DOI: 10.3745/KIPSTC.2009.16-C.2.189

모바일 RFID 시스템의 Private Zone에 적용 가능한 프라이버시 보호 기법

김 동 철[†] · 천 지 영[††] · 최 은 영[†††] · 이 동 훈[††††]

요 약

모바일 RFID 시스템은 기존 RFID 시스템과 모바일 시스템이 결합한 차세대 핵심 기술로써 사용자에게 새로운 부가서비스를 제공하고 일상생활에서 넓게 이용될 것으로 기대되고 있다. 하지만 모바일 RFID 시스템은 기존 RFID 시스템이 가졌던 프라이버시 문제 및 보안 취약성을 그대로 갖고 있으며 추가적인 프라이버시 및 보안문제를 발생시킨다는 문제점을 갖고 있다. 더군다나 이러한 문제점을 해결하기 위해 여러 기법들이 제안 되었지만 아직 현실에 적용하기 어렵거나 완벽히 안전성을 보장하지 못 한다는 문제점을 갖고 있다. 따라서 본 논문에서 모바일 RFID 시스템 환경에 적용 가능하고 안전한 프라이버시 보호 기법을 제안한다. 제안한 기법은 모바일 RFID 시스템 환경 중 개인의 프라이버시 보호가 필요한 환경인 Private Zone에 적용 가능한 기법으로 개인의 휴대 모바일 리더를 이용하여 프라이버시 보호가 필요한 자신의 태깅된 물품에 대해 자신 이외에 다른 리더에게 어떠한 정보도 제공하지 않도록 하는 기법이다. 추가적으로 제안한 기법은 서비스 거부 공격이나 시스템 오류가 발생했을 때 동기화를 유지하기 위한 과정을 획기적으로 줄인 향상된 기법이기도 하다.

키워드 : 모바일 RFID, 프라이버시, 보안, 동기화

The Privacy Protection Mechanism Applicable to Private Zone of Mobile RFID Systems

Dong-Chul Kim[†] · Ji-Young Chun[††] · Eun-Young Choi[†††] · Dong-Hoon Lee[††††]

ABSTRACT

Mobile RFID system is a next generation technology which combines the existing RFID systems with mobile systems. It is newly expected to provide additional services and will be broadly used in everyday life; however, it sometimes causes the privacy or security problems generated by existing RFID systems and the additional privacy or security problems. Moreover, even if many methods have been proposed to solve those problems, it is still difficult to adapt to reality or to guarantee the security perfectly. Therefore, in this paper, we propose the secure and practicable privacy protection mechanism suitable to mobile RFID systems. proposing mechanism is applicable the mechanism to Private Zone of mobile RFID systems which require to protect the privacy. This mechanism suggests that own tagging-products needed to protect privacy using mobile reader of personal don't provide any information to other readers except their own reader. In addition to, proposing mechanism is the efficient mechanism which largely reduces the process to maintain the synchronization when happen to the DoS attack or system error.

Keywords : Mobile RFID, Privacy, Syncronization

1. 서 론

RFID(Radio Frequency IDentification) 기술은 작은 전자 태그를 사물에 부착하여 사물에 대한 정보나 주위 환경에 대한 다양한 정보를 제공해주는 무선 인식 기술로써 기존 바코드 기술을 대체 할 유비쿼터스 환경의 핵심 기술로 주목받고 있다. 하지만 지금까지 주로 물류·유통관리등 기업적 목적으로만 그 응용분야를 찾아야 했던 RFID 기술은 최근 들어 모바일 기기 및 무선 인터넷을 접목한 모바일 RFID 기술이 등장함으로써 기업뿐만 아니라 일반 사용자들에게까지 RFID 기술을 쉽게 이용할 수 있게 되었다. 하지만 모바일 RFID 기술은 보안관점에서 볼 때 물리적인 접촉 없이도 무선 인식이 가능하다는 기존 RFID 기술의 특징에서 발생하는 보안 문제와 모바일 단말기의 이동성 및 무선인터넷 등이 모바일 환경에서 발생하는 취약성으로 인해 안전성 및 프라이버시 측면에서 기존 문제뿐만 아니라 예상하지 못

※ 이 연구에 참여한 연구자(의 일부)는 '2단계BK21사업'의 지원비를 받았음.
† 준 회 원 : 고려대학교 정보경영공학전문대학원 정보경영공학과 석사과정
†† 준 회 원 : 고려대학교 정보경영공학전문대학원 정보경영공학과 박사과정
††† 정 회 원 : 한국정보보호진흥원 암호응용팀 연구원
†††† 정 회 원 : 고려대학교 정보경영공학전문대학원 정보경영공학과 교수
논문접수 : 2008년 9월 12일
수 정 일 : 1차 2008년 10월 27일
심사완료 : 2008년 10월 27일

한 추가적인 문제점들을 발생시켰다. 더군다나 이를 해결하기위한 연구를 통해 여러 기법들이 연구되고 제안 되었지만 지금까지 제안된 보안 기법들은 아직 현실에 적용하기 어렵거나 완벽하게 안전성을 보장하지는 못하고 있다.

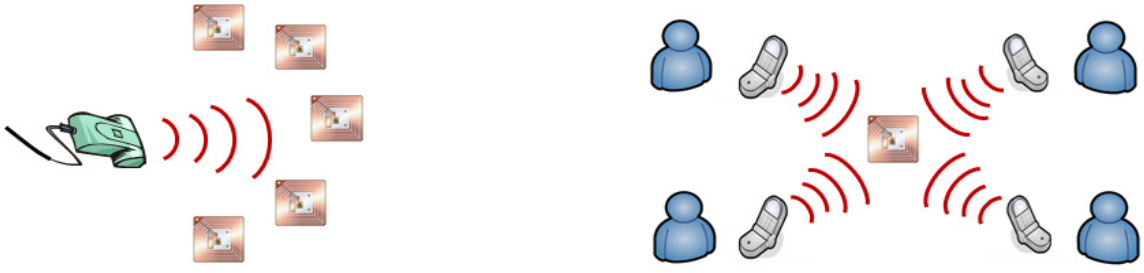
이에 따라 본 논문에서는 기존 기법들이 가진 문제점을 해결하면서 모바일 RFID 시스템 환경에서 적용 할 수 있는 안전하고 효율적인 프라이버시 보호 기법을 제안하고자 한다. 제안하는 기법은 Divyan M. et al[1] 등이 제안하고 정의한 모바일 RFID 시스템 환경 중 개인의 프라이버시 보호가 필요한 환경인 Private Zone에 적용 가능한 프라이버시 보호 기법으로 개인의 휴대 모바일 리더를 이용하여 자신의 태깅된 물품의 정보를 읽을 시 태그의 비밀 키를 모르는 제3자에게는 태그의 어떠한 정보도 제공하지 않도록 한 프라이버시 보호 기법이다. 일반적으로, RFID 시스템에서 태깅된 물품들은 객관적인 정보를 불특정 다수에게 제공해야 하는 환경과 특정한 사람에게만 정보를 제공해야 하는 환경으로 나눌 수 있다. 즉, 전자와 같이 프라이버시 보호가 필요하지 않는 환경과 필요한 환경으로 나눌 수 있다. 예를 들면, 일반 소비자가 RFID 시스템을 적용한 마트에서 물건을 구매하려고 할 때 구매 전에는 상품에 대한 정보를 모두에게 제공해야 하기 때문에 프라이버시 보호가 필요하지 않다. 하지만 물건을 구매 한 후 그 물건이 한 사람의 소유가 될 때부터는 이전과 같이 모든 모바일 리더에게 정보를 제공하는 것이 아니라 소유주에게만 그 물건에 대한 정보가 읽혀야 하므로 프라이버시 보호가 필요하다. 제안한 기법은 이러한 환경에 구매자의 프라이버시를 보호하기 위해 사용될 수 있다.

