-end server can authenticate mobile agents more easily using public key cryptography in this scheme. It guarantees not only privacy protection but also preventing forgery.

Ⅰ. 서 론

RFID(Radio Frequency Identification)는 IC칩에 내장된 정보를 무선 주파수를 이용하여 비접촉방식으로 읽어내는 기술로서 대상을 자동식별 할 수 있다. 일반적으로 RFID 태그에 사용 목적에 알맞은

※ 이 논문은 2005년도 정부(과학기술부)의 재원으로 한국과학재단의 지원을 받아 수행된 연구임(No. R01-2005-000-10568-0)
* 중앙대학교 컴퓨터공학부 알고리즘 및 정보보호 연구실(sckim@alg.cse.cau.ac.kr)
** 큐슈대학교 정보공학부 (ssyeo@itslab.csece.kyushu-u.ac.jp)
논문번호 : KICS2007-06-287, 접수일자 : 2007년 6월 29일, 최종논문접수일자 : 2008년 1월 4일

정보를 저장하여 적용 대상에 부착하여 사용한다. 그 후 판독기에 해당하는 RFID 리더를 통하여 태그 내의 정보를 인식한다. RFID 시스템은 바코드 시스템에 비해 보다 다양하고 효율적인 식별 체계 구축이 가능하다. 따라서 수년 내로 RFID 시스템이 바코드 시스템을 대신하여 유통, 물류 산업 등의 다양한 분야에 큰 변화를 줄 것이라고 전망하고 있다[1][2][3].

그러나 물리적 접촉 없이 무선으로 인식 가능하다는 RFID 시스템의 특징은 프라이버시 측면에서 새로운 문제점을 발생시킨다. 현재의 RFID 태그는 인증 프로토콜을 거치지 않고 어떤 리더에게나 태그 내부의 고유한 값을 응답 해준다. 따라서 RFID 리더를 가진 사람이라면 누구나 태그 정보를 읽어낼 수 있기 때문에, 태그가 삽입된 물품을 소유한 사람의 프라이버시가 쉽게 침해당할 수 있다[4].

RFID 시스템의 프라이버시 침해 문제는 크게 정보 유출과 위치 추적으로 분류할 수 있다. 첫째, 정보 유출(Information Leakage)은 태그 안의 직접적인 식별 정보나 고유한 아이디가 리더를 가진 모든 사람에게 전송이 된다는 것을 의미한다. 개인이 소지하고 있는 물품은 그 사람의 생활환경, 소득 수준, 소비 경향, 신체조건 등을 반영하기 때문에 태그의 정보 유출로 인한 프라이버시 침해는 상당한 수준이라고 보아야 할 것이다. 몇 년 안에 거의 모든 물품에 RFID 태그가 삽입되는 환경이 올 것으로 예상되는 현 시점에서, 태그로 인한 정보 유출과 프라이버시 침해는 큰 문제로 고려되어야 한다[5].

둘째, 위치 추적(Location Tracking)은 각각의 태그가 항상 동일한 값을 송신하는 데서 오는 문제이다. 이로 인해 리더를 가진 공격자는 특정 태그 소유자의 위치를 추적 할 수 있다. 사용자는 태그가 내장된 물건을 지니고 다니므로 공격자는 태그 고유 정보를 이용하여 사용자의 이동 경로를 쉽게 추적할 수 있다. 결국 태그를 가진 사람의 위치추적은 심각한 프라이버시 침해로 보아야 한다[6].

본 논문에서는 모바일 기기를 사용하여 높은 수준의 프라이버시 보호가 가능한 기법을 제안한다. 제안하는 기법은 특별한 모바일 기기가 태그내의 정보들을 일부 획득한 후 태그들을 관리하며 태그의 역할을 대신하는 것이다. 처리 능력에 한계가 있는 저가형 태그가 수행하기 어려운 높은 수준의 암호화 작업을 모바일 기기에서는 간단하게 할 수 있다. 제안하는 기법은 태그에 적은 연산량을 요구하기 때문에 저가의 태그에도 도입 가능하며 현재 RFID 시스템에 큰 변경 없이 추가적인 구성요소로 적용 가능하다.

본 논문의 구성은 다음과 같다. Ⅱ장에서는 기존에 제안된 기법들에 대해 분석한다. 특히 이전에 발표된 모바일 에이전트 기법에 대하여 자세히 설명하고 분석한다. Ⅲ장에서는 기존의 기법보다 향상된 기법을 제안한다. Ⅳ장에서는 제안하는 기법의 분석 및 평가를 한다. 마지막으로 Ⅴ장에서는 결론을 맺는다.

Ⅱ. 기존의 프라이버시 연구들과 그 접근 방식

RFID 프라이버시 보호 기법에 대한 많은 연구가 있다. 하지만 각각의 방법들이 완벽하게 프라이버시 보호 문제를 해결하진 못했다[7].

2.1 Kill 명령어

RFID 프라이버시 보호를 위한 가장 극단적인 방법은 사용자가 가게에서 물건을 사고 나면 태그를 파괴하거나 'Kill 명령어'를 작동시켜 태그의 사용을 영구적으로 중지시키는 것이다. 이 'Kill 명령어'는 Auto-ID 센터에 의해 제안된 기법이며, EPC 태그에 기본적으로 포함되어 있다[3][6]. 특별한 코드 값(PIN)을 입력하면 태그안의 칩이 기능을 상실하게 되는 방법이다. 간단하고 가장 확실한 프라이버시 보호 방법이라고 볼 수 있지만, 잠재적인 RFID 시스템의 장점을 모두 포기하게 되기 때문에 좋지 않은 접근 방법이다.

2.2 Blocker 태그

Juels는 일반 태그를 보호하기 위한 새로운 형태의 'Blocker 태그'를 제안하였다[8]. 이 방식은 태그-리더간의 사용되는 충돌 방지 프로토콜을 역이용하는 기법이다. 태그가 리더의 모든 질의에 응답을 하기 때문에 리더의 하나의 태그를 구분해낼 수 없게 된다. 따라서 특정 태그의 존재 여부를 숨기고, 리더가 중도에 태그 인식을 포기하게 만든다. 이 기법은 사용자가 'Blocker 태그'라는 도구를 가지고 다녀야 한다는 단점이 있다. 또한 'Blocker 태그'는 정상적인 태그의 기능을 못하게 하는 도구로 악용 가능성이 존재한다.

