情 報 保 護 學 會 誌
第 15 卷 第 3 號, 2005. 6

능동 및 모바일 RFID 서비스 환경에서의 정보보호 기술

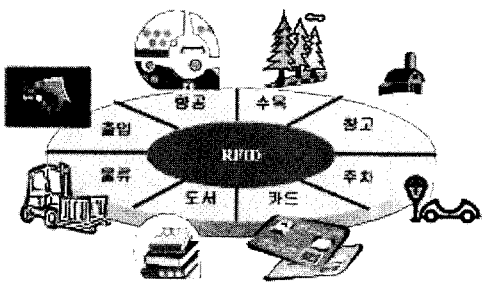
이 병 길*, 강 유 성*, 박 남 제*, 최 두 호*, 김 호 원*, 정 교 일*

요 약

RFID(Radio Frequency Identification)기술은 제조업체에서 상품 출하시 상품에 붙여서 유통, 물류, 판매, 사후관리 등 다양한 응용 분야로 적용될 수 있어 파급 효과가 큰 기술이다. 강력한 보안기능이 요구되는 환경에서는 능동형 RFID 기술이 적용되고 있으며, 이동환경에서 다양한 응용 서비스와 접목하기 위한 모바일 RFID 기술이 개발되고 있다. 그러나 RFID 서비스 환경에서 불법적인 위변조·도청·추적 등은 기업의 물품정보 뿐만 아니라 개인의 이동에 따른 위치, 시간 등 개인프라이버시 정보까지 파악될 수 있어, 보안 및 사생활 침해에 심각한 위협이 되고 있다. 따라서 최근 활발히 진행되고 있는 능동 및 모바일 RFID 서비스 환경에 적합한 정보보호 기술과 개인 프라이버시 보호 기술에 대한 연구동향과 표준화 동향에 대하여 소개하고자 한다.

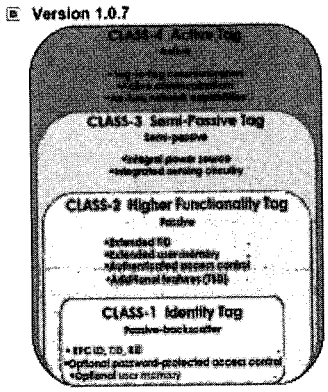
Ⅰ. 서 론

최근 활발하게 기술개발이 진행되고 있는 RFID 기술은 그림 1과 같이 기업의 물품생산, 물류, 판매, 고객관리 등 다양한 산업에 적용이 가능할 뿐 아니라, 개인의 이동환경에서 물품을 소지하고 관리하는 일상생활에서 부터 휴대 단말을 통하여 다양한 정보를 제공 받을 수 있는 매체로서도 확대될 수 있어 중요성 및 파급효과가 급속히 증대되고 있다. RFID 태그의 종류는 기술개발 단계와 적용될 수 있는 분야에 따라 전원이 공급될 수 있는 능동형과 상대적으로 전원이 제공되지 않는 수동형으로 구분될 수 있다. 그러나 최근 EPCglobal에서는 태그의 기능적 특성에 따라 기존의 메모리가 없는 읽기 전용 태그를 제외하고, 새로이 개발 적용될 태그는 그림 2와 같이 크게 4가지 클래스로 구분하고 있다. 그림 2에서 클래스 1은 수동형 태그로서, 읽기 및 쓰기 기능과 사용자 메모리 영역을 가지며, Kill 명령과 간단한 패스워드를 통한 보안기능이 포함되어 있다. 클래스 2는 좀 더 확장된 기능을 가지는 수동형 태그이며, 클래스 3은 센싱 기능과 전원제공이 되는 능동형으로 진화되는 단계의 태그이다. 즉, 태그에서 주변의 환경정보를 센싱하는 기능을 갖춤으로서 세미-수동형 또는 자체 전원기능을 가짐으로서 능동형으로 구분될 수 있는 구조이다. 그리고 클래스 4는 통신능력이 보강된 능동형 태그로서, 태그간 통신과 Ad-hoc망을 구성할 수 있는 USN 노드에 해당되는 가장 진화된 능동형 태그로 볼 수 있다. 이러한 태그는 기술의 발전과 요구 환경에 따라 맞는 클래스의 기능을 탑재한 형태로서 적용되어야 할 것이다. 태그에 적용될 보안 기술 또한 해당 클래스에 맞는 보안기능을 탑재하여야 하며, 좀 더 안전성이 요구되는 환경에서는 보안기능이 강화된 태그가 적용될 수 있을 것이다. 따라서 본 고에서는 최근 ISO에서 정의한 능동형 태그에서의 보안 기술과 국내에서 활발히 진행중인 모바일 RFID 표준화 기술동향 및 주요 이슈들에 대하여 검토하고자 한다.