따라서 프라이버시 보호가 필요한 Private Zone과 같은 모바일 RFID 환경에서 제안한 기법은 다음과 같은 공헌을 한다. 첫째 기존에 제안된 모바일 기법에서의 취약성을 모두 해결하였다. 둘째 이전 기법에서는 일반적으로 백엔드 서버와 태그가 비밀 키를 공유하여 프라이버시를 보호하였다. 하지만 제안한 기법에서는 정당한 모바일 리더와 태그가 태그의 비밀 키를 공유하여 태그의 프라이버시를 완벽하게 보호할 수 있음을 보여준다. 셋째 RFID 리더와 태그가 공유한 비밀 키를 통해 통신 중 발생 가능한 서비스 거부 공격이나 시스템 오류로 인한 데이터 손실이 발생하였을 때 이를 회복하기 위한 통신 효율을 크게 향상 시켰다.

본 논문의 구성은 다음과 같다. 2장에서 모바일 RFID 시스템에 대해 간략히 알아보고 3장에서는 모바일 RFID 시스템이 가지는 보안 문제와 만족해야 할 보안 요구사항을 알아본다. 그리고 4장에서는 지금까지 모바일 RFID 시스템 환경에서 제안되었던 기존 프라이버시 보호 기법 연구에 대해서 알아보고 5장에서 보안 요구사항을 모두 만족하고 기존 관련 기법들이 가진 취약성을 해결한 프라이버시 보호 기법을 제안한다. 6장에서는 제안한 기법에 대한 안전성과 효율성을 분석하고 마지막으로 7장에서 결론을 맺는다.

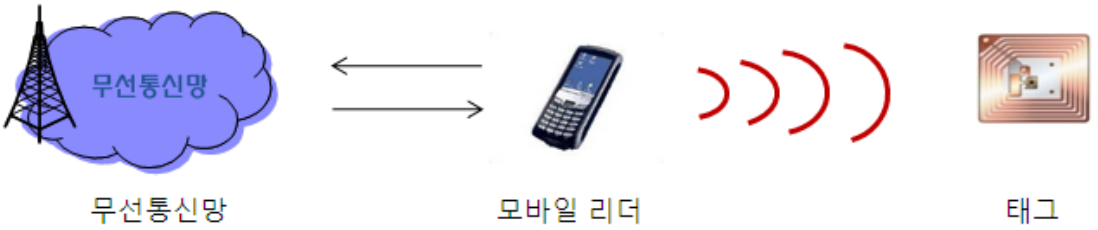
2. 모바일 RFID 시스템

모바일 RFID 시스템은 모바일 단말기의 사용 방식에 따라 두 가지 타입으로 분류된다. 첫째, 모바일 단말기에 RFID 리더를 장착함으로서 단말기 자체가 RFID 리더가 되는 시스템(그림 2)이고 둘째, 모바일 단말기가 태그와 RFID 리더 사이에 존재하여 중계역할을 하는 프록시(proxy)로 사용되는 시스템(그림 3)이다. 단말기가 RFID 리더인 시스템은 일반 RFID 시스템과 구성은 같으며 이동성이 있는 모바일 단말기에 리더를 부착한 것으로 리더의 이동성의 추가된 시스템이다. 따라서 이전의 시스템에서의 고정된 리더의 제약적인 기능을 모바일 RFID 시스템은 이동성을 추가함으로서 다양한 응용이 가능하게 되었다. 하지만 리더의 이동성이 추가됨으로서 리더의 보안을 고려해야 하는 문제도 발생하였다. 다음으로 단말기가 프록시로 사용되는 시스템은 일반적으로 RFID 시스템은 저가형 태그가 많이 사용되는데 저가형 태그는 연산 능력에 한계를 해결하기 위해서 사용되는 시스템으로 태그가 할 수 없는 연산 및 기능들을 대신함으로서 시스템의 효율을 극대화 시키고 보안 또한 강화할 수 있는 시스템이다. 본 논문에서 제안하는 기법은 자신의 소유한 휴대용 단말기를 이용하여 자신이 원할 때는 언제든지 자신의 휴대용 리더를 이용하여 물품의 정보



[기존 RFID 시스템] [모바일 RFID 시스템]

(그림 1) 일반 RFID 시스템 vs 모바일 RFID 시스템



(그림 2) 모바일 단말기가 리더인 시스템

(그림 3) 모바일 단말기가 프록시 역할을 하는 시스템

를 얻어오는 환경으로 리더의 이동성이 필요한 시스템에서 제안하였다. 다음은 모바일 RFID 시스템의 각 구성과 기능을 나타낸다.

- 태그(tag)
  제한된 연산과 데이터 저장을 위한 마이크로칩, 무선 통신을 위한 안테나 코일로 구성된 소형의 장치이다. 전력이 공급되는 방식에 따라 능동형 태그(positive tag)와 수동형 태그(passive tag)로 분류 하는 것이 일반적이다.

- 모바일 단말기(mobile Device)
  사용용도에 따라 모바일 단말기는 단말기 자체가 RFID 리더가 되어 태그에게 정보요청 신호를 보내고 태그로부터 정보를 받은 후, 무선인터넷망을 통해 정보를 얻어오는 경우와 RFID 리더와 태그 사이에서 전송되는 값들을 중계 및 관리하는 프록시(proxy)로 사용되는 경우로 나눌 수 있다.