2.3 해시 기반 인증 기법

S.Weis 등은 해시를 기반으로 하여 메타 아이디

(metaID)를 사용하는 기법을 제안하였다[6]. 이 기법에서 태그는 잠긴(locked) 모드 열린(unlocked) 모드의 두 가지 모드를 가진다. 태그가 잠긴 모드일 경우 단지 메타 아이디(metaID)만 전송한다. 인증된 리더만 메타 아이디를 기반으로 백엔드 서버에서 키값을 찾을 수 있다. 이 기법은 태그 안에 있는 식별 정보를 인증된 리더에게만 주게 함으로써, 기밀성을 보장하려는 기법이다. 그러나 공격자의 재전송, 스푸핑 공격에 안전하지 않다. 또한 잠긴 모드의 태그는 항상 같은 메타 아이디를 송신하기 때문에 위치 추적 문제를 해결하지 못했다.

그 문제를 해결하기 위해 S.Weis 등이 두 번째로 제안한 'randomized hash-lock' 기법이 있다[6]. 그전 기법을 보안하기 위하여 리더의 질의에 대해서 태그가 항상 랜덤한 값을 응답할 수 있도록 하는 기법이다. 하지만 이 기법은 인증된 리더가 태그의 잠긴 모드를 풀어주는 과정을 도청하는 공격자에게 태그의 비밀이 드러날 수 있다는 문제점이 있다. 또한 관리하는 태그가 많으면 많을수록 하나의 태그를 식별하기 위해서 서버가 계산하는 시간이 늘어난다는 단점이 있다[9].

2.4 모바일 에이전트 기법

그 외 모바일 기기(mobile device)를 사용하여 태그와 리더 사이의 통신을 중재하는 기법도 있다[10][11][12]. 본 논문에서 제안한 개념과 유사한 개념이다. 태그의 하드웨어적 제약사항이 근본적인 문제가 되기 때문에, 이전까지의 기법들은 한계를 가질 수 밖에 없었다. 하지만 모바일 기기를 사용한 기법은 기존의 통신 보안 기술을 그대로 이용할 수 있다. 그리고 프라이버시 보호 기능 외에 다른 여러 가지 부가 기능을 할 수 있는 장점도 있다.

예를 들어 Rieback이 발표한 'RFID Guardian' 기법에서도 모바일 기기를 사용한다[10]. 이 기기의 기능은 크게 4가지로 나뉘는데 첫 번째로 새로운 태그나 새로운 리더를 감시하는 역할을 한다. 리더의 스캔이 있을시 사용자에게 알려주어 대비하게 하고 Guardian 주위에 새로운 태그가 나타났을 시에도 알려준다. Guardian이 태그와 리더의 역할을 동시에 수행하는 것이다. 두 번째로 태그를 대신하여 키를 관리하는 역할을 한다. 태그의 키를 사용하여 리더와 통신을 할 수 있고 또한 Guardian의 의사난수기를 이용하여 태그의 키를 새로 설정해 줄 수도 있다. 세 번째로 태그나 리더의 접근을 제어해 주는 역할을 한다. 예를 들면 RFID Guadrdian은 RFID 보안 메커니즘의 자동화를 제공한다. 사용자가 태그를 사용하기 편하게 도와주는 것이다. 그리고 현재 위치와 시간 정보를 이용하여 태그의 활용도를 높여준다. 또한 선택적인 RFID 재밍을 통하여 접근 제어를 한다. 네 번째로 태그를 대신하여 리더가 정당한 리더인지 인증해주는 역할을 한다. 하지만 이 기법은 에이전트의 역할을 구분지어 간단하게 설명을 했을 뿐 실제 에이전트의 동작에 대해서는 언급하지 않았다.

다른 모바일 에이전트 기법으로는 Jeuls가 발표한 REP(RFID Enhancer Proxy)가 있다[12]. 이 기법은 모바일 에이전트가 태그 내의 모든 정보를 획득하여 태그를 대신하는 것이다. REP라고 불리는 에이전트는 4가지의 역할을 수행한다. 우선 REP는 태그 내의 모든 정보를 획득할 수 있다. 그리고 REP는 도청과 PIN 추적의 가능성을 피하기 위하여 Re-Encrypt를 통하여 태그 내의 정보를 다시 쓸 수 있다. 태그 내의 정보를 획득한 REP는 태그를 대신할 수 있다. 이 상태에서는 'Soft Blocking'을 이용하여 프라이버시를 보호한다. 마지막으로 REP가 획득한 태그를 일반 태그로 풀어줄 때 자신이 가진 정보를 다시 써서 이전 상태로 돌려줄 수 있다. 하지만 이 기법은 에이전트가 태그에 대해 너무 강력한 권한을 가지고 있기 때문에 태그에 대한 정보를 무작위로 위변조할 가능성이 있다. 역시 이 기법도 실제 에이전트의 동작에 대해서는 언급하지 않았다.

2.5 모바일 에이전트 기법(MARP)

본 절에서는 이전에 제안한 기법에 대하여 설명하겠다[13]. 이 기법에서 사용하는 에이전트(MARP)는 파워가 있고 많은 메모리를 가지고 있으며 높은 수준의 계산이 가능한 모바일 기기이다. RFID 사용자는 자신의 태그들을 모두 모바일 에이전트(mobile agent)에 등록 시킨 후 모바일 에이전트를 들고 다닌다. 모바일 에이전트가 태그 역할을 대신하는 것이다.