〔그림 1〕 RFID 응용 분야

* 한국전자통신연구원 RFID/USN보안연구팀 ({bglee, youskang, namjepark, dhchoi, khw, kyoil}@etri.re.kr)



〔그림 2〕 EPCglobal의 태그 분류

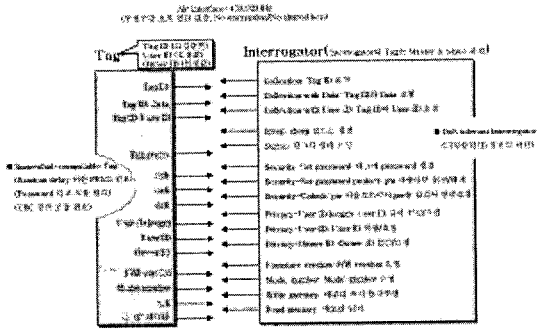
II. 능동형 RFID 보안 기술 및 표준화 동향

ISO 국제 표준으로 제정된 능동형 RFID 무선 접속 규격은 ISO/IEC 18000-7 규격이다.[1] 본 규격은 433.92 MHz에서의 능동형 RFID 태그의 물리 계층 특성과 리더와 태그 사이의 명령/응답 형식을 정의하고 있다. 능동형 RFID의 대표적인 활용은 화물 컨테이너 관리 시스템이며, ISO에서는 E-Seal(Electronic Seal)이라는 명칭으로 화물 컨테이너 관리를 위한 RFID 시스템 규격의 표준화를 진행하고 있다. 그 결과로써 2005년 상반기에 ISO 18185 규격의 일부가 드래프트 규격으로 공개되었다. 그 중 ISO 18185-7 규격은 WD(Working Draft) 상태로써 E-Seal의 물리 계층 규격을 정의하기 위하여 ISO/IEC 18000-7 규격을 따른다고 규정하고 있다.[2]

능동형 RFID 보안 기술의 표준화를 위하여 ISO/IEC 18000-7 규격은 낮은 수준의 리더 인증 메커니즘을 정의하고 있으며, ISO 18185-4 규격에서는 화물 컨테이너 관리용 E-Seal 시스템 보안 기술의 정의를 논의하기 시작하였다.[3] 따라서 본 고에서는 상기 2개 문서를 분석하여 능동형 RFID 보안 기술의 표준화 동향을 살펴보고자 한다.

2.1 ISO/IEC 18000-7

ISO/IEC 18000-7 규격은 2004년 8월에 공식적으로 발표된 ISO 국제 규격으로써 능동형 RFID 시스템의 호환성을 위해서는 반드시 지켜져야 하는 표준이다. 여기에는 패스워드에 기반하여 태그가 리더의 명령에 응답할지 안 할지를 결정하는 인증 방식을 정의함으로써 낮은 수준이지만 리더 인증 메커니즘을 포함하고 있다. 그림 3은 능동형 RFID 태그와 리더 사



〔그림 3〕 능동형 RFID 리더-태그 명령/응답

이의 명령/응답 종류를 보이고 있다. 능동형 RFID 태그는 3개의 ID 정보를 유지할 수 있는데, 태그의 유일성을 보장하는 태그 ID(Tag ID), 태그의 소유자 정보를 담고 있는 소유자 ID(Owner ID) 그리고 태그 사용자가 임의의 값을 할당하는 사용자 ID (User ID)이다.