- 리더(reader)
  태그가 전송하는 데이터를 수신하여 태그를 인식하거나 태그에 새로운 정보를 다시 쓰는 역할을 수행하는 장치이다. 리더가 태그에 무선 통신을 사용하여 정보를 요청하고 받은 정보를 백엔드 서버에 전송한다.

- 백엔드 서버 : 태그에 관련된 정보를 저장하고 관리 하는 역할을 하는 것으로 정당한 리더로부터 전송된 임의의 태그 정보를 통해서 개체를 식별하고 수집된 정보의 진위를 파악하는 기능을 수행한다. 백엔드 서버는 연산 능력이 낮은 리더나 태그를 대신하여 연산을 수행하기도 하며 보안 측면에서 신뢰할 수 있는 시스템으로 간주된다.

- 무선통신망 : 무선통신망은 크게 ODS(Object Directory Service)와 OIS(Object Information Service)서버로 구성되어 있다. ODS 서버는 인터넷 주소 정보를 제공하는 DNS(Domain Name System)과 유사한 형태로서 태그 ID에 대응되는 정보를 갖고 있는 서버의 URL(Uniform Resource Location)을 알려 주는 기능을 한다. OIS 서버는 객체의 식별 코드와 매치되는 데이터를 저장하고 있고 요청신호를 받으면 태그 ID에 매칭 되는 데이터를 출력하는 기능을 한다.

2.1 제안한 기법의 사용 어플리케이션

Divyan M. et al 등이 제안한 논문[5]에서는 모바일 RFID 어플리케이션 환경을 3가지(Location-Based Service Zone, Enterprise Zone, Private Zone)로 분류하였다. 첫째, LBS Zone은 공공장소, 길, 쇼핑몰, 극장, 음식점 등 사용자의 현재 위치를 기반으로 서비스를 제공하는 환경으로 모든 태그가 모바일 리더에 무조건 응답한다. 즉 위치기반의 인스턴트 정보를 무조건 제공한다. 따라서 이 환경에서는 특별히 프라이버시 및 보안 요구사항을 고려하지 않는다. 둘째 Enterprise Zone은 모바일 리더가 창고관리자, 현장 기술자, 수리공, 안전관 같은 기업의 직원이나 고용인을 보조하는 환경으로 실시간 창고관리, 출석관리, 태깅된 장비들이 어떻게 작동하는지에 대한 정보제공, 태깅된 물품에 대한 접근제어, 식별, 그리고 정기적인 모니터링 등을 제공한다. 이러한 Enterprise Zone의 범위는 특별한 조직에 국한되어 제한적이고 모니터링이 잘되기 때문에 효율적인 보안이 가능하다. 하지만 태깅된 물품에 대한 접근제어를 위해 모바일 리더와 태그사이의 인증, 모바일 리더의 정당성 식별등은 필요하다. 마지막으로 Private Zone은 모바일 리더가 집이나, 정원, 차안 등 극히 개인적인 공간에서 사용자를 보조

하는 환경으로 모바일 리더를 통해 개인 물품인 사진, 비즈니스 카드, 주소록 등에 대한 스캐닝을 가능하게 한다. 이러한 환경은 모바일 리더가 개인 물품에 대한 정보를 얻어오는 환경으로 인증되지 않은 모바일 리더에게는 정보를 제공하지 않아야 하는 환경이다. 따라서 이 환경은 개인의 프라이버시가 존재하는 환경으로 이를 보호할 수 있는 방법을 고려해야 한다. 제안한 기법은 사용자의 프라이버시를 보호하는 기법으로 위 3가지 모바일 RFID 어플리케이션 환경 중 프라이버시 보호가 필요한 Private Zone에서 사용 가능하다. 따라서 제안한 기법을 Private Zone에 적용하여 악의적인 의도를 갖고 개인의 프라이버시를 침해하고자 하는 대상으로부터 안전할 수 있을 것으로 기대된다.

3. 보안 문제 및 요구사항

일반적으로 RFID 시스템의 보안 문제는 크게 두 가지로 나눌 수 있다. 첫째 사용자의 프라이버시를 침해하는 개인 프라이버시 문제이고 둘째 태그 복제 및 재생공격 등에 취약한 시스템 보안 문제이다. 제안한 기법의 환경은 일반적인 RFID 시스템에 모바일 시스템이 추가된 모바일 RFID 시스템 환경으로 기존 시스템이 가진 문제점들과 추가적인 보안 문제 및 요구사항들을 발생시켰다. 우선 누구든지 모바일 리더를 휴대할 수 있기 때문에 악의적인 의도로 정보를 수집할 수 있다. 따라서 정당한 모바일 리더인지 인증을 통해 인증 받은 모바일 리더에게만 정보를 제공할 수 있도록 해야 한다. 그리고 모바일 리더는 태그처럼 소유자에 따라 이동하기 때문에 모바일 리더를 소유한 사람의 위치추적이 가능하다. 따라서 태그와 마찬가지로 모바일 리더의 위치추적을 할 수 없도록 하여야 한다. 다음은 이와같이 모바일 RFID 시스템 환경에서 추가적으로 발생하는 보안문제 및 요구사항을 고려하여 각 관점에서 보안 문제를 지적하고 요구사항을 살펴본다.

3.1 프라이버시 관점

- 정보노출(information leakage) : 모바일 RFID 시스템은 무선통신을 사용하기 때문에 공격자가 도청하는 것을 막는 것은 불가피하다. 그러므로 도청을 막는 것 보다 도청하는 것만으로는 사용자의 비밀 정보를 얻을 수 없도록 하거나 다른 공격에 활용 가능한 어떠한 정보도 얻을 수 없도록 하여야 한다. 즉, 정보의 기밀성을 보장하여야 한다.
- 위치추적(tracability) : 모바일 RFID 시스템의 사용자는 공격자 의해서 위치 추적이 될 수 있다. 우선, 만약에 태그가 모바일 리더의 질의에 대해 항상 같은 값으로 응답하게 된다면, 공격자는 사용자가 소유한 특정 태그를 추적함으로써 태그를 소지한 사용자의 위치 및 이동경로를 파악할 수 있다. 다음으로 만약에 모바일 리더가 태그에게 항상 고정된 값으로 질의 또는 응답을 하게 된다면, 공격자는 모바일 리더의 일정한 값의 질의나 응답을 추적하여 모바일 리더를 소지한 사용자의 위치추적을 할 수 있다. 따라서 태그와 모바일 리더는 위치 추적이 되지 않기 위해서 공격자가 예측할 수 없도록 항상 다른 값으로 응답하거나 질의를 하여야 한다.