ARP 기법의 핵심은 태그의 비밀 정보 일부분을 모바일 에이전트에게 넘겨주는 것이다. 그 일부분의 비밀 정보를 사용하여 모바일 에이전트가 태그 대신 리더에게 인증 받게 하는 것이다. 모바일 에이전트는 사용자의 모든 태그들을 등록하여 데이터베이스화 한 후, 리더와의 공개키 암호화를 통한 상호 인증을 수행한다. 그 후 인증된 리더의 권한을 확인하고 적합한 태그 정보를 제공하는 것이다.

Juels가 제안한 REP기법에서는 태그는 모든 정

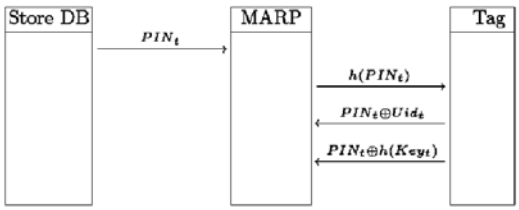

그림 1. MARP 논문에서의 태그 등록 과정

보를 에이전트에게 제공하였다. 이 점은 중대한 보안상 문제점을 발생시킨다. 모바일 에이전트는 자신에게 등록되어있는 태그가 해방된 이후에도 기존에 가지고 있던 정보로 태그를 소유하고 있다고 위조할 가능성이 생긴다. 그 외 소유권 이전과 같은 상황에서도 이전 사용자의 불법적인 공격 가능성이 해결하지 못했다. 그와 달리 MARP에서는 모바일 에이전트 자체에 의한 위변조 가능성도 생각하여 태그가 전체 정보를 넘기지 않고 일부만 넘겨서 차후에 태그 위변조 검사를 할 수 있게 하였다. 이 점은 태그 위변조 가능성을 크게 감소시켰다.

하지만 MARP 기법에는 다음과 같이 몇 가지 보안상 공격 가능성이 존재한다.

첫째, 그림 1의 태그 등록 과정에서 도청에 대한 대비가 부족한 점이다. 이전 논문에서는 태그의 계산량을 최대한으로 줄이고 다시 쓸 필요 없이 읽기 전용 태그에 초점을 두었기 때문에 생긴 문제점이다. 예를 들면 태그 등록 과정에서 PIN값을 보호하지 않고 보내기 때문에 악의적인 공격자가 쉽게 PIN을 갈취하여 태그 권한을 뺏는 경우가 생긴다. 이전에는 최대한 근접거리에서 등록한다고 했지만 리더의 기술이 발전함에 따라 먼 곳에서도 쉽게 도청이 가능하다.

둘째, 그림 2에서 이전 기법의 전체적인 프로토콜을 살펴보면 각 리더와 에이전트가 상호인증을 위해서 brute-force 방법을 통한 아이디 획득과 공개키를 설정하는 경우가 많다. 소규모의 리더와 에이전트가 존재하는 공간에서는 크게 문제시되지 않지만, 실제로 이 기법이 현실에 적용된다면 하나의 리더가 에이전트를 식별하는데 걸리는 시간이 너무 많이 걸릴 것이다. 보안이 유지되더라도 효율성이 떨어지면 문제가 있는 프로토콜이다.

마지막으로 태그 등록 후 과정에서는 위변조 방지를 위해서라지만 매번 태그와 서버의 인증을 수행하기 때문에 과부하가 많이 생긴다. 이전 기법에서는 태그 위변조에 대한 검사를 항상 수행했기 때문에 에이전트가 태그를 대신한다는 개념보다 태그

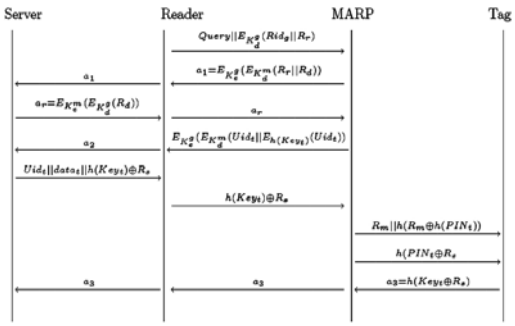

그림 2. MARP 논문에서의 에이전트 활동 단계

에서 하기 어려운 계산을 대신 처리해주는 방식이었다. 결국 리더가 스캔할 시 매번 태그에게 질의를 함으로서 효율적인 측면에서도 문제가 생기고 여러 번의 테스트는 공격자가 태그를 공격할 여지를 남겨두었다.

Ⅲ. 향상된 모바일 에이전트 기법(eMARP)

본 장에서는 이전 기법의 약점을 보완한 새로운 기법을 제안한다.

3.1 제안 기법에서의 RFID 시스템

RFID 시스템은 일반적으로 태그와, 리더, 백엔드 서버로 이루어져 있다. 본 논문에서는 리더와 태그를 중재해주는 개인 프라이버시 보호 에이전트가 추가된다. 또한, 공개키 암호화를 위해 공개키를 관리해주는 신뢰받는 공개키 데이터베이스 센터(PKC, Public Key Center)가 추가된다. 그림 3은 본 논문에서 제안하는 RFID의 시스템 구성을 나타낸 것이다.

