랜덤 키 분할을 이용한 모바일 RFID 사용자의 프라이버시를 보호하는 상호 인증 프로토콜

정회원 정 윤 수*, 김 용 태**, 박 길 철**°, 종신회원 이 상 호***

Mutual Authentication Protocol for Preserving Privacy of Mobile RFID User using Random Key Division

Yoon-Su Jeong*, Yong-Tae Kim**, Gil-Cheol Park**° *Regular Members*,
Sang-Ho Lee*** *Lifelong Member*

요 약

이동 통신망에 RFID 기술을 접목한 모바일 RFID는 사용자 자신이 휴대한 휴대전화로 제품에 부착된 RFID 태그의 식별자를 읽고, 이 식별자를 이동통신망을 통해 네트워크로 전달하여 제품에 대한 정보를 얻는 기술이다. 그러나 모바일 RFID는 기존 RFID에서 요구되어지는 보안 요구사항 중 프라이버시 문제가 여전히 존재하는 문제점이 있다. 이 논문에서는 모바일 RFID 사용자가 태그 정보를 백 엔드 서버로부터 안전하게 전달받기 위해서 초기화 과정과 상호 인증과정에서 모바일 RFID 리더와 태그가 생성한 랜덤키를 임의의 크기로 분할하여 프라이버시 보호가 필요한 태그에 대해서 모바일 RFID 리더가 매 세션마다 난수생성기에 의해 항상 다른 하부키 값을 생성함으로써 태그의 어떤 정보도 제 3자에게 제공하지 않도록 하고 있다. 성능 평가 결과 제안 프로토콜은 등록 계산량과 로그인 계산량에서 모듈러 연산을 사용하는 기존 프로토콜과 달리 일방향 해쉬 함수를 사용하여 사용자의 정보를 등록하기 때문에 MARP 기법[7]과 Kim 등의 기법[12]보다 저장 공간과 계산량에서 효율성이 높았다.

Key Words : 모바일 RFID(Mobile RFID), 상호 인증(Mutual Authentication), 프라이버시(Privacy), 랜덤 키 분할(Random Key Division)

ABSTRACT

Mobile RFID which integrates mobile network with RFID technique is the technique to get the information of products by transmitting the identifier through mobile network after reading the identifier of RFID tag. It attached on the equipment as the mobile phone. However, mobile RFID has the privacy-related problem among requested secure problems required from the existing RFID. In this paper, the random key created by mobile RFID reader and Tag during the inter-certificating and initialization procedure for mobile RFID users to receive tag information from backend server securely is divided into random sizes and any information on the tag which requires the protection of privacy shouldn't be provided to anyone. In performance analysis, previous protocol used modulo operation in registration and login computation. But the proposed protocol has higher efficiency in saving space and computation volume than MARP scheme[7] and Kim. et. al[12] scheme because our protocol is accomplished by mutual authentication and registering user information through one-way hash function.

※ 이 논문은 2011년도 한남대학교 학술연구 조성비 지원에 의하여 연구되었음.
* 충북대학교 전자계산학과 네트워크보안 연구실(bukmunro@gmail.com),
** 한남대학교 멀티미디어공학부 교수(ky7762@hannam.ac.kr, gcpark@hnu.kr) (° : 교신저자)
*** 충북대학교 전기전자컴퓨터공학부 교수(shlee@chungbuk.ac.kr)
논문번호 : KICS2010-08-403, 접수일자 : 2010년 8월 18일, 최종논문접수일자 : 2010년 12월 8일

Ⅰ. 서 론

최근 IT 기술의 빠른 발전으로 인해 휴대 단말은 다양한 정보 서비스와 유비쿼터스 환경을 지원하기 위해 저전력·초경량화된 복합·지능형 단말기로 진화되고 있다. 특히, 모바일 단말기는 디지털 방송, MP3 음악 감상은 물론 증권, 텔레매틱스, 게임 등 다양한 디지털 콘텐츠 서비스가 가능하다[1]. 모바일 RFID 서비스는 기존 RFID 태그 식별자 인식과는 다른 서비스 환경을 가진다. 모바일 RFID 기술은 이동통신망에 RFID 기술을 접목한 것으로 사용자가 자신이 휴대한 휴대전화로 제품에 부착된 RFID 태그의 식별자를 읽고 이 식별자를 이동통신망을 통해 네트워크로 전달하여 제품에 대한 정보를 얻거나 활용하는데 사용하고 있다[2-4]. 특히, 모바일 RFID는 기술 발전에 따라 모바일 단말기에 근거리 무선통신(NFC, Near Field Communication) 기능을 탑재하여 개인뱅킹, 신용카드, 정보 공유 등의 기능을 수행하는 모바일 RFID 시장으로 더욱 확대되고 있다.

모바일 RFID 서비스 환경에서 기능적으로 가장 중요한 것은 개인 사용자가 RFID 태그가 부착된 제품의 정보를 정확하고 신뢰성 있게 얻는 것이며, 보안 측면에서 가장 중요한 것은 제품의 안전한 제공 및 개인 프라이버시 보호이다. 각 개인마다 태그가 부착된 아이템을 다양한 이유로 소유하고 태그가 부착된 아이템이 일반적으로 인식이 될 때 프라이버시 침해와 개인 정보의 유출이 발생하기 쉽다[1,5].

모바일 RFID 시스템의 문제점을 보완하기 위해 많은 기법들이 현재까지 연구되고 있다[6-8]. Rieback의 RFID 가디언(Guardian)기법[8]은 사용자가 소유하고 있는 상품에 대해 외부 리더의 접근을 통제하도록 모바일 단말기가 프록시와 같은 기능을 수행하는 기법을 제안하였다. Rieback의 RFID 가디언(Guardian)기법은 태그의 정보가 외부에 노출되는 것을 막았지만 과거에 소유했던 태그에 대한 정보를 저장함으로써 현재 태그를 소유하고 있지 않으면서도 소유하고 있는 것처럼 외부 리더를 속일 수 있는 단점이 있어 실생활에 적용하기에는 어렵다. Juels et. al 의 High-Power 프록시 기법[6]은 Rieback et.al[8]과 유사하지만 자체적으로 태그의 정보를 갱신하여 제 3자가 태그에 의미 없는 값을 삽입하는 것을 예방하고 있다. 그러나 Rieback et.al[8]과 마찬가지로 프록시가 외부의 모든 신호를 먼저 감지해야 한다는 강력한 가정을 기반으로 하기 때문에 실생활에 적용하기 어려운 단점이 있다. MARP 기법[7]은 프록시의 역할을 수행하는 모바일 단말기가 특정 태그를 Sleep/Wake 모드 상태로 만들고 그 태그들로부터 정보를 받아 대신 역할을 수행하는 기법이다. 그러나 이 기법은 공개키 시스템을 기반으로 하기 때문에 추가적으로 외부 시스템이 구축되어야 하고 외부 서버가 모든 키를 관리하므로 시스템은 외부서버에 의존적이라는 문제점을 가지는 단점이 있다.