3.2 시스템 보안 관점

- 태그 위조 및 복제 (tag forgery and cloning) : 공격자는 이전의 통신에서 도청한 정보를 정당한 모바일 리더에게 재전송하여 자신이 정당한 태그인 척 위장할 수 있다. 그리고 이전 값을 새로운 태그에 저장함으로써 복제된 태그를 생성해 낼 수 있다. 따라서 이를 막기 위해서는 모바일 리더와 태그사이에 정보를 계속적으로 업데이트 하거나 상호인증을 통해 위조 및 복제를 막아야 한다.
- 재생공격(replay attack) : 공격자는 리더와 태그 사이의 무선통신을 도청하여 정보를 저장한다. 이 후 공격자는 도청한 태그의 정보를 이용하여 리더가 태그에게 정보를 요청할 때 대신 응답한다. 이 때 공격자는 진짜 태그인 것처럼 모바일 리더를 속일 수 있다. 따라서 이 공격을 막기 위해서는 전송된 정보의 재사용을 못하도록 태그의 정보를 매번 업데이트하거나 인증을 통해 이전에 사용되었던 값을 구분하여 재생공격을 막도록 해야 한다.
- 스푸핑 공격(spoofing attack) : 공격자는 태그에게 리더인 척하여 태그의 정보를 얻는다. 이때 공격자는 태그로부터 정보를 받고 통신이 정상적으로 끝나기 전에 세션을 종료한다. 그리고 공격자는 태그로부터 얻어낸 정보를 이용하여 리더를 속일 수 있다. 따라서 이를 막기 위해서는 태그가 리더를 인증하는 과정이 필요하다. 즉, 태그와 리더 또는 백엔드 서버는 사전에 공유한 비밀 값을 가져야 하며, 이를 이용하여 태그는 리더를 인증한다.
- 비동기화 공격(desyncronization attack) : 공격자가 메시지 블로킹으로 정상적인 인증과정이나 키 업데이트 과정을 방해 했을 경우, 태그와 리더 또는 백엔드 서버는 비동기화 상태에 빠질 수 있다. 즉, 태그는 키를 업데이트 하지만 리더 또는 백엔드 서버는 키를 업데이트 하지 못하거나 리더 또는 백엔드 서버는 키를 업데이트 하지만 태그는 업데이트 하지 못하는 경우가 발생한다. 따라서 이후 RFID 시스템은 정상적으로 서비스를 할 수 없다. 따라서 이를 막기 위해서는 재동기화 과정이 필요하다.

4. 모바일 RFID 시스템 관련 연구

본 절에서는 기존에 모바일 RFID 시스템 환경에서 제안된 두 가지 유형의 보안 기법들에 대해서 살펴본다. 제안된 기법들을 살펴보면 아직까지 비현실적이거나 보안에 취약한

기법들이 대부분이다.

4.1 모바일 단말기가 프록시 역할을 수행하는 시스템

Rieback 등이 제안한 RFID 가디언(Gaurdian) 기법[1]에서 모바일 단말기는 사용자가 소유하고 있는 상품에 대해 외부 리더의 접근을 통제한다. 모바일 단말기가 프록시로써 제공하는 기능은 감시(auditing) 기능, 키 관리(key Management) 기능, 접근 제어(access Control) 기능으로 태그의 정보가 외부에 노출되는 것을 막았으며 태그를 대신하여 인증 과정을 수행 하도록 제안되었다. 하지만 가디언 기법은 과거에 소유했던 태그에 대한 정보를 저장함으로써 현재 태그를 소유하고 있지 않으면서도 소유하고 있는 것처럼 외부 리더를 속일 수 있으며 외부의 모든 신호를 감지할 수 있다는 강력한 가정을 기반으로 하기 때문에 실생활에 적용하기에는 약간의 어려움이 존재한다. Juels 등이 제안한 High-Power 프록시 REP 기법[2]은 가디언과 유사하지만 좀 더 향상된 기능을 제공하는 기법으로 자체적으로 태그의 정보를 갱신함으로써 제 삼자가 태그에 의미 없는 값을 써 넣는 공격에 대한 취약성을 해결하였다. 하지만 프록시 REP 기법 역시 앞의 가디언 기법과 마찬가지로 프록시가 외부의 모든 신호를 먼저 감지할 수 있다는 강력한 가정을 기반으로 하기 때문에 실생활에 적용하기에는 약간의 어려움이 있다. 이후 Kim.등은 좀 더 강력한 보안을 제공하는 MARP(Mobile Agent for RFID Privacy Protecting)기법[3]을 제안하였다. MARP 기법은 프록시의 역할을 수행하는 모바일 단말기가 특정 태그를 Sleep/Wake모드 상태로 만들고 그 태그들로부터 정보를 받아 대신 역할을 수행하는 기법으로 모바일 단말기와 리더 사이에 공개키 시스템을 기반으로 구축된 시스템이다. 하지만 이 기법은 공개키 시스템을 기반으로 하기 때문에 추가적으로 외부 시스템이 구축되어야 하고 외부 서버가 모든 키를 관리하므로 시스템은 외부 서버에 의존적이라는 문제점을 지니고 있다.

4.2 모바일 단말기가 RFID 리더인 시스템

제안된 기법[4]은 상품을 구매하는 환경에서 사용자의 프라이버시를 보호하는 기법으로 상품을 구매하기 전과 상품을 구매한 후의 두 과정으로 이루어져 있다. 상품을 구매하기 전의 과정은 매장 내에서 상품에 대한 신뢰성 있고 객관적인 정보를 얻어오는 과정으로 정보노출이나 위치추적과 같은 개인의 프라이버시 문제는 크게 고려되지 않는다. 상품 구매 후의 과정은 개인의 프라이버시를 고려해야 하는 경우로 상품을 구매한 후 안전한 채널을 통해 서버로부터 상품에 대한 비밀키(K)를 모바일 리더에 다운받아 개인의 프라이버시를 보호한다. 즉 비밀 키(K)를 모르는 제 삼자가 상품의 정보를 확인 할 수 없게 하여 구매 후에도 상품에 대한 신뢰성 있는 정보를 확인할 수 있으며 사용자의 프라이버시를 보호한다. 하지만 제안된 기법은 위치 추적이 가능하다는 문제점을 갖고 있다. 즉 상품 구매 후 공격자는 상품에 고정된 값과 요청 메세지를 보내면 태그는 반응하는 두메세지의 XOR를 통해 항상 고정된 값을 내놓게 되어 위치추적이 가능하다.