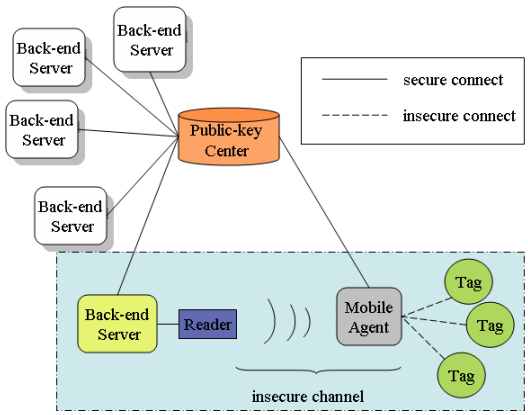

그림 3. 제안 기법에서의 RFID 시스템

- 태그(Tag, Transponder) : 태그는 IC 칩과 안테나로 이루어져 있다. 리더가 질의를 보내면, 내부에 가지고 있는 정보를 리더에서 송신해 주는 것이 태그의 일반적인 역할이다. RFID 태그는 크게 능동형 태그(active tag)와 수동형 태그(passive tag)로 나뉜다. 능동형 태그는 태그 자체에 배터리(battery)를 장착하고 있어서, 자체적인 연산 수행이 가능하며 데이터의 전송 범위도 수십 미터 정도까지 이른다. 수동형 태그는 태그 자체에 배터리가 없는 종류로서 리더 측에서 보내는 전자파를 이용하여 전원을 확보하도록 설계된다. 본 논문에서 사용되는 태그는 해시 연산이 가능한 수동형 태그로 가정한다.
- 리더(Reader, Transceiver) : 리더는 태그에 RF 신호를 송출하여 태그로부터 정보를 수신하는 장치이다. 리더가 전체 RFID 시스템에서 하는 역할은 태그에게 요청 신호를 보내고 태그로부터 정보를 받은 후, 백엔드 서버 시스템을 이용하여 태그를 식별하는 것이다. 본 논문에서는 리더들이 특정한 그룹을 가지고 그룹 아이디와 그룹 개인키, 공개키를 가지고 있다고 가정한다. 제안 기법에서는 리더 그룹 아이디로 태그로의 접근 권한을 구별 한다. 또한 리더는 모바일 에이전트와 일반 태그를 구분하여 통신할 수 있다.
- 백엔드 서버(Back-end Server) : 백엔드 서버는 리더로부터 전송되어 오는 정보를 처리해주는 서버 시스템이다. 백엔드 서버는 태그와 관련된 정보를 데이터베이스화해서 관리하고 있다. 백엔드 서버는 보안 측면에서 신뢰할 수 있는 시스템으로 간주된다. 각 서버는 공개키, 비밀키를 가지고 있고 공개키 센터에 자신의 공개키를 등록해둔다.
- 프라이버시 보호 에이전트(eMARP : Enhanced Mobile Agent for Privacy Protection) : 본 논문에서 제안하는 기법의 핵심 부분이다. RFID 시스템에서의 능력의 한계를 가지는 태그를 대신하는 역할을 한다. 태그의 비밀 정보를 일부 획득하여 태그를 대신한다. 그 외, 추가적인 태그 관리 능력이 있다. 프라이버시 보호 에이전트는 핸드폰이나 PDA를 가정하고 있으며 개인 사용자가 항시 소지하여 자신의 태그들을 관리한다. 에이전트는 높은 메모리와 강력한 계산능력을 가지고 있어 태그 내에서 구현하기 어려운 암호학적 기법들을 간단하게 처리할 수 있다. 따라서 안전한 RFID 시스템 구축에 큰 역할을 할 수 있다. 본 논문에서는 공개키 기반 암호를 사용하기 위해 각 에이전트도 공개키 쌍을 가지고 있다.
- 신뢰받는 공개키 센터(PKC : Trusted Public-key Center) : 제안 기법에서는 공개키를 이용한 상호인증을 사용한다. 제안 기법에서는 서버, 리더, eMARP가 공개키를 사용한다. 따라서 공개키를 관리하고 알려주는 신뢰받는 제 3자, 즉 공개키 분배 센터가 필요하다. 공개키 센터는 인증된 서버, 리더 eMARP의 공개키를 가지고 있고 분배하는 역할을 한다. 본 논문에서는 신뢰받는 공개키 센터와의 통신은 안전하다고 가정한다.

3.2 시스템 계수

제안하는 기법을 설명하기 위하여 필수한 시스템 계수들이다.

- $h()$: 일방향 해시 함수
- $\|$: 문자열 연접 연산
- Uid_t : 태그의 유일한 아이디
- $Data_t$: 태그와 관련된 데이터
- Key_t : 인증을 위한 태그의 비밀값
- PIN_t : 태그 모드 변경을 위한 키
- $\oplus$: Exclusive or 연산
- Rid_g : 리더 그룹 아이디
- K_d^g : 리더 그룹의 개인키
- K_e^g : 리더 그룹의 공개키
- Uid_{ma} : 모바일 에이전트의 유일한 아이디
- K_d^m : 모바일 에이전트의 개인키
- K_e^m : 모바일 에이전트의 공개키
- Sid_s : 리더 그룹 아이디
- K_d^S : 백엔드 서버의 개인키
- K_e^S : 백엔드 서버의 공개키
- R_r : 리더가 생성한 난수
- R_m : 모바일 에이전트가 생성한 난수
- R_s : 백엔드 서버가 생성한 난수

3.3 초기 설정 단계

제안 기법을 시행하려면 몇 가지 준비 사항이 필요하다. 일단 각 태그는 모드 변경키(PIN)를 가진

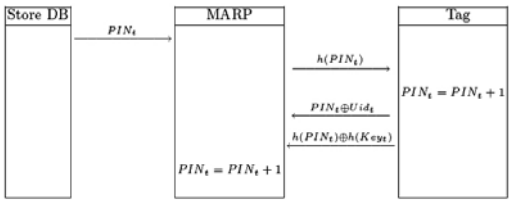

그림 4. 제안 기법에서의 태그 등록 단계

다. 그 키를 가진 에이전트만이 태그를 등록시킬 수 있다. 상점에서 물건을 진열할 경우 상점의 데이터베이스에 진열된 상품의 PIN을 저장해둔다. 그리고 상점에서 물건이 팔린 경우 개인의 모바일 에이전트에게로 PIN을 넘겨준다. 그 PIN을 사용해 구입한 물건을 에이전트에 등록시킬 수 있는 것이다.

MARP에서는 보호대책 없이 해시된 PIN값을 전송하여 도청의 가능성이 존재하였다. 흔히 사용되는 backward secure channel을 이용할 수도 있다. 즉 모바일 에이전트(리더의 역할을 함)가 태그에게 해시된 PIN값을 일방적으로 전송하는 대신 backward channel로 난수 R을 모바일 에이전트에게로 전송하고 모바일 에이전트가 난수와 PIN값을 해시하여 전송하면 보다 안전성을 높일 수 있을 것이다. 그러나 이 기법을 사용하려면 태그가 난수발생기를 가져야 하기 때문에 태그의 요구사항이 너무 커지게 된다. 따라서 다른 대안으로 인증이 끝나면 태그는 자신이 가지고 있는 PIN값을 업데이트하는 방법을 택한다. 그러면 공격자가 해시된 PIN값을 도청하더라도 PIN자체의 값을 알지 못하므로 다음번 등록 단계에 사용되는 값도 알지 못한다. 다음 그림 4는 제안 기법의 태그 등록 과정을 나타낸다.