본 규격에서는 태그가 가지는 중요 정보에 대한 비인가 접근을 방지하기 위하여 패스워드 기반의 리더 인증을 수행하는 명령을 정의하고 있다. 그림 3의 우측이 리더이며, 명령어 중에 Security-Set password, Security-Set password protect 그리고 Security-Unlock이 그 명령어들이다. Security-Set password는 태그에 패스워드를 지정하는 명령이고, Security-Set password protect는 패스워드 지정 후에 패스워드 기반 리더 인증을 할 것인지 아닌지를 설정하는 명령이다. 즉, 패스워드를 지정했다 하더라도 그 기능을 활성화 시킬 수도 있고, 비활성화 시킬 수도 있다는 의미이다. 만일 Security-Set password protect 명령을 통해 그 기능이 활성화 되었다면 리더는 태그 정보의 수집을 위하여 반드시 Security-Unlock 명령을 먼저 수행하여 패스워드 보유를 증명하여야 한다. 태그는 패스워드 일치를 확인한 이후에 30초 동안은 리더의 모든 명령에 응답하며 30초가 지나면 다시 잠긴다. 그러나 브로드캐스트 명령에 대해서는 패스워드 설정 유무에 상관없이 모든 태그가 응답해야 한다. 즉 패스워드를 모르더라도 브로드캐스트 명령을 통해서 태그 ID, 사용자 ID 및 사용자 데이터 영역을 읽을 수 있기 때문에 결국 보호되는 영역은 소유자 ID 영역으로 한정되는 약점을 지닌다.

소유자 ID는 또 다른 형태의 인증 기능을 제공한다고 볼 수 있다. 즉, 태그의 소유자가 초기에 Privacy-Owner ID/Write 명령을 통해 태그에 소유자 ID를

설정하고, 그 태그는 소유자 ID를 포함한 명령에 대해서만 응답하는 정책을 편다면 소유자 ID를 모르는 불법 리더에게는 어떠한 명령에도 응답하지 않게 할 수 있다.

그러나 본 규격이 정의하고 있는 리더 인증 방식은 리더와 태그의 무선 구간에서 패스워드가 평문으로 전송되는 구조로 되어 있기 때문에 도청에 의한 패스워드 노출의 위험이 존재하며 또한 소유자 ID 필드가 리더의 명령에서 평문으로 전송되기 때문에 이 역시 도청에 의한 노출의 위험이 있다.

2.2 ISO 18185-4

ISO 18185-4 규격은 현재 표준화를 진행 중에 있으며, 2004년 8월에 작성된 WD(Working Draft) 문서를 살펴보면 세부적인 기술 규격은 전혀 없고 단지 보안 요소 정도만 나열하고 있다. E-Seal 서비스의 안전한 활용을 위해서 필요한 보안 요소로 접근 제어(Accessibility), 비밀성 보장(Confidentiality), 데이터 무결성 보장(Data integrity), 인증(Authentication), 저장 데이터의 부인 방지(Non-repudiation of stored data) 및 암호화 연산(Encryption) 등의 6가지 항목을 규정하고 있다.

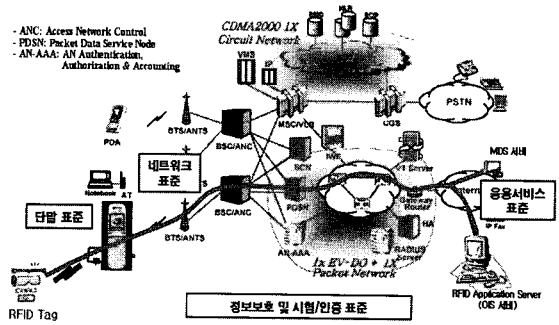
그리고 보안 수준(Levels of Security)을 세분화하여 기능적으로 지원할 수 있는 수준을 정의하려고 시도하고 있다. 다양한 활용 환경에 대해 해당 환경이 요구하는 수준의 보안 강도를 유지하면서 최소의 비용으로 능동형 RFID 시스템을 구성할 수 있는 기초 자료를 제공할 수 있을 것으로 판단된다.