5. 제안한 기법

본 절에서는 앞 절의 사용자의 프라이버시 문제 및 시스템 보안 문제에 안전한 기법을 제안한다. 제안하는 기법은 태깅된 물품을 한 사람이 소유하게 되었을 때 사용자의 휴대 모바일 리더를 이용하여 프라이버시 보호가 필요한 태그에 대해 자신 이외에는 어떠한 정보도 제공하지 않는 기법으로 태그의 비밀 키를 모르는 제 3자에게는 태그의 어떠한 정보도 제공하지 않도록 한 프라이버시 보호 기법이다. 다시 말하면 정당한 모바일 리더가 프라이버시 보호가 필요한 태그를 소유하게 되었을 때 태그의 비밀 키를 다운 받아 공유함으로써 태그에 대한 접근 제어를 할 수 있게 된다.

5.1 용어 정의

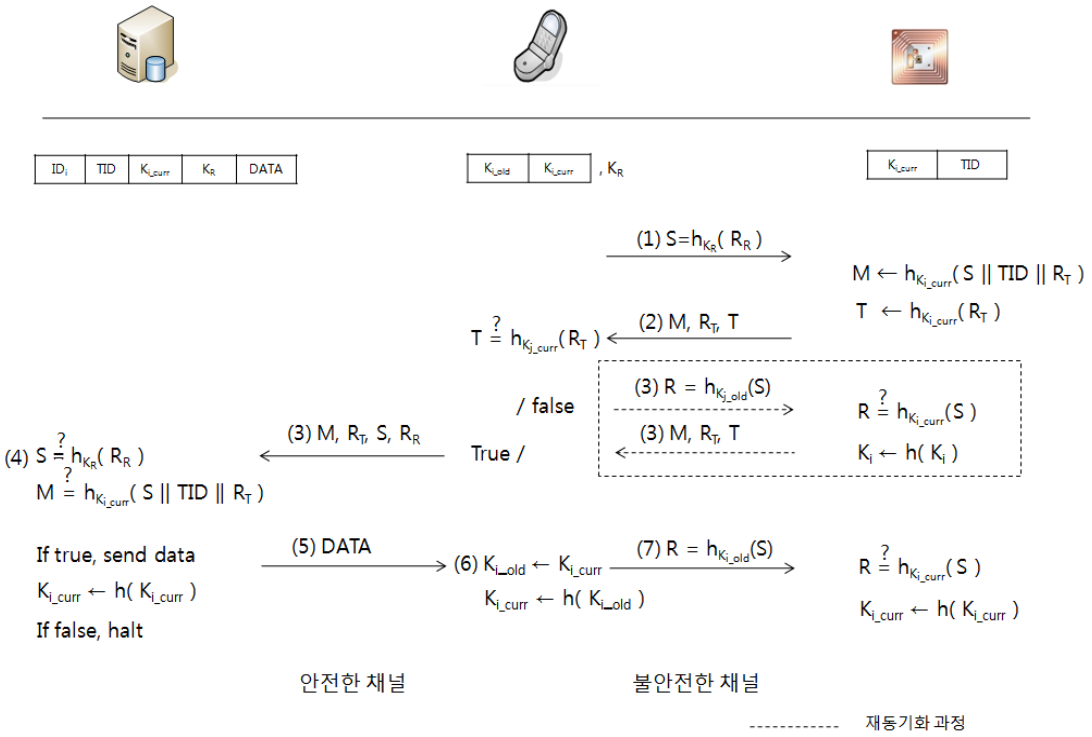
다음은 제안한 기법에서 사용하는 용어에 대한 설명이다.

〈표 1〉 용어 정의

용 어	내 용
ID	태그의 ID
Kcurr	백엔드 서버, 모바일 리더, 태그가 서로 공유한 비밀 키
Kold	이전 세션의 비밀 키
KR	모바일 리더와 백엔드 서버가 공유한 비밀 키
RR	모바일 리더에서 생성하는 랜덤 값
RT	태그에서 생성하는 랜덤 값
TID	태그가 가진 고유의 시리얼 넘버(제조 넘버)
hk()	일방향 키드 해쉬함수
||	연접

5.2 제안한 프라이버시 보호 기법

본 절에서는 모바일 리더를 이용하여 개인의 프라이버시를 보호하는 기법을 제안한다. 우선 백엔드 서버는 각 태그마다 [IDi, TIDi, Ki_curr, KR, DATA] 테이블을 구성하고 있으며(이 때 TID는 제조당시 생성된 넘버로써 읽기는 가능하지만 다시 쓰기가 불가능한 유일한 값이다.) 모바일 리더는 각 태그마다의 이전의 비밀 키(Ki_old), 현재의 비밀 키(Ki_curr) 쌍을 [Ki_old, Ki_curr]의 테이블로 구성하고 있고 모바일 리더와 백엔드 서버가 공유하는 리더의 비밀 키 KR를 초기 설정으로 갖고 있다. 다음은 정당한 모바일 리더 소유자가 태깅된 상품에 대한 정보를 안전하게 읽어 오는 과정이다.



(그림 4) 제안한 프라이버시 보호 기법

(1) 모바일 리더는 위치추적에 안전하기 위해 난수생성기(PRNG)를 이용하여 난수 RR을 생성하고 모바일 리더의 비밀 키(KR)을 이용하여 RR값을 해쉬한 S(=hKR(RR)) 값을 태그에게 요청 메세지와 함께 전송한다.

(2) 이 때 태그는 태그 정보의 기밀성을 제공하기 위해 모바일 리더에게 받은 S값과 각 태그마다 유일하게 갖고 있는 고유의 값 TID 그리고 태그 난수 RT를 연접한 후 태그의 비밀 키 Ki_curr를 이용하여 해쉬한 M(=hKi_curr(S||TID||RT)) 값을 생성한다. 그리고 태그 난수 RT를 비밀 키 Ki_curr로 해쉬한 T(=hKi_curr(RT))값(비동기화 공격이나 시스템 오류로 인한 데이터의 손실을 탐지를 위해)을 생성한다. 이후 태그는 M, RT, T값을 모바일 리더에게 전송한다.

(3) 태그로부터 데이터를 받은 모바일 리더는 태그와의 동기화를 유지하고 있는지 확인하기 위해 받은 T값을 모바일 리더가 가진 태그의 비밀 키(Kj_curr)들로 각각 RT값을 해쉬한 값과 비교한다. 만약 일치하는 값이 없다면, 전송과정에서 비동기화가 발생했음을 탐지하고 재동기화를 위해 동기화 요청 메세지와 R=hKi_old(S) 값을 태그에 재전송한다. 이때 태그는 R값과 태그의 비밀 키 Ki_curr로 S를 해쉬한 값을 비교한다. 일치한다면 재동기화를 위해 현재의 비밀 키를 해쉬하여 비밀 키를 업데이트 한 후 업데이트된 비밀 키로 M, T, RT값을 다시 생성하여 다시 모바일 리더에 재전송 한다. 반면 모바일 리더는 T값을 비교분석한 후 태그와 동기화를 유지하였다고 판단한다면, 태그로부터 받은 M, RT, S값에 모바일 리더가 생성했던 난수 RR값을 백엔드 서버에게 전송한다.