[상세 프로토콜]

단계 1 : 상점 데이터베이스에서 안전한 채널을 통해 모바일 에이전트에게 물품태그의 PIN을 보낸다.

$$StoreDB \rightarrow MA : PIN_t$$

단계 2 : 모바일 에이전트는 태그에게 해시된 PIN을 보내어 인증 받는다.

$$MA \rightarrow Tag : h(PIN_t)$$

단계 3 : 태그는 자신이 가지고 있는 정보를 이용해 해시된 PIN값을 계산하여 비교해보고 일치하면 모바일 에이전트를 인증한다. 모바일 에이전트가 인증되면 PIN값을 업데이트 하여 재전송 공격을 방지한다. 그리고 태그는 자신의 비밀 정보(유일한 아이디와 해시된 비밀키)를 해시한 PIN과 XOR 연산 수행 후 보낸다. 그 후 무응답 모드로 들어간다. 만약 PIN값이 일치하지 않으면 PIN을 업데이트 하지 않고 태그는 아무런 반응도 보이지 않는다.

$$Tag : h(PIN_t) = h(PIN_t')\text{비교}$$
$$Tag : MA\text{인증}$$
$$Tag : PIN\text{ 업데이트 } (PIN_t = PIN_t + 1)$$
$$Tag \rightarrow MA : h(PIN_t) \oplus Uid_t \parallel h(PIN_t) \oplus h(Key_t)$$

단계 4 : 모바일 에이전트는 태그한테서 응답이 오면 PIN값을 업데이트 하여 사용한다. 태그가 보내온 정보들은 업데이트 한 PIN값으로 축출해 낸다. 만약 정당한 PIN값을 보냈는데도 태그가 무응답일 경우 태그와의 동기화가 깨졌으므로 PIN값을 PIN+1로 업데이트 하여 처음부터 다시 시도한다.

$$MA : PIN\text{ 업데이트 } (PIN_t = PIN_t + 1)$$
$$MA : \text{자신의 } DB\text{에 } Uid_t,\ h(Key_t),\ PIN_t\text{를 저장}$$
$$MA \rightarrow Tag : h(PIN_t \oplus Uid_t)$$

3.4 태그 등록 후 단계

태그가 등록 된 후 모바일 에이전트가 태그의 역할을 대신한다. 이 단계는 제안 기법의 가장 일반적인 단계이다. 여러 개의 모바일 에이전트가 존재할 경우 리더는 하나의 모바일 에이전트를 선택하여 통신을 시작한다. 그림 5는 eMARP의 태그 등록 후 일반적인 통신을 나타내고 있다.

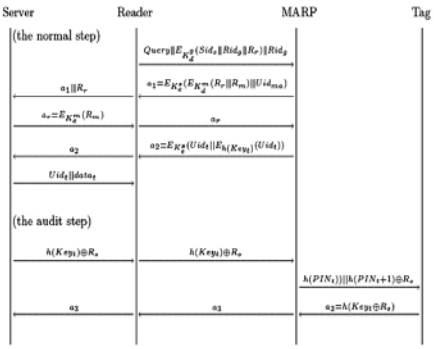

그림 5. 제안 기법에서의 에이전트 활동 단계

[상세 프로토콜]

1)일반적인 단계

단계 1 : 리더는 모바일 에이전트에게 자신의 그룹 아이디와 자신이 생성한 난수, 백엔드 서버 아이디를 리더그룹 개인키로 서명한 후 보낸다.

$$Reader \rightarrow MA : Query \| E_{K_d^g}(Sid_s \| Rid_g \| R_r) \| Rid_g$$

단계 2 : 모바일 에이전트는 리더가 보내온 정보를 확인하기 위해 다음과 같은 과정을 수행한다. 일단 리더그룹 아이디를 이용하여 신뢰받는 공개키 센터에서 리더그룹 공개키를 받아온다. 그리고 그 공개키를 사용하여 리더가 보내온 정보를 복호화 한다.

$$MA : Sid_s \| Rid_g \| R_r = D_{K_d^g}(E_{K_d^g}(Sid_s \| Rid_g \| R_r))$$

단계 3 : 모바일 에이전트는 난수 R_m을 생성한다. 그리고 리더가 보낸 난수와 자신이 생성한 난수를 모바일 에이전트 비밀키로 암호화한다. 암호화된 정보를 이용해 a_1을 만들어서 리더에게 보낸다. 서버의 공개키는 공개키 센터를 통하여 획득한다.

$$MA : \text{리더 그룹 아이디 } Rid_g \text{를 체크한다.}$$
$$MA : \text{난수 } R_m \text{을 만든다.}$$
$$MA \rightarrow Reader : a_1 = E_{K_e^s}(E_{K_d^{cm}}(R_m \| R_r) \| Uid_{ma})$$

단계 4 : 리더는 모바일 에이전트가 보내온 a_1과 자신이 생성한 난수 R_r을 백엔드 서버에 보낸다.

$$Reader \rightarrow Server : a_1 \| R_r$$

단계 5 : 백엔드 서버는 a_1을 통해 모바일 에이전트의 아이디를 알아낼 수 있다. 모바일 에이전트의 아이디를 알면 공개키 센터를 통하여 모바일 에이전트의 공개키도 알 수 있다. 그러면 모바일 에이전트가 보내온 암호화된 정보에서 난수 R_r을 알 수 있다. 만약 리더가 보내온 R_r과 에이전트가 보내온 R_r이 동일하다면 서버는 모바일 에이전트를 인증할 수 있다. 마지막으로 백엔드 서버는 모바일 에이전트가 생성한 난수 R_m을 모바일 에이전트의 공개키로 암호화하여 리더를 거쳐 모바일 에이전트에게 보낸다. 여기서 리더는 a_1을 복호화 할 수 없고 모바일 에이전트의 아이디를 알 수 없다.