Ⅲ. 모바일 RFID 보안 기술 및 표준화 동향

최근 IT 기술의 빠른 발전으로 휴대 단말은 다양한 정보서비스와 유비쿼터스 환경을 지원하기 위해 저전력·초경화된 복합·지능형 단말기기로 진화되고 있으며, 현재의 서비스에서 더욱 발전된 모습으로 변화될 것이다. 이동통신과 인터넷이 결합된 무선인터넷 인프라에 RFID 융합을 통해 사용자에게 새로운 서비스를 제공하는 모바일 RFID 기술이 출현하였고 이와 함께 개인정보보호나 인증, 권한부여, 키관리 등과 같은 모바일 RFID 정보보호 기술의 표준화와 기술 개발이 추진되고 있다.

3.1 모바일 RFID 서비스 개요

RFID 리더는 RFID 태그칩을 인식하는 무인 정보생산 단말로서 주로 활용되었으나, RFID 태그칩과 RFID 리더칩을 휴대폰에 장착하여 다양한 RFID 태그의 정보를 읽어 사용자에게 유용한 정보서비스를 제공하는 모바일 RFID 서비스로 확대되어가고 있다. 모바일 RFID 서비스란 모바일 단말기에 RFID 리더칩을 내장함으로써 이동 중에도 무선 인터넷 네트워크를 통해 물품의 정보를 검색, 구매, 인증, 결제 절차를 즉시에 처리하는 등 개인화된 안전한 서비스 제공하는 것을 말하며, 개념도는 그림 4와 같다.

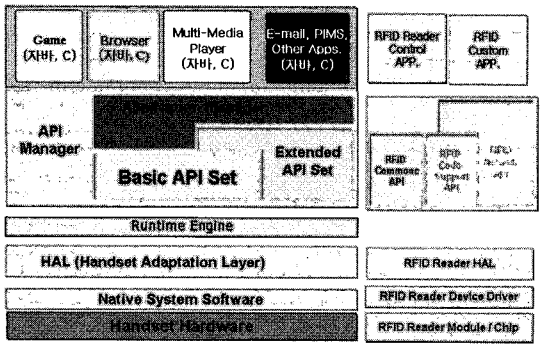


〔그림 4〕 모바일 RFID 서비스 개념도

3.2 WIPI 기반 모바일 RFID 단말 기술

휴대 전화에서 여러 종류의 RFID 리더와 어플리케이션 또는 미들웨어 사이에서 공통된 제어 인터페이스가 필요하며, 이는 RFID 리더가 공통적으로 지원해야 하는 기능에 대한 정의 및 다양한 공통된 명령어, 메시지 형태에 대한 표준화가 EPC Global Inc. 및 ISO 등에서 진행되고 있다. 모바일 RFID 기능을 지속적으로 확장하여 표준형 휴대폰 RFID 리더로 진화될 예정이며, 무선인터넷 표준 플랫폼인 WIPI를 이용한 RFID 지원 WIPI 확장 모델은 다양한 장치 간의 호환성을 유지하되 모바일 환경에 적합한 RFID 리더 사용을 가능하도록 리더 사용에 필요한 API를 무선인터넷 표준 플랫폼인 WIPI의 API 확장 요소로서 추가적인 기능을 정의하는 것이다.