이 논문에서는 모바일 RFID 리더가 태그의 정보를 백엔드 서버로부터 안전하게 8비트 형태의 스트림 방식으로 메시지를 안전하게 전달받기 위해서 초기화 과정과 상호 인증과정을 통해 RFID 사용자의 프라이버시를 보호하는 프로토콜을 제안한다. 제안된 프로토콜은 모바일 RFID 리더와 태그에서 생성한 랜덤 키를 임의의 크기로 분할하여 모바일 RFID 리더와 태그간 상호 인증을 통해 백엔드 서버의 정보에 저장된 모바일 RFID 리더와 태그의 정보를 난수생성기에 의해서 매번 하부키를 접속마다 갱신함으로써 모바일 RFID 시스템에서 많이 발생하는 정보 노출, 추적 가능, 재사용 공격, 스푸핑 공격 등과 같은 보안 공격을 예방한다.

제안 프로토콜을 기존 기법들과 비교하면 제안 프로토콜의 주된 기여는 크게 2가지이다. 첫째, 제안 프로토콜은 RFID 시스템을 사용하여 모바일 RFID 환경에 사용하기 위한 안전하고 확장 가능한 RFID 사용자 프라이버시 보호 프로토콜을 제안하고 있다. 특히, 제안 프로토콜은 AES 메커니즘을 사용하기에 적합하며 AES을 사용하여 디바이스 간 안전한 통신을 수행하기 위해 통신 주체 사이에 키 쌍-AES의 경우에 공유된 비밀 키-을 유지하고 분배함으로써 오버헤드를 줄이고 있다. 둘째, 제안 프로토콜은 모바일 RFID 환경에서 발생가능한 여러 종류의 공격에서 잘 동작되는 것을 증명하기 위해서 여러 공격 시나리오에 기반하여 제안 프로토콜을 분석하였다.

이 논문의 구성은 다음과 같다. 2장에서는 모바일 RFID 시스템과 모바일 RFID 시스템의 보안 요구사항을 알아본다. 3장에서는 보안 요구사항을 만족하는 사용자 프라이버시 보호 기법을 제안한다. 4장에서는 제안 기법과 기존 기법의 안전성과 효율성을 분석하고 마지막으로 5장에서 결론을 맺는다.

Ⅱ. Background

2.1 모바일 RFID 기술

모바일 RFID 서비스는 휴대전화를 이용하여 사물과 사람 사이의 직접적 정보 소통 관계를 제공하기 위

하여 시작된 융합 서비스이다[2,3]. 그림 1은 모바일 RFID 시스템 개념도이다. 그림 1의 모바일 RFID 서비스 네트워크에 존재하는 ODS(Object Directory Servcice) 서버는 RFID 태그 식별자와 관련된 제품정보가 있는 OIS(Object Information Service) 서버의 위치를 알려주는 역할을 하며, OTS 서버는 개인 사용자에게 제품의 유통 정보 또는 OIS 서버의 이력을 제공하는 역할을 하며, OIS 서버는 RFID 태그 식별자와 관련된 제품의 주요 정보를 저장하고 관리하는 역할을 한다. 휴대전화를 소유한 개인 사용자가 휴대전화에 장착된 RFID 리더로 제품에 부착된 RFID 태그로부터 식별자를 읽는다. 휴대전화는 이동통신망을 통해 태그 식별자를 로컬 ODS 서버로 전달하여 태그 식별자와 관련된 제품정보를 가진 OIS 서버의 위치를 파악한다[9]. 휴대전화는 OIS 서버로부터 제품정보를 얻어 사용자에게 보여준다.

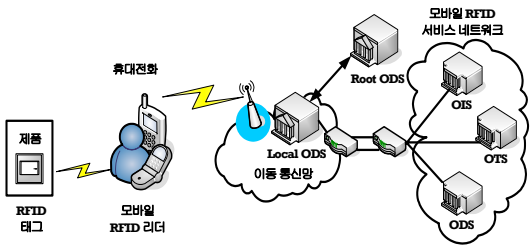

그림 1. 모바일 RFID 개념도

2.2 모바일 RFID 보안 요구사항

현재 RFID 태그는 992비트의 저장 공간을 가지면서 약 초당 100KB의 데이터 전송 비율을 나타내고 있다. 그러나 현재까지 개발된 RFID 태그는 저비용의 강한 암호 프리미티를 사용하여 프라이버시를 보호하고 있어 강한 암호 프리미티를 사용하지 않을 경우 RFID의 프라이버시 보호는 보장받지 못한다. 낮은 가격의 범위를 벗어나지 않으면서 보안 및 프라이버시 위험을 고려한 태그 및 리더의 설계가 현재 중요한 문제로 대두되고 있다. 미국의 시민단체인 전자프라이버시정보센터(EPIC: Electronic Privacy Information Center)[10]는 클리퍼 칩, 디지털 전화통신 제안, 의료기록 프라이버시, 그리고 소비자 개인정보 판매 같이 National Information Infrastructure(국가 정보 인프라)와 관련된 새로운 프라이버시 이슈에 대해 공공의 관심을 불러일으키기 위해 1994년에 설립되었다. EPIC는 소송을 수행하고, 각종 회의를 후원하고, 보고서를 생산하고, EPIC Alert를 출판하고 프라이버시 이슈에 대한 캠페인을 이끌고 있다. EPIC에서 RFID

표 1. EPIC의 분석한 RFID 위협요인

구 분	설 명
숨겨진 태그 장소	- RFID 태그들이 소유주인 개인들이 알지 못한 상황에서 사물들과 문서에 내장되어 질 수 있음 - 무선전파는 섬유, 플라스틱, 다른 물질들을 쉽게 조용하게 통과할 수 있기 때문에 지갑, 쇼핑 백, 옷가방 등에 들어있는 사물 또는 옷에 부착된 RFID 태그들을 읽을 수 있음
전세계 모든 사물들을 위한 유일한 식별자	- 전자제품코드(EPC)는 지구상에 있는 모든 사물에 유일한 ID를 가지게 할 수 있음 - 유일한 ID 번호의 사용으로 개별 물리적인 사물이 판매 또는 이전 시점에서 신원이 확인되고 구매자 또는 소유자와 연결될 수 있는 전 세계적인 사물 등록 시스템의 개발이 가능
대규모 데이터 통합	- RFID 배치는 유일한 태그 데이터를 포함하고 있는 대량 데이터베이스의 개발을 요구 - 이들 기록들은 특히 컴퓨터 메모리와 프로세서 능력이 확장되면서 개인 신원확인 데이터와 연결될 수 있음
숨어있는 리더	- 인간 또는 사물이 모여져 있는 어떤 환경에서도 보이지 않게 섞여질 수 있는 리더들에 의해 태그들은 시야의 제한 없이 멀리서 읽혀질 수 있음 - RFID 리더들은 이미 실제로 바닥 타일들에 내재되어 소비자들이 언제 또는 "스캔"되고 있는지 없는지에 대한 인식을 불가능하게 하고 있음
개인추적과 개인정보 프로파일	개인적인 신원이 유일한 RFID 태그 넘버와 연결되어 있다면 개인들이 인식하지 못하는 사이에 프로파일(profile)되고 추적당할 수 있음

를 이용하는 환경에서의 정보 위험요인을 표 1처럼 분석하고 있다.