$$Server : E_{K_d^{cm}}(R_r \| R_m) \| Uid_{ma} = D_{K_d^s}(a_1)$$
$$Server : Uid_{ma} \text{ 확인}, R_r \text{의 적합성 확인}$$
$$Server \rightarrow MA : a_r = E_{K_e^{cm}}(R_m)$$

단계 6 : 모바일 에이전트는 R_m을 확실함을 확인하면 상호인증은 종료된다. 그리고 모바일 에이전트는 등록된 태그의 정보를 백엔드 서버에게 공개키 암호 알고리즘을 이용해 보낸다.

$$MA : \text{정보 확인} = \text{상호인증 완료}$$
$$MA \rightarrow Server : a_2 = E_{K_e^s}(Uid_t \| E_{h(Key)}(Uid_t))$$

단계 7 : 백엔드 서버는 모바일 에이전트, 태그 아이디 쌍을 (Uid_{ma}, Uid_t) 데이터베이스에 저장한다. 이 아이디 쌍은 이후 태그 위변조 검사 단계를 시행을 결정할 때 사용한다. 만약 기본 단계에서 (Uid_{ma}, Uid_t) 아이디쌍이 변경되지 않으면 소유권 이전과 같은 상황이 발생하지 않았다는 증거이므로 서버는 간단하게 리더에게 태그 관련 정보 $(Uid_t \| data_t)$를 보내면 된다. 만약 저장된 (Uid_{ma}, Uid_t) 정보와 다른 경우가 발생한다면 태그 위변조 검사 단계를 진행시켜 프라이버시 보호를 한다.

$$Server : \text{받은 정보 복호화}$$
$$Server : (Uid_t, Uid_{ma}) \text{ 비교}$$
$$Server : (Uid_t, Uid_{ma}) \text{ 저장}$$
$$Seaver \rightarrow Rerder : Uid_t \| data_t$$

2) 태그 위변조 검사 단계

단계 8 : 만약 서버에 저장된 모바일 에이전트와 태그의 (Uid_{ma}, Uid_t) 조합과 다른 모바일 에이전트가 태그의 소유권을 주장하는 경우가 있을 수 있다. 불법적인 모바일 에이전트가 소유권을 주장하는 경우도 있을 수 있고, 원소유자가 다른 사람에게 소유권 이전을 한 경우 서버에 저장되어 있는 정보와는 다르다. 이럴 경우 새로운 사용자는 서버에 저장되어 있는 정보를 갱신해야 하는데 서버는 정보를 갱

신하기 전 확실한지 확인을 하는 단계가 필요하다. 우선 서버는 난수 R_s를 하나 생성한다. 그리고 해시된 태그의 비밀정보를 자신이 생성한 난수와 XOR 연산 수행 후 보낸다. 만약 이 위변조 검사 단계가 성공하면 백엔드 서버는 자신의 데이터베이스 정보를 수정한다. 그렇지 않고 위변조 검사 단계가 실패하면 인증을 거부하고 인증을 시도한 모바일 에이전트를 블랙리스트에 올린다.

$Server$: 위변조 검사 단계 시작
$Seaver \rightarrow Rerder \rightarrow MA : h(Key_t) \oplus R_s$

단계 9 : 모바일 에이전트는 저장되어 있는 해시된 비밀값을 이용하여 서버가 생성한 난수를 획득한다. 그리고 2가지 정보를 태그에게 보낸다. 우선 현재 모드 변경키를 보내어 자신이 마스터 모바일 에이전트임을 증명한다. 또한 다음번 모드 변경키인 $h(PIN_t+1)$ 과 서버의 난수 R_s를 XOR 연산 수행 후 보낸다.

$MA : R_s = h(Key_t) \oplus R_s \oplus h(Key_t)$ 계산
$MA \rightarrow Tag : h(PIN_t) \| h(PIN_t+1) \oplus R_s$

단계 10 : 태그는 모바일 에이전트가 보내온 정보를 분석한다. 이후 모바일 에이전트가 자신의 마스터 에이전트임을 확인한 후에만 응답한다. 태그는 자신이 가지고 있는 비밀정보 Key_t를 이용해 a_3을 만든다. 이 a_3을 모바일 에이전트와 리더를 거쳐 서버에게 보낸다. a_3에서 모바일 에이전트나 리더는 태그의 정보를 알 수 없다. 태그의 응답을 받은 서버는 정보를 확인해보고 태그를 인증하게 된다. 태그 인증이 되면 (Uid_{ma}, Uid_t) 정보를 갱신한다.

Tag : 모바일 에이전트 인증
$Tag \rightarrow Server : a_3 = h(Key_t \oplus R_s)$
$Server$: 태그 인증 , DB 업데이트

Ⅳ. 분 석

본 장에서는 제안 프로토콜에 대한 분석을 하고자 한다. 제안 방식은 저가형 태그에도 사용가능한 안전한 RFID 시스템 설계를 목적으로 한다. 다음은 RFID 시스템에 가능한 공격과 제안된 기법의 안정성을 설명한다.