모바일 RFID 기능 동작을 위한 WIPI 확장 API 내용을 살펴보면 그림 5와 같이 RFID 태그 목록 수집방식 / RFID 리더기 사용관련 기본 함수, RFID 태그 관련 기본 함수 / RFID 태그 목록 수집, 필터링 조건설정 / RFID 사용자 데이터 정보, 리더기 기본 정보 / 설정 등의 기능을 위한 모바일 장치에 RFID 리더기를 부착하기 위한 표준 API 기능과 리더의 초기화와 종료, 태그 데이터 입출력, 태그 및 리더 관리 기능을 하는 모바일 RFID 리더기의 동작과 제어를



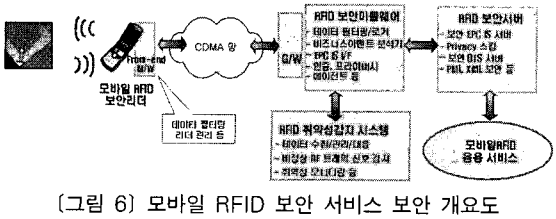
〔그림 5〕 WIPI 플랫폼상의 RFID S/W 기능 역할

위한 WIPI-HAL 확장 구현 API로 구성된다.

위피(WIPI)에서 HAL(Handset Adaptation Layer)은 플랫폼 이식에 있어서 하드웨어 독립성을 지원하기 위한 계층이다. 즉, 이는 플랫폼의 하드웨어 독립성을 유지하기 위한 추상화 계층으로 플랫폼의 상위 Layer 들은 HAL API를 호출하여 하드웨어 자원에 접근할 수 있다. 이를 통해 단말기의 네이티브 시스템에 대한 추상화가 이루어지고 하드웨어 독립적으로 플랫폼을 구성할 수 있다.

3.3 모바일 RFID 정보보호 기술

모바일 RFID 리더기의 이동성으로 인한 개인정보보호 침해 위협 증가 및 이동통신 및 무선인터넷 환경으로 인한 정보 노출의 위협이 예상되며 모바일 RFID 서비스의 불법적 이용 및 RFID 태그 정보의 위변조가 가능하므로, 개인정보 침해 및 누출의 위협을 최소화하기 위해 모바일 RFID 태그 및 단말기, 응용 서버간 안전한 서비스를 제공하기 위한 새로운 보안 기술이 요구된다. 따라서 RFID 태그의 극도로 제한된 계산 능력과 메모리 크기, 통신 대역폭, 가용 전력에 적합한 보안 프로토콜 및 암호 알고리즘의 저전력, 저면적의 최적화된 모바일 RFID 정보보호 기술에 대한 연구가 수행되고 있으며, 구조도는 그림 6과 같다.



〔그림 6〕 모바일 RFID 보안 서비스 보안 개요도

3.4 모바일 RFID 주요 기술 개발 동향

모바일 RFID기술은 기술의 시발점인 시작단계에 있으며 RFID 표준 기술들은 도입 기대 단계로서 관련 기술의 상용화 예상시기가 평균 4b~9년 이후로 예측되고 있다. 시장규모를 살펴보면 Venture Development Corp.가 최근 RFID 시장에 대한 중기 전망을 상향 조정하여 2005년도에는 S/W, H/W 및 서비스의 시장규모가 $2.13 billion에 이를 것이며, 매년 약 37%씩 성장할 것이고, 2005년까지는 서서히 성장하나 이후부터는 매우 급속히 커질 것으로 예상하고 있다. 현재 모바일 RFID 기술은 탈착형 RFID 리더칩이 개발된 해외사례는 일부 소개되었으나 아직 ISO/IEC, EPC 등의 국제표준화 활동은 진행되고 있지 않아 이 분야에서 세계를 선도할 수 있는 좋은 기회이다. 국내에서는 이동통신사, 제조업체 등을 중심으로 모바일 RFID 솔루션 개발을 준비중이며, 한국전자통신연구원은 금년말 휴대전화 내장형 리더칩 시제품을 개발하고, 내년부터 시범서비스 적용을 추진할 예정이다. 모바일 RFID 정보보호 기술은 금년도부터 한국전자통신연구원 정보보호연구단에서 RFID/USN 정보보호분야의 국제적인 기술 경쟁력 확보를 위해 기반기술 개발을 추진하고 있다.