(4) 백엔드 서버는 우선 S의 값이 정당한 모바일 리더의 비밀 키 KR 이용하여 생성된 것인지를 판단하기 위해 모바일 리더로부터 받은 S의 값을 백엔드 서버가 보유한 모바일 리더의 비밀 키로 RR값을 해쉬하여 비교한다. 만약에 일치한다면 정당하다고 판단하고 모바일 리더를 인증한다. 그리고 백엔드 서버는 태그가 복제되었는지 아닌지를 판단하기 위해 모바일 리더로부터 받은 M값과 자신의 데이터 테이블에서 비밀 키 Ki_curr에 대응하는 TID값을 대입하여 생성한 hKi_curr(S||TID||RT)값을 비교한다. 만약에 일치한다면 복제되지 않은 정당한 태그로 인식하고 태그를 인증한다.

(5) 모바일 리더와 태그의 인증이 정상적으로 끝나면 백엔드 서버는 재생공격을 막고 전방향 안전성을 만족하기 위해 비밀 키를 업데이트 한다. 새로운 비밀 키는 현재의 비밀 키를 해쉬한 값이다. 비밀 키 업데이트 후 백엔드 서버는 태그의 정보 데이터를 모바일 리더에게 전송한다.

(6) 안전한 채널을 통해 태그의 정보를 얻은 모바일 리더는 동기화를 위해 백엔드 서버와 마찬가지로 현재의 비밀 키를 해쉬함수를 이용하여 업데이트 한다. 업데이트 된 비밀 키는 Ki_curr 테이블에 저장되고 이전의 비밀 키는 Ki_old 테이블에 저장된다.

(7) 이 후 모바일 리더는 태그의 키 업데이트를 위해 인증용 값 R=hKi_old(S)을 태그에게 전송한다. 태그는 R값

의 비교를 통해 정당한 리더로부터 전송된 값인지 인증한 후 현재의 비밀 키를 해쉬하여 업데이트 한다.

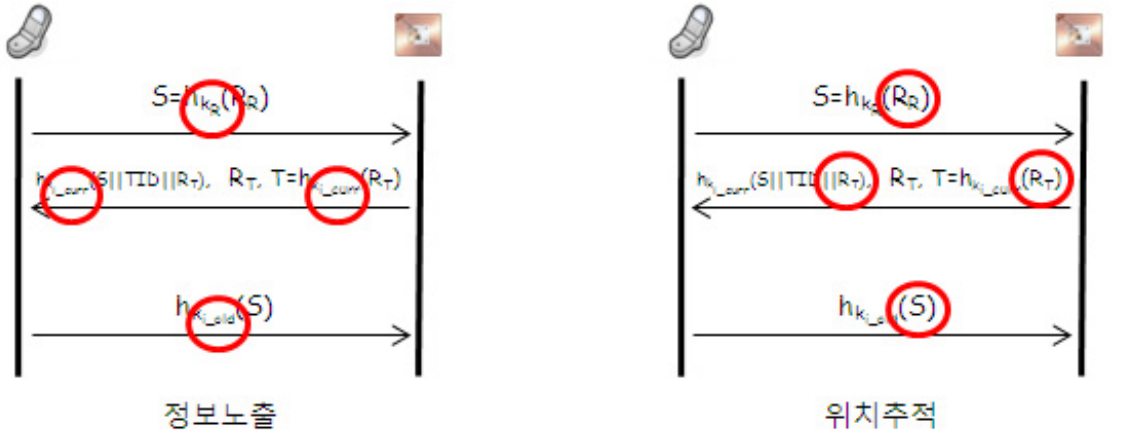
6. 안전성 및 효율성 분석

본 절에서는 제안한 프라이버시 보호 기법의 안전성과 효율성을 분석한다. 제안한 기법은 현재 알려진 모든 공격에 안전하며 비동기화 공격이나 통신 중 데이터 손실이 발생했을 때마다 재동기화를 위한 효율을 이전 기법들 보다 통신량을 20%, 연산량을 50% 줄인 효율적인 기법이다.

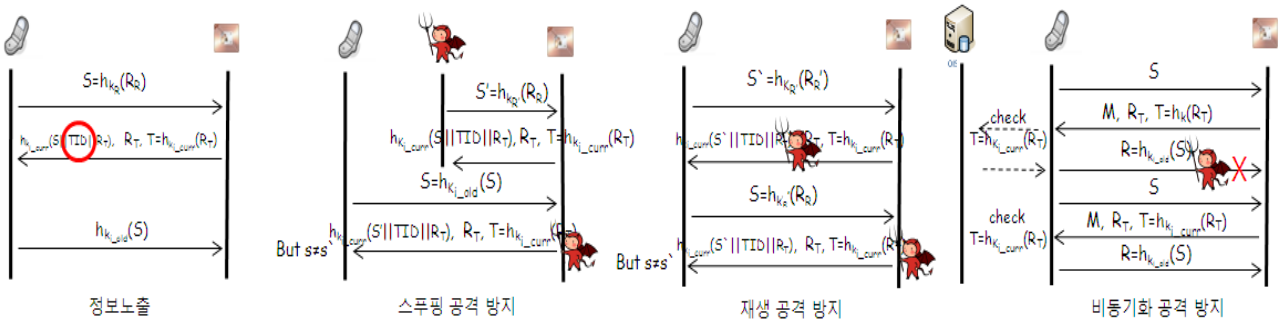
6.1 안전성 분석

프라이버시 보호 관점에서 볼 때 제안한 기법은 태그 및 모바일 리더 정보의 노출과 위치추적에 안전하다. 즉 아래 (그림 5)와 같이 무선공간에 전송되는 태그와 모바일 리더의 데이터의 값은 모바일 리더의 비밀 키 KR로 키드 해쉬하여 전송한다. 그러면 해쉬함수의 일 방향성에 의해 공격자는 전송되는 값에서 해쉬되기 이전의 값을 알아낼 수 없어 의미 있는 정보를 하나도 얻을 수 없다. 태그나 모바일 리더의 위치추적은 태그와 모바일 리더가 매 세션마다 난수생성기(PRNG)를 이용하여 난수를 발생하여 계산된 값을 내놓기 때문에 항상 다른 값을 내놓는다. 따라서 공격자는 모든 세션에 어떠한 값이 나올지 예상할 수 없어 태그나 모바일 리더의 위치를 추적하는 것은 현실적으로 불가능하다.