모바일 RFID 시스템은 기존 RFID 시스템의 보안 요구사항 이외에 다음과 같은 추가 보안 요구사항이 필요하다[9,11]. 첫째, 태그는 정당한 이동 리더인지 인증을 통해 인증 받은 이동 리더에게만 정보를 제공해야 하며 둘째, 이동 리더는 태그처럼 소유자에 따라 이동하기 때문에 이동 리더를 소유한 사람의 위치 추적을 할 수 없어야 한다. 모바일 RFID 시스템에서 사용자의 프라이버시 침해 문제는 다음과 같이 나타난다[1,12].

2.2.1 정보의 노출(information leakage)

모바일 RFID 시스템은 무선통신을 사용하기 때문

에 사용자의 비밀정보가 쉽게 노출될 수 있기 때문에 제 3자에게 사용자의 비밀 정보를 노출시키지 않도록 사용자의 비밀정보에 대한 기밀성을 보장하여야 한다.

2.2.2 추적 가능(traceability)

모바일 RFID 시스템에서 태그가 이동 리더의 질의에 대해 항상 같은 값으로 응답하게 된다면 공격자는 사용자가 소유한 특정 태그를 추적함으로써 태그를 소유한 사용자의 위치 및 이동경로를 파악할 수 있기 때문에 공격자가 태그와 이동 리더의 위치 추적을 할 수 없도록 항상 다른 값으로 응답하거나 질의를 할 수 있도록 하여야 한다.

2.2.3 재사용 공격(Replay Attack)

제 3자가 리더와 태그 사이의 통신을 도청하여 정보를 저장함으로써 제 3자는 도청한 태그의 정보를 이용하여 리더가 태그에게 정보를 요청할 때 대신 응답할 수 있다. 이 공격을 막기 위해서는 전송된 정보의 재사용을 못하도록 태그의 정보를 매번 업데이트하거나 인증을 통해 이전에 사용되었던 값을 구분하여 재사용 공격(Replay attack)을 막아야 한다.

2.2.4 스푸핑 공격(Spoofing Attack)

제 3자가 태그에게 리더인 척하여 태그의 정보를 얻는 방법으로써 제3자는 정보를 받고 태그와의 통신이 정상적으로 끝나기 전에 세션을 종료함으로써 제 3자는 태그로부터 얻어낸 정보를 이용하여 리더를 속일 수 있다. 이 공격을 막기 위해서는 태그와 리더 또는 백 엔드 서버는 사전에 공유한 비밀 값을 가져야 하며 이를 이용하여 태그는 리더를 인증한다.

2.3 기존 연구

최근 휴대폰에 RFID 리더를 부착한 기술이 폭넓게 사용되면서 모바일 RFID 리더의 프라이버시 문제가 대두되고 있다. 모바일 RFID 리더의 프라이버시 문제를 해결하기 위해서 현재까지 여러 프로토콜이 제안되었다. Rieback et.al 기법[8]은 사용자가 소유하고 있는 상품에 대해 외부 리더의 접근을 통제하도록 모바일 단말기가 프록시와 같은 기능을 수행하는 기법을 제안하였다. Rieback의 RFID 가디언(Guardian)기법은 가디언(Guardian)이라는 모바일이나 PDA를 이용하여 사용자가 소유한 물건에 외부의 리더가 접근하는 것을 모두 컨트롤하면서 프록시를 사용하여 RFID 시스템에서 발생 할 수 있는 문제점들을 해결하고 있다. Juels et.al 기법[6]은 Rieback et.al 기법[8]과 유사한 기능을 제공하지만 프록시의 기능을 향상시켰으며 외부에서 태그에 의미 없는 값을 넣는 공격을 해결하기 위해서 프록시 자체에서 태그의 정보를 갱신하도록 하였다. Kim 등의 기법[12]은 Juels et. al 기법[6]과 Rieback et. al 기법[8]에 비해 도청 가능성과 에이전트 자체에 발생한 위변조를 방지할 수 있는 장점을 가졌지만 Juels et. al 기법[6]과 Rieback et. al 기법[8]처럼 프록시의 강력한 가정을 요구하지는 않는다. 그러나 리더와 태그 그리고 프록시의 키를 관리해주는 공개키 센터와 같은 신뢰성 있는 기관을 필요로 하는 단점이 있다. Kim 등의 기법[12]은 Juels et. al 기법[6]과 Rieback et. al 기법[8]처럼 부가적인 장치인 프록시를 사용하지는 않지만 프록시 기능을 모바일 RFID 리더가 수행하도록하여 RFID 시스템의 문제를 해결하기 위한 모바일 기반의 RFID 프라이버시를 보호하였으며 Kim 등의 기법[12]처럼 공개키 센터와 같은 신뢰성 있는 기관이 필요하지도 않는다. 특히, Kim 등의 기법[12]은 Juels et. al 기법[6], MARP 기법[7], Rieback et. al 기법[8]처럼 리더와 태그사이의 통신을 모두 감지하여 관리할 필요가 없기 때문에 해쉬 함수의 사용을 줄여 효율적이다. 그러나 모바일 RFID 리더의 프라이버시를 보호하기 위해 태그에서 처리하는 계산량이 높은 단점을 가진다. Cheon et. al 기법[13]와 Won et. al 기법[14]은 이동형 리더 소지자의 프라이버시를 보호하기 위한 AES-128을 사용하여 동선이 노출되는 문제를 해결하고 있지만 이동형 리더가 수동적으로 동작하기 때문에 이동성이 높은 모바일 환경에서는 비효율적인 단점이 있다. Ha et. al 기법[15]은 랜덤 수 발생기를 태그에서 사용하지 않으면서 인증에 필요한 태그의 연산량을 해쉬 체인을 이용하여 효율성을 향상시켰지만 상호 인증에 사용되는 ID가 재사용 공격기법을 통해 노출되기 때문에 사용자의 프라이버시를 보장받지 못하는 단점이 있다.

Ⅲ. 제안하는 프로토콜의 비교분석

이 절에서는 모바일 RFID 리더와 태그 사이에 송·수신되는 8비트 형태의 사용자 프라이버시 정보를 제 3자가 악용하지 않도록 모바일 RFID 리더의 랜덤수 R_{SR}을 임의의 크기로 분할하여 태그가 생성한 랜덤수를 해쉬함수에 적용하여 사용자의 프라이버시를 보호하는 인증 프로토콜을 제안한다. 제안 프로토콜에서는 리더가 이동성을 가지고 있기 때문에 태그와 인증을 수행하는 환경이 에이전트 기반의 인증 프로토콜을 수행한다.