3.5 모바일 RFID 표준화 동향

최근 노키아와 필립스, 소니 등 세계적인 전자통신 업체들이 최근 RFID 기술을 응용한 이종 시스템간 13.56㎒ 주파수를 이용하는 근거리 통신(NFC, Near Field Communication) 표준기술 개발을 위해 포럼을 결성하고 표준화를 진행하고 있으며, 국내에서는 한국정보통신기술협회의 RFID 기술표준화 그룹인 PG311과 연계하여 900㎒ 대역 RFID와 모바일 망 연동 기술 표준을 위한 모바일 RFID 포럼을 2005년 2월 3일 창립하였고, 5개의 분과 위원회 중 정보보호 분과에서 한국전자통신연구원, 한국정보보호진흥원, 이동통신사 등 관련 전문가들이 모바일 RFID 정보보호 및 프라이버시 보호 기술의 표준화 및 정보보호 서비스 이용환경 구축을 위한 법제도적 기반 마련을 위해 활동을 하고 있다. 현재 모바일 RFID 포럼에서 검토중인 모바일 RFID 관련 주요 표준화 추진 대상은 다음 표 1과 같다. 현재 모바일 RFID 정보보호기술은 국내외에서 관련 요소기술들이 개발되고 있으며, 앞으로 서비스 상용화를 위하여 사용자에게 편리함과 안전성 보장을 해주는 WIPI 플랫폼 기반 경량형 미들웨

〔표 1〕 모바일 RFID 표준화 추진현황

	표준화 내용	추진현황
단말분과	· RFID 리더칩 등 H/W 인터페이스 규격표준화 · 휴대폰과 리더칩간 통신 인터페이스 · RFID 리더칩 및 휴대폰 복합 단말기 기술 기준	· MRF 무선 규격 : 현재 고시된 RFID 기술 기준 범위 내에서 모바일 RFID 서비스에 필요한 세부 파라미터 정의 · MRF 리더 규격 : 리더 규격, 물리적, 전기적 인터페이스 규격, 동작 환경 등 정의 · MRF 리더 제어 WIPI API : 리더와 WIPI RFID 미들웨어간의 통신을 위한 명령어 정의, 메시지 규격 등 정의 · MRF WIPI RFID 미들웨어 규격 : 모바일 RFID 서비스를 위한 필요한 Event 처리 규격 등
네트워크 분과	· 네트워크 통신, 데이터 전송, 네트워크연동,미들웨어 등 의 규격 표준화	· 모바일 ODS 프로토콜 : Code resolution을 위한 mODS와의 통신 프로토콜 규격 · 다중 RFID 코드인식을 위한 모바일 단말기 규격 : ISO15963, EPC Code 등 다수의 RFID 코드 체계 규격을 지원하는 코드 인식 알고리즘 규격 · 모바일 RFID 서비스 구조 : 모바일 RFID 서비스를 위한 전체 표준 규격들의 상호 관련성 및 연동을 규명하는 구조적 프레임워크 · 모바일 RFID 네트워크 통신지원 WIPI API 확장규격: 모바일 RFID 서비스 모델의 네트워크 통신을 지원하기 위한 WIPI 확장 규격
응용서비스분과	· 응용서비스 요구사항 프로파일 표준화 · 컨텐츠 작성, 표현, 관리 등 규격 표준화	· 통신사업자(KT, SKT, KTF, LGT) 중심의 4개 서비스 개발 WG 및 공공 부문 서비스 개발 WG 구성 · 서비스 모델/시나리오 공모 진행 중 (~4/30) · 서비스 모델/시나리오& ARP(Application Requirement Profile) 지침
정보보호 분과	· 정보보안 관련된 규격 표준화 · 개인정보보호법 준수를 위한 RFID 기능 규격 표준화	· 모바일 RFID 서비스보안 요구사항 : 모바일 RFID 서비스 분류별 요구되는 보안 요구사항 정의 · 모바일 RFID 단말 보안 확장 : 단말의 WIPI 보안 확장 API 정의 · 모바일 RFID 프라이버시 보호 가이드라인 : 모바일 RFID 서비스 프라이버시 보호 지침
시험인증 분과	· H/W 및 S/W 등 각종 시험 대상 항목들의 시험, 인증규격 표준화	· 900MHz RF 적합성 시험 표준 · 모바일 RFID 단말기 표준 적합성 시험 표준 · 모바일 RFID 네트워크 프로토콜 표준 적합성 시험 표준 · 모바일 RFID 응용별 상호운용성 시험 표준

어 개발 및 해당 보안 기술들과 연동하는 방안이 과제로 남아 있다. 그리고, 프라이버시 보호를 위한 기술 개발 및 체계 수립 등의 지속적인 연구가 필요하다.