다음으로 시스템 보안 관점에서 볼 때 (그림 6)과 같이 태그복제, 스푸핑, 재생, 비동기화 공격 등에 안전하다. 우선



(그림 5) 프라이버시 보호 관점에서의 안전성 분석

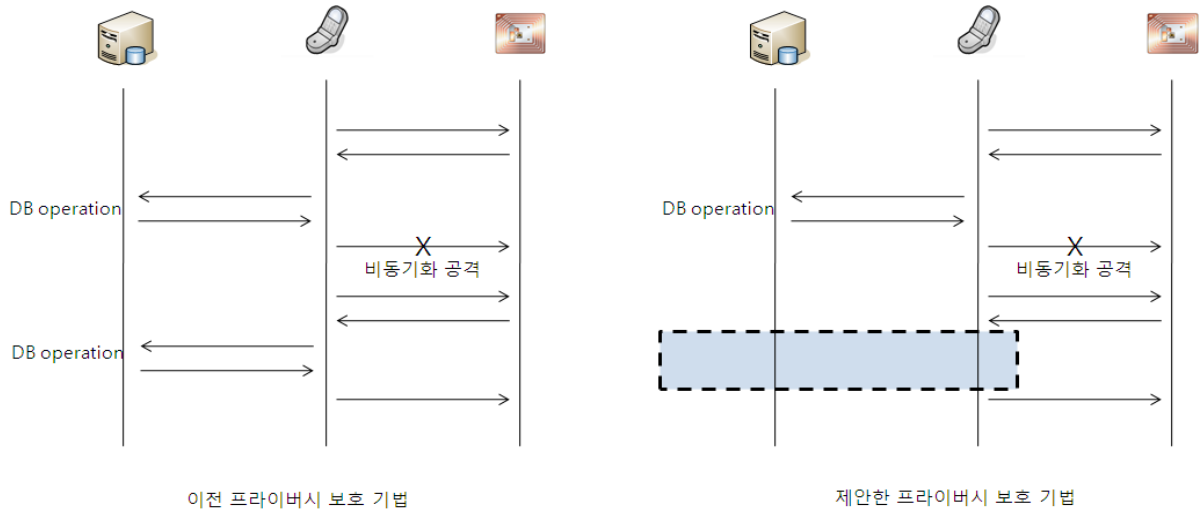


(그림 6) 시스템 보안관점에서의 안전성 분석

〈표 2〉 효율성 분석

구 분	Kim [4]	Hung [6]	제안한 기법
비동기화 공격시 동기화 유지를 위한 통신량 (개체간 통신 1회로 간주)	10 × N	10 × N	8 × N
비동기화 공격시 동기화 유지를 위한 DB 연산량 (연산 및 전수조사)	2 × N	2 × N	1

N : 비동기화 공격 발생 횟수



(그림 7) 비동기화 공격 시 재동기화 과정에 대한 비교

태그 복제 방지는 태그 제조 당시에 부여하는 유일한 값 TID를 이용한다. 이 TID 값은 모든 태그가 유니크하게 저장하고 있으며, 외부의 신호에 읽기는 가능하지만 쓰기가 금지된 영역에 저장되어 있다. 따라서 공격자는 새로운 태그를 이용하여 복제를 시도하지만 TID 값이 불일치하기 때문에 복제에 실패한다. 제안한 기법에서 살펴보면 태그는 TID를 포함하여 계산한 M(=hKi_curr(S||TID||RT))값을 내놓고 백엔드 서버는 모바일 리더를 통해 값을 전송 받아 사전에 공유하고 있던 TID 값과 비교하여 복제 여부를 확인할 수 있다. 둘째, 스푸핑 공격은 공격자가 비밀 키를 모르기 때문에 정당한 S를 만들 수 없어서 가능하다. 즉 공격자가 S′(hKR′(RR))을 생성하여 태그에게 전송한다고 하자. 그러면 태그는 M(=hKi_curr(S′||TID||RT)을 생성하여 전송한다. 이때 공격자는 태그의 출력 값을 저장하고 있다가 정당한 모바일 리더의 요청이 있을 때 대신 저장한 값을 보낸다. 이때 모바일 리더는 백엔드 서버에 M값을 전송하고 백엔드 서버는 S≠S′ 파악하여 공격을 막을 수 있다. 셋째, 재생공격을 막을 수 있다. 공격자는 정당한 모바일 리더가 S′을 태그에 전송할 때 태그의 출력 값을 도청하여 저장한다. 다음 세션에서 정당한 모바일 리더가 S를 태그 전송할 때 공격자는 이전 세션에 도청하여 저장한 값을 대신 전송한다. 이때 모바일 리더는 백엔드 서버에 그 값을 전송하지만 스푸핑 공격에서와 마찬가지로 S′≠S을 통해 공격을 탐지하고 공격을 막을 수 있다. 넷째, 비동기화 공격에 안전하다. 아래 그림의 4번째 프로토콜을 보면 알 수 있듯이 공격자는 한 세션의 마지막 통신을 방해함으로써 태그가 키를 업데이트 하지 못하게 한다. 이 때 모바일 리더와 태그 사이에 비동기화가 발생한다. 하지만 다음세션에서 모바일 리더는 태그의 전송 값 T값을 현재의 모바일 리더 비밀 키 값을 이용하여 체크함으로서 비동기화 공격이 발생했음을 탐지한다. 이후 모바일 리더는 이전세션에서 전송한 S값을 재전송하고 태그는 정상적으로 비밀 키를 업데이트 한다. 따라서 모바일 리더와 태그는 재동기화 과정을 통해 동기화를 유지한다.

이외에도 제안한 기법은 백엔드 서버에서 모바일 리더에서 전송된 S값을 체크하여 모바일 리더의 정당성을 인증하고 태그에서는 한 세션의 마지막 통신에서 전송되는 R의 값을 비교함으로서 모바일 리더의 정당성을 인증한다.

6.2 효율성 분석

제안한 기법은 앞에서 지적한 여러 공격에 안전하면서 이전 기법들과 비교할 때 비동기화 공격이나 통신 중에 시스템 오류로 인한 데이터 손실이 발생하였을 때 재동기화를 위한 과정의 효율성을 향상 시킨 기법이다. 제안한 기법은 이전 기법들에서 벡엔드 서버와 태그가 태그의 비밀 키를 공유하는 것과 달리 모바일 리더가 태그의 비밀 키를 공유하고 있다. 따라서 백엔드 서버가 아닌 모바일 리더에서 태그와의 동기화 유지 여부를 파악할 수 있다.