3.1 개요

모바일 RFID 시스템은 휴대폰에 RFID 리더를 내장하여 휴대폰으로 태그를 읽었을 때, 여러 가지 서비스를 이동 통신망을 통해 제공받으려고 하는데 이때 모바일 RFID 리더는 개인화된 태그 정보에 대해서 개인 프라이버시 침해가 이루어지지 않아야 한다. 그림 2는 제안 프로토콜의 전체 인터페이스를 보여주고 있으며 그림 2에서 모바일 RFID 리더가 태그를 소유하게 되었을 때 모바일 RFID 리더와 태그는 데이터베이스와 사전에 동의된 공유키 K_{DB-R}와 K_{RT}를 이용하여 메시지를 전달한다.

모바일 RFID 리더를 부착한 사용자는 태그로부터 시리얼 넘버를 요청하여 전달받은 후 태그의 시리얼 넘버를 난수생성기에 적용하여 임의의 랜덤 수 R_{SR}를 생성하며 생성된 랜덤 수 R_{SR}을 태그에게 전달하기 위해서 모바일 RFID 리더는 자신이 생성한 랜덤 수 R_{SR}을 임의의 크기로 R'_{SR1}와 R'_{SR2}로 만들어 태그와 상호인증을 수행한다. 만약 상호인증이 수행되는 과정에서 백 엔드 서버에 저장되어 있는 모바일 RFID 리더와 태그의 정보가 일치한다면 모바일 RFID 리더는 태그에 대한 안전한 접근 제어를 수행할 수 있다. 제안기법에서 이동 RFID 리더가 랜덤 수 R_{SR}을 생성해서 임의의 크기로 분할하는 것은 첫째 전체 키 크기를 128비트에서 96비트로 줄이기 위해서이고 둘째, 기존 기법들과 마찬가지로 경량화 연산(XOR, OR) 만으로 보안을 제공하기 위해서이다. 마지막으로 수동형 공격뿐만 아니라 능동형 공격자에 대해서도 무결성을 제공하기 위해서 XOR 연산과 함께 충돌성이 없는 안전한 해쉬 함수를 사용하여 인식 거리가 먼 RFID 시스템에서도 사용하기 위해서이다.

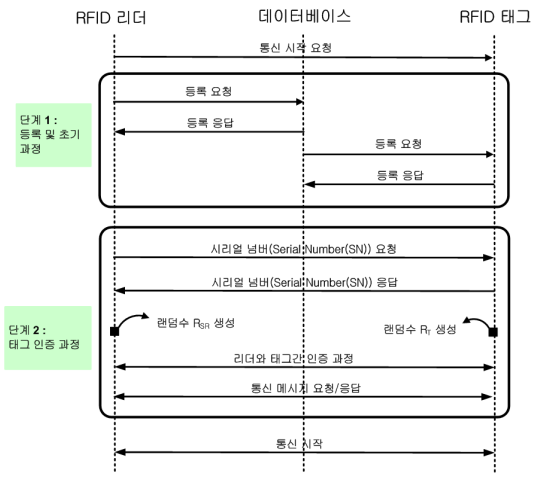

그림 2. 제안된 인증 프로토콜을 위한 시스템 구조

3.2 용어정의

표 2는 제안된 프로토콜에서 사용하는 용어에 대한 설명이다.

표 2의 SID_i는 태그의 보안 인식자로써 모든 사용자에게 태그와 함께 제공되며 인증을 위해 사용되는 공유키는 크게 K_{DB-R}와 K_{RT}가 있다. 정보의 최신성을 위해 제안 프로토콜에서는 랜덤 수 R_{SR}와 R_T를 사용하며 일방향성의 해쉬 함수 $h()$로 연접되어 공격자의 메시지 정보 노출 시도를 예방한다.

표 2. 제안 프로토콜의 용어 정의

용 어	정 의
SID_i	태그 i의 보안 ID
K_{DB-R}	벡엔드 서버와 리더가 공유한 공유키
K_{RT}	리더와 태그가 공유한 공유키
R_{SR}	리더가 생성한 랜덤 키
R'_{SR1}, R'_{SR2}	임의의 크기로 R_{SR}을 분할한 리더의 랜덤 키
R_T, R''_T	태그가 생성한 랜덤키
R'_{T1}, R''_{T1}, R'_{T2}, R''_{T2}	임의의 크기로 R_T을 분할한 태그의 랜덤 키
I	현재 세션에서 리더와 태그의 통신 연결 상태 정보
M, M', T, T', S	XOR 연산과 해쉬함수를 이용하여 생성한 정보
$E_K(D)$	키 K를 이용하여 메시지 D를 암호화
$D_K(D)$	키 K를 이용하여 메시지 D를 복호화
$h_n()$	n 값으로 해쉬한 keyed hash 알고리즘
$\|\|$	연접

3.3 모바일 RFID 사용자의 프라이버시 보호 프로토콜

이 절에서는 모바일 RFID 리더와 태그 사이에 송·수신되는 8비트 형태의 스트림 방식의 메시지를 보호하기 위해 초기화 과정과 상호 인증과정으로 분류하고 있다.

3.3.1 초기화 과정

초기화 과정은 모바일 RFID 리더와 태그가 벡 엔드 서버의 데이터베이스에 상호인증에 필요한 사전 정보를 생성하는 과정이다. 모바일 RFID 리더와 태그

는 메시지를 암호화하기 위해서 사전에 공유된 공유키 K_{RT}을 해쉬 체인에 적용하여 공유키 K_{RT}을 초기화한다. 벡엔드 서버는 모바일 RFID 리더와 태그가 사전에 등록한 RFID 태그의 보안 인식자 SID를 이용하여 RFID 태그의 사용자 인증과 무결성을 체크한다. RFID 태그의 보안 인식자 SID는 RFID 태그의 메모리내에 존재하는 보안 ID의 위치 코드값을 추출한 후 계산되어진다. 보안 인식자 SID는 메모리에 저장된 보안 ID의 시작 주소로부터 일정 크기만큼 떨어진 옵셋 크기만큼을 실시간으로 암호학적 해쉬(e.g. SHA-1)에 적용하여 생성한다. 보안 인식자 SID는 옵셋 리스트와 해쉬 값이 일치하는 경우에만 내부 메모리에 안전하게 저장되면서 외부 프로그램에 노출되거나 읽히지 않는다. 태그가 새로운 모바일 RFID 리더 인식자 정보를 메모리에 갱신하려고 할 때도 새로운 모바일 리더 인식자는 이전 모바일 리더 인식자와 함께 해쉬체인되어 암호화된다. 제안 프로토콜에서 생성되는 태그의 보안 인식자 SID는 수신기마다 서로 다른 인식자를 사용하기 때문에 제 3자가 복제된 자신의 태그를 다른 모바일 RFID 리더에 사용할 경우 모바일 RFID 리더가 태그를 인식하지 못하도록 한다.