- 도청/통신내용 분석 : 공격자가 프로토콜이 진행 도중에 흐르는 통신내용을 도청하거나 직접 태그나 리더에게 질의를 하여 통신내용 분석을 할 수 있다. 이와 같은 공격법은 RFID 프라이버시 문제에 치명적이다. 따라서 제안하는 기법에서는 안전을 위하여 매 세션마다 세션키 값으로 태그의 PIN이나 해시된 PIN을 사용한다. 그리고 사용된 PIN값을 업데이트 하여 리플레이 공격에 대비한다. 또한 중요한 세션마다 해시 연산을 수행하여 공격자가 도청을 하더라도 태그의 비밀정보를 알 수 없게 한다. 그리고 난수를 생성하여 사용하기 때문에 정당한 리더와 정당한 태그들만이 제안하는 프로토콜에 만족하는 정당한 메시지를 생성할 수 있다.
- 스푸핑 공격 : 이 공격은 공격자가 태그로부터 전송되는 데이터를 이용하여 리더를 속여 특정 태그인척 하는 것이다. 공격자는 리더로 위장하여 특정 태그의 정보를 얻는다. 제안하는 기법에서는 PIN을 알고 있는 정당한 리더와 에이전트만이 태그의 정보를 얻을 수 있다. 태그에서는 PIN값을 인증한 후에만 응답을 하기 때문에 이전 h(PIN)값으로는 태그의 정보를 얻어낼 수 없다. 그러므로 PIN을 알지 못하는 공격자는 태그의 정보를 알아낼 수 없다. 정당한 에이전트와 태그 사이의 정보를 도청하더라도 그 정보는 PIN 업데이트를 시행하기 때문에 소용이 없어진다.
- 위치 추적 : 공격자가 태그의 위치를 추적할 수 있으면 사용자의 프라이버시에 큰 문제가 된다. 제안하는 기법에서 위치 추적 가능성은 난수를 이용하기 때문에 불가능하다. 서버와 모바일 에이전트는 난수를 생성하여 매 세션마다 사용하므로 항시 응답값이 달라지고, 태그는 PIN값의 업데이트를 통해 추적 가능성을 막는다. 태그가 응답하는 값은 PIN을 업데이트 한 후 해시한 값이기 때문에 공격자가 태그의 다음 응답값을 예측할 수 없다. 또한 PIN을 확실하게 알지 못하면 응답하지 않기 때문에 위치 추적의 가능성은 없다.
- 태그 위변조 : 기존의 에이전트 기법들은 에이전트가 태그를 위조하거나 변조하여서 불법적인 이득을 획득하려는 시도를 막지 못하였다. 제안 기법에서는 모바일 에이전트데 의한 태그 내용의 위변조를 막을 수 있다. 모바일 에이전트에 등록된 태그가 해지되거나 소유권이 이전된 상

태에서는 위변조 가능성이 존재한다. 하지만 제안 기법에서는 인증 단계를 추가하여 새로운 소유자가 태그 소유자임을 인증 받을 수 있다. 따라서 이전 사용자가 저장된 정보를 이용하여 태그를 가진 것처럼 응답할 가능성을 배제시켰다.

eMARP 기법에서 태그는 해시 연산과 XOR 연산만을 수행한다. 제안 기법은 크게 태그 등록 단계와 모바일 에이전트에 태그가 등록된 단계로 나눌 수 있다. 초기화 단계에서 태그가 수행하는 일은 자신의 비밀 정보를 넘겨주는 일이다. 만약 PIN과 비밀키(Key)값을 해시한 후 저장해두고 있다면 모바일 에이전트가 보내온 값을 확인하는 절차와 PIN을 업데이트 하는 연산 그리고 비밀 정보를 넘겨주는 일을 수행한다. 결국 태그는 1번의 해시 연산과 3번의 XOR 연산만 수행하면 된다. 모바일 에이전트에 태그가 등록된 단계에서 태그가 수행하는 일은 서버와의 상호 인증 단계만 수행하면 된다. 모바일 에이전트가 보내온 정보를 분석하는데 한 번의 해시와 XOR 연산이 필요로 하고, 자신의 응답을 만들 때 한 번의 해시와 XOR 연산이 필요로 한다. 따라서 태그는 2번의 해시와 2번의 XOR 연산을 수행한다. 하지만 인증 단계는 소유권 이전과 같이 특별한 경우에만 이용된다. 따라서 인증 단계를 수행하지 않는 보통의 경우에 태그는 등록 단계의 연산을 제외하고는 연산을 하지 않는다.

표 1은 제안한 프로토콜과 기존의 시스템에 대해 비교 분석하여 평가한다. 기존에 에이전트 기법을 제외하고는 보안에 대하여 신경을 많이 썼지만 약점이 있거나 효율이 떨어졌다. 그리고 기존에 제안된 모바일 에이전트 기법은 태그 위변조에 대한 가능성을 해결하지 못하고 이론적인 방식만 제안하였다. MARP 기법은 안전성과 효율성을 만족하고 태그 위변조 가능성을 막는 기법으로 보였지만 몇 가지 약점이 존재하였다. 하지만 본 논문에서 제안한 eMARP는 기존 MARP 기법의 약점을 보완하고 개선하였다. 기존 MARP의 문제점이었던 태그 등록 단계에서의 도청 가능성이 있었다. 제안하는 기법에서는 PIN값의 업데이트를 통하여 재사용 공격을 막았다. 그리고 에이전트와 태그의 비동기화 가능성도 고려하여 프로토콜을 작성하였다. 또한 기존 MARP에서는 brute-force 기법으로 태그를 판독하여서 프로토콜 진행 시간이 길었다. 하지만 eMARP 기법의 서버에서는 공개키 해독을 이용해서 태그를 판별하기 때문에 전체적인 프로토콜의 진행시간도 짧아지게 되었다. 그리고 기존 MARP에서는 태그 위변조 검사 단계를 항상 시행하였지만 제안하는 기법에서는 에이전트와 태그의 마스터-슬레이브 관계에 대한 정보를 서버측에 데이터베이스화하여 관계 변화가 발견되는 경우에만 시행하게 하였다. 따라서 보통의 경우에는 태그가 프로토콜에 참여하지 않아도 되도록 제안되었다. 그래서 에이전트를 사용하는 장점을 부각시켰다.

V. 결 론

저가형 RFID 태그는 몇 백 비트의 메모리와 몇 천 개의 논리 게이트만 가지고 있기 때문에 기존 유무선 통신에서 사용되던 프라이버시 보호 기법의 적용이 힘들다. 따라서 제한된 자원을 가지고 프라이버시 보호를 하려는 기법이 많이 제안되었다. 본 논문에서는 기존의 RFID 프라이버시 보호 기법들에 대해 알아보았으며, 그들의 단점에 대하여 언급하였다.