다시 말하면 태그는 모바일 리더에 데이터를 보낼 때 태그의 비밀 키로 태그 난수 RT를 해쉬한 T값을 전송한다. 이 때 모바일 리더는 이 값을 체크함으로서 태그의 비밀 키와 모바일 리더가 공유한 비밀 키가 동기화 되었는지 파악한다. 따라서 제안한 기법은 이전 기법들에서 동기화 여부를 백엔드 서버에서 파악하는 것과 달리 모바일 리더에서 체크함으로써 모바일 리더와 백엔드 서버와의 불필요한 통신량을 줄인다. 게다가 이전 기법들에서 재동기화 과정 중 백엔드 서버에서 행하는 전수조사나 해쉬함수를 제안한 기법은 하지 않기 때문에 백엔드 서버의 비효율을 없앴다. 다음 (그림 7)은 제안한 기법이 이전 기법들과 비교할 때 효율성이 크게 향상됨을 볼 수 있다. 즉 이전 기법과 비교할 때 통신량을 20% 줄였고, 백엔드 서버에서의 연산량을 50% 줄이는 효과를 볼 수 있다. 또한 [표2]에서 보면 최근에 모바일 환경에서 제안된 이전 기법들의 효율성을 비교 분석해 보면 비동기화 공격이 발생하였을 때 Kim 의 기법과 Hung

의 기법은 10×N (N : 비동기화횟수)의 통신이 필요한 반면 제안한 기법은 8×N의 통신만 필요한 것을 볼 수 있다. 비동기화 공격 등의 횟수가 많아지고 누적되면 통신횟수의 차이는 더욱 커지게 것이다. 그리고 백엔드 서버의 연산량을 보면 이전 기법들은 비동기화 공격이 발생할 때마다 2×N의 연산량인 반면에 제안한 기법은 동기화가 유지될 때까지 딱 한번의 연산만 한다. 여기서 엄청난 효율을 얻을 수 있다. 대부분의 RFID 보안 기법들은 전방향 안전성을 보장하거나 재생공격에 안전하기 위해 매 통신마다 키를 업데이트 하는 과정을 제안한다. 하지만 이에 따라 비동기화 공격이 발생하여 재동기화를 위한 과정을 수행하게 된다. 하지만 이러한 공격이 무수히 많이 반복된다면 백엔드 서버는 정상적으로 시스템을 운용할 때 보다 2배의 자원과 시간을 소비해야 한다. 이것은 아주 비효율적이다. 따라서 제안한 기법은 최근 비동기화 공격에 안전한 기법을 제안하는 연구에 효율성을 향상시킬 수 있는 아이디어로 제공되기를 기대한다.

7. 결 론

최근 국내에서는 모바일 단말기 및 무선 인터넷과 접목한 모바일 RFID 서비스가 등장하여 사용자에게 새로운 부가서비스를 제공하고 있다. 하지만 모바일 RFID 시스템도 기존 시스템이 가진 개인 프라이버시 및 보안 문제를 그대로 갖고 있어 이에 대한 연구가 필요하다. 따라서 본 논문에서는 모바일 RFID 환경에 적합한 프라이버시 보호 기법을 제안하였다. 제안하는 기법은 개인의 프라이버시 보호가 필요한 태그에 대한 접근 권한을 오직 비밀 키를 아는 모바일 리더에게만 부여함으로서 프라이버시를 보호하는 기법으로 개인의 프라이버시를 보호해야 하는 모바일 RFID 시스템 환경에 다양하게 쓰일 것으로 기대된다. 그리고 제안한 기법은 시스템의 효율 측면에서 비동기화 공격이나 시스템 오류로 인한 비동기화가 발생했을 때, 이를 해결하기 위한 과정을 단순화함으로서 불필요한 자원의 낭비를 줄일 수 있는 기법으로 RFID 시스템의 효율성을 증가시킬 수 있을 것으로 기대된다.

참 고 문 헌

[1] M. Rieback, B. Crispo, A. Tanenbaum, “RFID Guardian: A Battery-powered Mobile Device for RFID Privacy Management”, Australasian Conference on Information Security and Privacy of LNCS, 3574, pp.184-194, 2005

[2] A. Juels, P. Syverson, and D. Bailey “High-Power Proxies for Enhancing RFID Privacy and Utility”, Center for High Assurance Computer Systems of LNCS, 3856, pp.210-226, 2005

[3] Soo-Cheol Kim, Sang-Soo Yeo, and Sung Kwon Kim, “MARP:Mobile Agent for RFID Privacy Protection”, Smart Card Research and Advanced Application IFIP Conference of LNCS, 3928, pp.300-312, 2006

[4] Il-jung Kim, Eun-young Choi, Dong-hoon Lee, “Secure Mobile RFID system against privacy and security problems”, International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing, 2863, pp.67-72, 2007

[5] Divyan M. Konidala and Kwangjo Kim, “Mobile RFID Applications and Security Challenges”, International Conference on Information Security and Cryptology of LNCS, 4296, pp.194-205, 2006

[6] Hung-Min Sun, Chen-En Lu, Shuai-Min Chen, “An Authentication Protocol in Mobile RFID Environment”, TENCON 2007 of IEEE, pp.1-4, 2007

김 동 철

e-mail : ifineedu0707@korea.ac.kr

2006년 8월 고려대학교 수학과(학사)

2007년 3월~현 재 고려대학교 정보경영공학전문대학원 석사과정

관심분야 : 정보보호, RFID 정보보호 기술, 유비쿼터스 보안

천 지 영

e-mail : jychun@korea.ac.kr

1997년 2월 이화여자대학교 수학과(학사)

2006년 2월 단국대학교 수학과(석사)

2006년 3월~현 재 고려대학교 정보보호대학원 박사과정

관심분야 : 암호 이론, PET 기술, 유비쿼터스 보안

최 은 영

e-mail : bluecey@kisa.or.kr

2001년 8월 고려대학교 수학과(학사)

2003년 8월 고려대학교 정보보호대학원(공학석사)

2006년 2월 고려대학교 정보보호대학원 박사수료

2007년 3월~현 재 한국정보보호진흥원 암호응용팀 연구원

관심분야 : 암호 이론, 정보보호 이론, RFID 정보보호

이 동 훈

e-mail : donghlee@korea.ac.kr

1983년 8월 고려대학교 (경제학사)

1987년 12월 Oklahoma University 전산학(석사)

1992년 5월 Oklahoma University 전산학(박사)

1993년 3월~1997년 2월 고려대학교 전산학과 조교수

1997년 3월~2001년 2월 고려대학교 전산학과 부교수

2001년 2월~현 재 고려대학교 정보보호대학원 교수

관심분야 : 암호프로토콜, 암호이론, USN 이론, 키 교환, 익명성 연구, PET 기술