3.3.2 상호 인증 과정

상호 인증 과정은 다수의 모바일 RFID 리더가 백엔드 서버에 접속하여 프라이버시 보호가 필요한 태그에 대해서 모바일 RFID 리더 자신 이외에는 어떠한 정보도 제공하지 않도록 모바일 RFID 리더와 태그 사이에 상호 인증하는 과정으로써 모바일 RFID 리더와 태그 자신이 생성한 랜덤 수를 임의의 크기로 나누어 상호인증에 사용되기 때문에 추가적인 암호 계산이 필요없어 계산 비용이 적은 특징이 있다. 상호 인증과정의 세부적인 동작 과정은 다음과 같다.

- 단계 1 : 모바일 RFID 리더는 통신 범위안에 들어온 태그들에 대해서 안전한 채널을 통해 사전에 공유된 공유키 K_{RT}를 이용하여 프라이버시 보호가 필요한 태그들에게 시리얼 번호 요청 메시지를 보내고 응답을 받는다. 이때, SN은 태그의 사용자가 임의로 선택하는 값이므로 최초 등록이 이루어지면 모바일 RFID 리더의 랜덤 수 R_T을 보호하기 위해 사용되는 값이므로 모바일 RFID 리더와 태그가 최초에 안전하게 공유하였다면 이후에는 사용할 필요가 없다.

- 단계 2 : 모바일 RFID 리더는 태그로부터 전달받은 태그의 시리얼 번호(SN, Serial Number)를 난수 생성기에 적용하여 태그에게 전달할 태그의 랜덤 수 R_T를 생성하는 동시에 태그에게 전달한다. 태그는 전달받은 정보 $E_{SN}(R_T)$를 복호화($D_{SN}(R_T)$)하여 모바일 RFID 리더가 생성한 R_T를 얻는다.
  이 때, 모바일 RFID 리더는 난수 생성기를 이용하여 랜덤 수 R_T를 생성한다. 모바일 RFID 리더는 랜덤 수 R_{SR}을 임의의 크기로 나누어(Concatenation) R'_{SR1}과 R'_{SR2}을 생성한다.

- 단계 3 : 모바일 RFID 리더는 사전에 태그와 공유된 공유키 K_{RT}을 이용하여 R'_{SR2}를 암호화한 후 챌린지를 통해 태그에게 전달하고 태그의 시리얼 번호를 이용하여 $R_T \| R'_{SR1}$ 값을 해쉬한 S(=$h_{SN}(R_T \| R'_{SR1})$)값을 태그에게 요청 메시지와 함께 전송한다.

- 단계 4 : 단계 1에서 모바일 RFID 리더와 태그가 서로 공유한 시리얼 번호 SN을 이용하여 모바일 RFID 리더로부터 전달받은 S에서(로부터) $R_T \| R'_{SR1}$을 추출한 후 태그는 단계 2-3에서 복호화한 R'_T와 XOR하여 랜덤 수 R'_{SR1}을 얻는다. 이 과정은 불법적으로 태그의 프라이버시를 침해하는 스푸핑 공격을 예방하기 위해서 필요하다. 태그는 태그 정보의 기밀성을 제공하기 위해 모바일 RFID 리더에게 받은 S값과 각 태그마다 생성된 보안 인식자 SID 그리고 태그의 랜덤 값 R''_T을 연접한 후 모바일 RFID 리더의 R'_{SR2}로 해쉬한 M(=$h_{R'_{SR2}}(SID \| S \| R''_T)$)을 생성한다. 태그는 R''_T를 임의의 크기로 나누어 R''_{T1}과 R''_{T2}을 생성한 후 비동기화 공격으로 인해 데이터가 손실되는 것을 탐지하기 위해 모바일 RFID 리더의 R'_{SR2}로 해쉬한 $h_{R'_{SR2}}(R''_{T1})$값과 상태정보 I를 연접한 T(=$h_{R'_{SR2}}(R''_{T1}) \| I$)를 생성한다.

- 단계 5 : 태그는 사전에 모바일 RFID 리더와 태그간 공유한 K_{RT}을 이용하여 R''_{T2}를 암호화 한 $E_{K_{RT}}(R''_{T2})$와 M, T, I, S 등을 모바일 RFID 리더

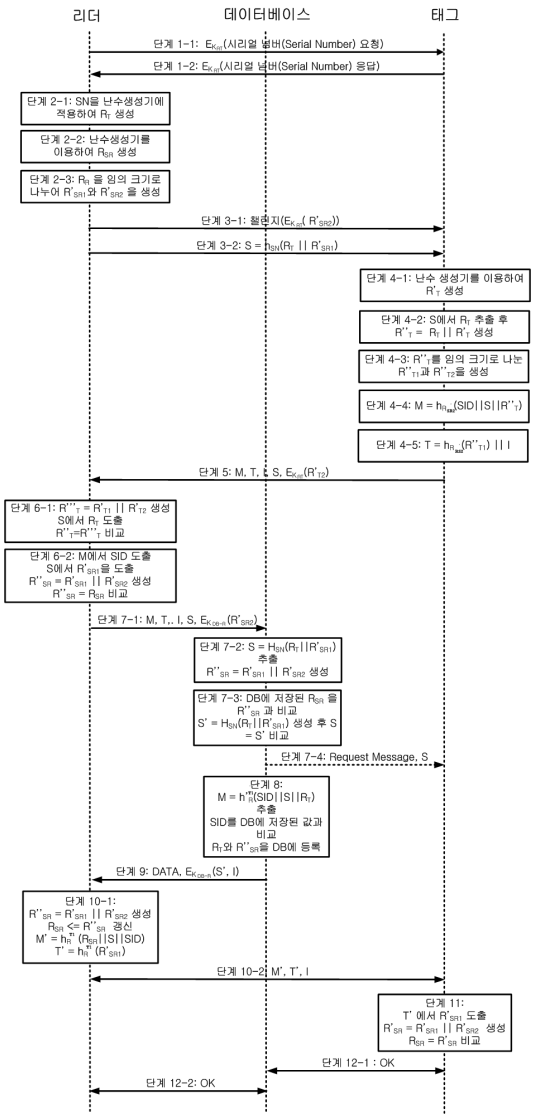

그림 3. 프라이버시를 보장받기 위한 상호인증과정

에게 전송한다.

- 단계 6 : 태그로부터 데이터를 전달받은 모바일 RFID 리더는 태그와의 동기화를 유지하고 있는지 확인하기 위해서 전달받은 M과 T 을 모바일 RFID 리더의 비밀키 R'_{SR2}로 해쉬하여 R'''_T(= $R''_{T1} \| R''_{T2}$)와 R''_{SR}(=$R'_{SR1} \| R'_{SR2}$)을 생성하여 모바일 RFID 리더가 보유하고 있는 R''_T와 R_{SR}을 비교한다.