본 논문에서 제안한 개인 프라이버시 보호 에이전트는 태그의 비밀 정보의 일부분을 획득하여 인증된 리더 그룹과 높은 수준의 보안 모드로 통신한다. 따라서 태그의 기본적인 한계를 해결할 수 있는 특별한 방법이다. 태그에서 하기 힘들었던 공개키 암호화 같은 보안을 모바일 에이전트에서는 구현 가능하다. 따라서 현재 문제시 되고 있는 RFID 시

표 1. 기존 방식과 제안 프로토콜의 비교

	도청	통신내용분석	스푸핑	위치추적	태그 위변조	효율성
Kill 명령어[3]	취약	취약	취약	취약	취약	낮음
Blocker 태그[8]	취약	취약1	취약	취약	취약	보통
해쉬기반 인증[6]	보통	보통	취약	취약	취약	높음
에이전트 기법[10]	보통	안전	안전	안전	취약	보통
MARP[13]	보통	안전	안전	안전	안전	보통
eMARP	안전	안전	안전	안전	안전	높음

스템의 프라이버시 문제 해결에 큰 도움이 될 것이다. 또한 제안하는 기법에서는 다른 모바일 에이전트 기법과는 달리 모바일 에이전트 자체에 의한 위변조 가능성도 막을 수 있기 때문에 큰 장점이 있다. 뿐만 아니라. 제안하는 모바일 에이전트 기법은 현재 RFID 시스템의 일부만 수정하면 바로 적용될 수 있는 추가적인 구성 요소이며, RFID 태그 자체의 높은 계산 능력도 요구하지 않는다. 제안하는 모바일 에이전트 기법은 독립적인 모바일 장치 형태로도 구현될 수 있으며, 휴대폰 또는 PDA의 모듈 형태로도 구현될 수 있을 것으로 보인다.

참 고 문 헌

〔1〕 K. Finkenzeller, RFID Handbook, *John Wiley& Sons*, 2002.

〔2〕 조정식, 여상수, 김성권, “RFID tag를 위한 강력한 Yoking Proof Protocol”, 한국통신학회논문지, 32(3) , pp.310-318, March 2006.

〔3〕 S. Sarma and S. Weis and D. Engels, “Radio-Frequency identification: security Risks and Challenges”, In Cryptobytes, Vol.6, No.1, pp.2-9, RSA Laboratories, Spring 2003.

〔4〕 G. Avoine and P. Oechslin, “RFID Traceability: A Multilayer Problem”, In Proceeding of the Financial Cryptography ’05 - FC’05, Vol.3570 of LNCS, pp.125-140, February 2005.

〔5〕 R. Anderson and M. Kuhn, “Low cost attacks on tamper resistant devices”, Proceeding of the International Workshop on Security Protocols - IWSP, Vol.1361 of LNCS, pp.125-135, April 1997.

〔6〕 S. Weis, S. Sarma, R. Rivest, and D. Engels, “Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems”, *Springer-Verlag,* International Conference on Security in Pervasive Computing - SPC 2003, LNCS, Vol 2802, pp.454-469, 2004

〔7〕 P. Golle and M. Jakobsson and A. Juels and P. Syverson, “Universal Re-Encryption for Mixnets”, Proceedings of the The Cryptographers’ Track at the RSA Conference - CT-RSA ’04, Vol.2964 of LNCS, pp 163-178, February 2004.

〔8〕 A. Juels and Rivest and M. Szydlo, “The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy”, Proceeding of the Conference on Computer and Communications Security - ACM CCS 2003, ACM, pp.103-111, October 2003.

〔9〕 G. Avoine, “Adversarial Model for RFID Frequency Identification”, Cryptology ePrint Archive, Report 2005/049, 2005

〔10〕 M. Rieback and B. Crispo and A. Tanenbuam, “RFID Guardian; A battery-powered mobile device for RFID privacy management”, Proceedings of the Australasian Conference on informaiton Security and Privacy - ACISP 2005, Vol.3574 of LNCS, pp.184-194, July 2005.

〔11〕 S. Konomi, “Personal Privacy Assistants for RFID Users”, Proceedings of the International Workshop Series on RFID 2004, November 2004

〔12〕 A. Juels and P. Syverson and D. Bailey, “High-Power Proxies for Engancing RFID Privacy and Utility”, Proceedings of the Center for High Assurance Computer Systems - CHACS 2005, August 2005.

〔13〕 S.C. Kim and S.S. Yeo and S.K. Kim, “MARP: Mobile Agent for RFID Privacy Protection”, International Conference on Smart Card Research and Advanced Applications - CARDIS’06, pp.300-312, April 2006.

김 수 철 (Soo-Cheol Kim) 정회원

2004년 2월 중앙대학교 컴퓨터공학과 학사 졸업

2007년 2월 중앙대학교 컴퓨터공학과 석사 졸업

2007년 3월~현재 중앙대학교 컴퓨터공학과 박사과정

<관심분야> RFID 보안, Sensor network 보안, 암호 응용 및 정보보호

여 상 수 (Sang-Soo Yeo) 정회원

1997년 2월 중앙대학교 컴퓨터공학과 공학사
1999년 2월 중앙대학교 컴퓨터공학과 공학석사
2005년 8월 중앙대학교 컴퓨터공학과 공학박사
2006년 3월~2007년 2월 단국대학교 강의전임강사
2007년 3월~현재 큐슈대학교 정보공학부 방문연구원
<관심분야> RFID 보안, 암호 응용 및 정보보호, 컴퓨터 알고리즘

김 성 권 (Sung Kwon Kim) 정회원

1981년 2월 서울대학교 계산통계학과 학사 졸업
1983년 2월 한국과학기술원전산학과 석사 졸업
1990년 8월 Univ. of Washington 전산학 박사 졸업
1991년 3월~1996년 2월 경성대학교 전산통계학과 조교수.
1996년 3월~현재 중앙대학교 컴퓨터공학과 교수
<관심분야> 생물정보학, 계산기하학, 암호응용 및 정보보호