- 단계 7 : 모바일 RFID 리더의 랜덤 수의 비교가 만약 일치한다면 재동기화를 위해 모바일 RFID 리더와 데이터베이스간 공유한 K_{DB-R}을 이용하여 R''_{T2}를 암호화 한 $E_{K_{DB-R}}(R''_{T2})$, M, T, I, S 등을 데이터베이스에 전송하고 만약 일치하지 않는다면 전송과정에서 비동기화가 발생했음을 탐지하고 재동기화를 위해 동기화 요청 메시지와 S(= $h_{SN}(R_T \| R'_{SR1})$)을 태그에게 재전송한다.

- 단계 8 : 데이터베이스는 사전에 등록된 태그의 시리얼 번호를 이용하여 $R_T \| R'_{R1}$ 값을 SN으로 해쉬한 S(=$h_{SN}(R_T \| R'_{SR1})$)와 R''_{SR}(=$R'_{SR1} \| R'_{SR2}$)을 생성한 후 데이터베이스에 저장되어 있는 R_{SR} 값과 비교한다. 그리고 데이터베이스는 태그의 시리얼 번호 SN을 이용하여 $R_T \| R'_{SR1}$ 값을 해쉬하여 S'(=$h_{SN}(R_T \| R'_{SR1})$)값을 생성하여 모바일 RFID 리더로부터 전달받은 S 값과 비교한다. 만약 일치하면 데이터베이스에 R_T와 R''_{SR} 값을 새로 업데이트한 후 새로 갱신된 S값과 데이터를 모바일 RFID 리더에게 전달하고 일치하지 않으면 통신을 종료한다.

- 단계 9 : 모바일 RFID 리더는 R''_{T1} 값을 이용하여 $R_{SR} \| S \| SID$ 값을 해쉬한 M'(=$h_{R''_{T1}}(R_{SR} \| S \| SID)$)와 R'_{SR1} 값을 해쉬한 T'(=$h_{R''_{T1}}(R'_{SR1})$)을 상태정보 I와 함께 태그에게 전달한다.

- 단계 10 : 태그는 모바일 RFID 리더로부터 M', T', I을 전달받은 후 T'에서 R'_{SR1}을 도출하여 R'_{SR2}와 연접(concatenate)하여 R'_{SR}을 생성한 후 M'로부터 추출된 모바일 RFID 리더의 랜덤수 R_{SR}과 비교한다.

- 단계 11 : 모바일 RFID 리더는 데이터베이스로부터 전달받은 태그의 상태정보 I와 S를 비교한 후 일치하면 데이터베이스에게 확인 메시지를 전달하고 그렇지 않으면 종료한다. 태그는 모바일 RFID 리더의 랜덤수 R_{SR}와 R'_{SR}을 비교한 후 일치하면 데이터베이스에게 확인 메시지를 보내고 그렇지 않으면 종료한다.

- 단계 12 : 모바일 RFID 리더와 태그의 상호 인증

과정이 정상적으로 이루어졌다면 데이터베이스에게 *OK* 확인 메시지를 전달한다.

Ⅳ. 제안 프로토콜의 비교분석

4.1 보안 평가

이 절에서는 백 엔드 서버와 모바일 RFID 리더 사이나 모바일 RFID 리더와 태그 사이의 무선 구간에서 발생하시 쉬운 재사용 공격, 스푸핑 공격, 정보노출, 비동기화 공격, 불추적성 등에 대해서 제안 프로토콜를 평가한다.

4.1.1 재사용 공격

제안된 프로토콜에서 사용되는 해쉬 함수는 역으로 변환하기 어렵기 때문에 태그 인식자의 출력값이 공격자에 의해 캡처되더라도 태그의 보안 인식자 *SID*는 안전하며 태그가 새로운 모바일 RFID 리더 인식자 정보를 메모리에 갱신하려고 할 때도 새로운 모바일 리더 인식자는 이전 모바일 리더 인식자와 함께 해쉬 체인되어 암호화되기 때문에 리더와 태그사이의 통신이 도청될 때 안전성을 보장받는다. 제안된 프로토콜에서 생성되는 태그의 보안 인식자 *SID*는 수신기마다 서로 다른 인식자를 사용하기 때문에 제 3자가 복제된 자신의 태그를 다른 모바일 RFID 리더에 사용할 경우 모바일 RFID 리더가 태그를 인식하지 못하도록 한다.

4.1.2 스푸핑 공격

제안 프로토콜에서는 태그의 시리얼 넘버 값을 이용하여 계산된 S(=$h_{SN}(R_T \| R_{R1}^{'})$)값을 제 3자가 불법적으로 생성하려고 할 때 태그는 난수 생성기를 이용하여 태그 자신의 $R_T^{'}$를 생성한 후 모바일 RFID 리더로부터 전달받은 S에서 모바일 RFID 리더가 태그를 위해 생성한 랜덤 수 R_T을 추출 후 연접(concatenate)하여 $R_T^{''}$을 생성한다. 제 3자는 랜덤수를 모르기 때문에 올바른 S를 생성할 수 없어 스푸핑 공격에 안전하다. 또한 공격자가 정당한 모바일 RFID 리더로 가장하여 $S^{'}$를 태그에게 전송할 때 태그의 출력값을 도청하여 저장한 후 다음 세션에서 정당한 모바일 RFID 리더가 S를 태그에게 전송할 때 공격자는 이전 세션에 도청하여 저장한 값을 대신 전송한다. 이 때 모바일 RFID 리더는 백엔드 서버에 그 값을 전송하지만 스푸핑 공격과 마찬가지도록 S≠S'을 통해 공격을 막을수 있다.

4.1.3 정보노출방지

제안 프로토콜에서는 다수의 태그들이 모바일 RFID 리더에게 접근할 때마다 모바일 RFID 리더와 태그가 랜덤수(R_R, R_T)를 생성하여 비밀 정보의 노출을 예방하고 있다. 제안 프로토콜에서는 모바일 RFID 리더와 태그 사이의 무선구간에서 제 3자가 태그를 인식하지 못하도록 태그의 인식자를 비밀 인식자 *SID*를 사용한다. 백엔드 서버는 다량의 모바일 RFID 리더 사용자가 프라이버시 보호가 필요한 태그된 물품에 대해 자신 이외에 다른 모바일 RFID 리더에게 어떠한 정보도 제공하지 않도록 하기 위해서 태그가 모바일 리더에게 접속을 요청하여 통신을 수행할 때마다 랜덤 수(R_R, R_T)를 생성하여 모바일 리더의 데이터베이스에 저장되어 있는 정보를 업데이트한다.

4.1.4 비동기화

제안 프로토콜에서는 태그 정보의 기밀성을 제공하기 위해서 모바일 RFID 리더에게 받은 S값과 각 태그마다 생성된 보안 인식자 *SID* 그리고 태그의 랜덤값 $R_T^{''}$을 연접한 후 모바일 RFID 리더의 $R_{R2}^{'}$로 해쉬한 M(=$h_{R_{R2}^{'}}(SID \| S \| R_T^{''})$)을 생성하게 된다. 이 때, 태그는 생성된 정보 중 $R_T^{''}$를 $R_{T1}^{''}$와 $R_{T2}^{''}$로 임의의 크기로 나눈 후 모바일 RFID 리더의 $R_{R2}^{'}$로 해쉬한 $h_{R_{R2}^{'}}(R_{T1}^{''})$값과 상태정보 I를 연접한 T(=$h_{R_{R2}^{'}}(R_{T1}^{''}) \| I$)를 모바일 RFID 리더에게 전달한다. 모바일 RFID 리더는 전달된 랜덤수의 비교가 일치한다면 재동기화를 위해 모바일 RFID 리더와 데이터베이스간 공유한 K_{DB-R}을 이용하여 $R_{T2}^{''}$를 암호화 한 $E(K_{DB-R}, R_{T2}^{''})$, M, T, I, S 등을 데이터베이스에 전송하고 만약 일치하지 않는다면 전송과정에서 비동기화가 발생했음을 탐지하고 재동기화를 위해 동기화 요청 메시지와 S(=$h_{SN}(R_T \| R_{R1}^{'})$)을 태그에게 재전송한다.

4.1.5 불추적성

무선 구간에서 전송되는 데이터는 모바일 RFID 리더와 태그가 생성한 랜덤수를 임의의 크기로 분할한 하부 키($R_{R1}^{'}$, $R_{R2}^{'}$, $R_{T1}^{'}$, $R_{T2}^{'}$)로 해쉬하여 전송한다. 이 때, 일방향성의 특성에 의해 해쉬되기 이전의 값을 알아낼 수 없어 의미 있는 정보를 얻을 수 없기 때문에 정보 노출을 예방할 수 있다. 또한 매 세션마다 모바일 RFID 리더와 태그가 생성한 랜덤수를 난수생성기에 의해 항상 다른 키 값을 만들기 때문에 공격자는

어떤 값이 나올지 예상할 수 없어 모바일 RFID 리더와 태그의 위치를 추적하는 것은 현실적으로 불가능하다. 제안 프로토콜은 다수의 모바일 RFID 리더들을 위해 백 엔드 서버내에 모바일 RFID 리더의 랜덤 값과 태그의 시리얼 넘버를 저장하는데 이때 저장된 모바일 RFID 리더의 랜덤값과 태그의 시리얼 넘버는 테이블 검색 방법을 통해 검색되어 모바일 RFID 리더들의 테이블내 정보를 노출하지 않아도 된다.

4.2 효율성 평가

모바일 RFID 환경의 모바일 RFID 리더와 태그 사이의 통신을 [7,12]의 기존 기법들과 비교 평가한 결과 MARP 기법[7]은 프록시를 사용하는 가정을 기반으로 동작되기 때문에 RFID 시스템에서 내포하고 있는 문제들을 완전하게 해결하기 어려운데 반해 Kim 등의 기법[12]과 제안 프로토콜은 모바일 RFID 리더가 태그의 정보를 읽어올 때만 태그에게 신호를 보내기 때문에 효율적이다. 표 3은 [12]에서 언급한 평가항목을 기반으로 모바일 RFID 시스템의 효율성을 향상시키기 위해 제시된 프로토콜, 즉 MARP 기법[7]과 Kim 등의 기법[12]들의 저장 공간과 계산량(등록 계산량, 로그인 계산량, 인증 계산량 포함)을 태그, 모바일 RFID 리더, 데이터베이스 항목으로 평가하고 있다.

MARP 기법[7]과 Kim 등의 기법[12]에서는 96bit의 키를 4개로 분할하여 분할된 키길이를 24비트로 사용하여 리더에서 두 개의 난수를 생성하여 보안을 제공하고 있지만 제안 기법에서는 64 비트의 키를 2개로 분할하여 기존 기법에서는 24비트의 키를 사용하여 2^{24}개의 키를 생성하는 고정에서 키 값이 노출되나 제안 기법에서는 32비트의 키를 사용하여 2^{32}개의 키를 생성하여 키 노출에 대하여 MARP 기법과 Kim 등의 기법보다 안전성을 향상시키고 있다.

제안 프로토콜은 등록 계산량과 로그인 계산량에서 모듈러 연산을 사용하는 기존 프로토콜과 달리 일방향 해쉬 함수을 2번 사용하여 사용자의 정보를 등록한다. 인증 계산량에서는 기존 프로토콜에 비해 일방향 해쉬 함수를 많이 사용하지만 상호인증을 지원하는 특징이 있다. 저장 공간과 계산량 측면에서 제안 프로토콜은 Kim 등의 기법[12]에 비해 모바일 리더에서 $1l$과 $1H$ 만큼 더 필요하지만 태그에서는 Kim 등의 기법[12]보다 적은 계산량을 가진다. 태그의 특성상

표 3. 효율성 비교평가

동작 \ 프로토콜		MARP 기법[7]	Kim 등의 기법[12]	제안 프로토콜
저장공간	태그	$3l$	$2l$	$2l$
	모바일 리더	$7l$	$1l$	$2l$
	데이터베이스	$5l$	$2l$	$2l$
등록 계산량		1 T_{Exp}, 2 T_H	1 T_{Exp}, 2 T_H	2 T_H
로그인 계산량		1 T_{Exp}, 2 T_H	1 T_{Exp}, 2 T_H	2 T_H
인증 계산량		1 T_H (상호인증 포함하지 않음)	1 T_{Exp}, 2 T_H	4 T_H (상호 인증 포함)
전체 키 길이		96bit/4	96bit/4	64bit/2
분할 키 길이		24bit	24bit	32bit
키 조합 개수 (안전성)		2^{24}	2^{24}	2^{32}
계산량	태그	$2H+3X$	$1H+1X$ (구매 전) $1H+2X$ (구매 후)	$H+2X+D$
	모바일 리더	$(3E+1\ D+2\ V+2S+1H+1X)M$	- (구매 전) $(1H+2X)N$ (구매 후)	$(2H+2X)N+E$
	데이터베이스	$1E+3D+2V+1S+2H+1X$	$1H+1X$ (구매 전) - (구매 후)	$1H+1X$

T_{Exp} : 모듈러 연산에 대한 계산 시간 T_H : 일방향 해쉬 함수에 대한 계산시간
l : 해쉬 함수의 출력 길이나 키의 길이 또는 ID의 길이 M : MARP가 감지할 수 있는 영역 내에 존재하는 태그의 수
X : XOR 비트 연산 E : 한 번의 암호화 연산 D : 한번의 복호화 연산
V : 한번의 서명 검증 연산 S : 한 번의 서명 연산 H : 한번의 해쉬 연산
N : 모바일 리더가 소유한 키의 수 - : 고려사항 없음

연산비용에 대한 부담을 줄이면서 연산비용의 부담이 태그보다 비교적 적은 모바일 RFID 리더에 1*l* 만큼 부과함으로써 제안 프로토콜은 모바일 RFID 시스템의 효율성을 Kim 등의 기법[12]보다 향상시키고 있다.

V. 결 론

모바일 RFID 서비스가 휴대폰에 접목하여 최근 급속하게 증가하고 있지만 백엔드 서버와 모바일 RFID 리더, 모바일 RFID 리더와 태그 사이의 무선구간은 보안 위협에 노출되어 있다. 이 논문에서는 모바일 RFID 리더가 태그 정보를 백엔드 서버로부터 안전하게 전달받기 위해서 초기화 과정과 상호 인증과정에서 모바일 RFID 리더와 태그가 생성한 랜덤키를 임의의 크기로 분할하여 프라이버시 보호가 필요한 태그에 대해서 어떠한 정보도 제 3자에게 제공하지 않는 프라이버시 보호 프로토콜을 제안했다. 제안된 프로토콜은 DoS 공격이나 시스템 오류로 인해 발생할 수 있는 보안 문제를 해결하기 위해서 모바일 RFID 리더, 태그 그리고 백엔드 서버의 동기화를 유지하도록 하고 있으며 통신 파티 사이에 키 쌍을 유지하고 분배할 때 발생하는 오버헤드를 제거함으로써 효율성을 향상시켰다. 성능 평가 결과 제안 프로토콜은 일방향 해쉬함수와 키 분배 방법을 통해 상호인증을 수행하기 때문에 MARP 기법과 Kim 등의 기법보다 계산량에서 효율성이 높았다. 향후 연구에서는 이동 사용자의 권한 접근 및 레벨을 부여하여 사용자 프라이버시를 보장하는 메커니즘을 연구 수행할 계획이다.

참 고 문 헌

〔1〕 박남제, 강유성, “모바일 RFID 보안기술”, TTA Journal No.115, pp.108-114, 2008. 2.

〔2〕 장병준, 이윤덕, “모바일 RFID 기술 동향 및 주요 이슈”, IITA, 주간기술동향, 통권 1206호, pp. 26-35, 2005.

〔3〕 이승민, 김은환, 전문석, “모바일 RFID를 위한 보안 RFID 상호인증 프로토콜 설계”, 한국통신학회논문지 제35권 제2호(네트워크 및 서비스), pp. 183-190, 2010.2

〔4〕 이병길, 강유성, 박남제, 최두호, 김호원, 정교일, “능동 및 모바일 RFID 서비스 환경에서의 정보보호 기술”, 정보보호학회논문지 제15권 제3호, pp.40-47, 2005. 6.

〔5〕 김수철, 여상수, 김성권, “RFID 프라이버시 보호를 위한 향상된 모바일 에이전트 기법”, 한국통신학회논문지 제 33권 제2호(통신이론 및 시스템), pp.208-218, 2008. 2.

〔6〕 A. Juels, P. Syverson, and D. Bailey, “High-Power Proxies for Enhancing RFID Privacy and Utility”, CHACS 2005, LNCS 3856, pp.210-226, 2005.

〔7〕 S. C. Kim, S. S. Yeo, S. K. Kim,“MARP: Mobile Agent for RFID Privacy Protection”, 7th Smart Card Research and Advanced Application IFIP Conference(CARDIS’06), Lecture Notes in Computer Science, vol. 3928, pp.300-312, 2006.

〔8〕 M. Rieback, B. Crispo, and A. Tanenvaum, “RFID Guardian: A Battery-powered Mobile Device for RFID Privacy Mangement”, ACISP 2005, LNCS 3574, pp.184-194, 2005.

〔9〕 정윤수, 김용태, 박길철, 이상호, “RFID를 이용한 IPTV 사용자의 경량화 인증 프로토콜“, 한국정보보호학회논문지, v.19, no.2, pp.105-115, 2009년 4월.

〔10〕 EPIC, http://epic.org/

〔11〕 H. Y. Chien, T. C. Wu, “Improving Varying-Pesudonym-Based RFID Authentication Protocols to Resist Denial-of-Service Attacks”, 한국정보보호학회논문지, v.18, no.6B, pp.259-269, 2008년 12월.

〔12〕 김일중, 최은영, 이동훈, “모바일 기반의 RFID 프라이버시 보호 기법”, 정보보호학회논문지 제17권 제 1호, 2007.2.

〔13〕 천지영, 황정연, 이동훈 “이동형 리더 소지자의 프라이버시를 보호하는 RFID 태그 검색 프로토콜”, 한국정보보호학회논문지, Vol.19, No.5, pp.59-69, 2009년 10월.

〔14〕 원태연, 천지영, 박춘식, 이동훈, “수동형 RFID 시스템에 적합한 효율적인 상호 인증 프로토콜 설계”, 한국정보보호학회논문지, Vol.18, No. 6A, pp.63-73, 2008년 12월.

〔15〕 하재철, 백이루, 김환구, 박제훈, 문상재, “해쉬함수에 기반한 경량화된 RFID 인증 프로토콜”, 한국정보보호학회논문지, Vol.19, No.3, pp.61-72, 2009년 6월.

정 윤 수 (Yoon-Su Jeong) 정회원

1998년 2월 청주대학교 전자계산학과 학사
2000년 2월 충북대학교 대학원 전자계산학과 석사
2008년 2월 충북대학교 대학원 전자계산학과 박사
2008년 3월~현재 충북대 및 한남대 시간강사
2009년 9월~현재 한남대 산업기술연구소 전임연구원
<관심분야> 유·무선 보안, 암호이론, 정보보호, Network Security, 이동통신보안

박 길 철 (Gil-Cheol Park) 정회원

1983년 2월 한남대학교 전자계산학과 학사
1986년 2월 숭실대학교 전자계산학과 석사
1998년 2월 성균관대학교 전자계산학과 박사
2006년 3월~2007년 2월 UTAS, Australia 교환교수
1998년 8일~현재 한남대학교 멀티미디어학부 교수
2005년 2월~현재 한국정보기술학회 이사 멀티미디어 분과 위원장
<관심분야> multimedia and mobile communication, network security

김 용 태 (Yong-Tae Kim) 정회원

1984년 2월 한남대학교 계산통계학과 학사
1988년 2월 숭실대학교 전자계산학과 석사
2008년 2월 충북대학교 전자계산학과 박사
2002년 12월~2006년 2월 (주) 가림정보기술 이사
2010년 9월~현재 한남대학교 멀티미디어학부 교수
<관심분야> 모바일 웹서비스, 정보보호, 센서 웹, 모바일 통신보안

이 상 호 (Sang-Ho Lee) 종신회원

1976년 2월 숭실대학교 전자계산학과 학사
1981년 2월 숭실대학교 전자계산학과 석사
1989년 2월 숭실대학교 전자계산학과 박사
1981년 3월~현재 충북대학교 전기전자 컴퓨터 공학부 교수
<관심분야> 네트워크보안, Protocol Engineering Network Management,