Ⅳ. RFID 개인 프라이버시 보호 기술

RFID 기술은 자동화된 태그 인식을 기반으로 다양한 산업 - 공급망 관리, 창고 관리, 항공 수하물 관리, 항만 컨테이너 관리 등 - 자동화에 사용되어질 수 있다. 그러나, 이러한 RFID 기술의 핵심인 자동 인식 및 물품 정보 열람 기능은 최종 사용자인 소비자 단계부터는 심각한 프라이버시 침해 요소가 된다. RFID 기술의 개인 프라이버시 침해는 다음과 같은 두 가지 유형으로 나타난다.

(1) RFID 태그 부착 물품을 들고 가거나, RFID 태그를 부착하고 있는 개인에 대한 추적이 가능하다.
(2) 개인이 소유하고 있는 태그부착 물품의 태그 ID를 읽은 후, 그 ID에 연결된 물품 정보를 네트워크로부터 열람하여 개인이 무엇을 소유하고 있는지를 알 수 있다.

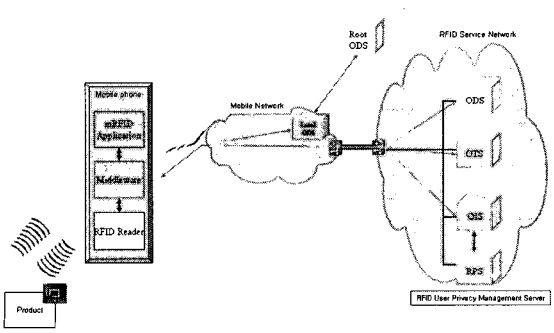
이러한 프라이버시 침해를 해결하기 위한 가장 확실한 방법은 RFID 태그를 물리적으로 제거하거나, RFID 태그 기능을 정지 - kill 명령을 사용한 기능 정지 - 시키는 것이다. 그러나, 많은 RFID 응용 서비스 - RFID를 이용한 AS 서비스/소고기 이력 추적 서비스/RFID 태그를 이용한 DVD 관리 등 - 에서는 개인이 RFID 태그 부착 물품을 소유한 이후에도 계속 서비스가 이루어져야 하기 때문에, RFID 태그 기능 정지만이 최상의 프라이버시 보호 방법은 아니다.[3] 태그 기능 정지 외에 프라이버시 보호를 위해 현재까지 제시된 해결방법은 다음과 같다.

- Hash Lock 방법[1] : hash lock 방법은 RFID 리더가 태그에게 ID를 요청하면 태그는 자신의 비밀키를 해쉬한 값(메타ID)를 가지고 응답하고, 리더가 백엔드 서버로부터 메타ID에 대한 키값을 받아온 후, 이를 태그에게 제시하고, 이 키가 자신의 비밀키와 일치하는지를 확인한 후, 태그가 자신의 진짜 ID를 제시하는 방법이다. 그러나, hash lock 방법에서 태그는 늘 동일한 메타ID를 전송하기 때문에, 개인을 추적할 수 있는 위치기반 프라이버시는 보호될 수 없다.
- Randomized Hash Lock 방법[1,2] : 본 방법은 hash lock 방법에서의 약점을 보완하기 위해 태그가 랜덤값 생성기를 이용하여 매번 틀린 메타ID를 제시하는 방법이다. 그러나, 본 방법을 위해서는 백엔드 서버는 많은 추가적인 계산을 수행해야 하며, 태그에는 랜덤값 생성기가 구현되어야 한다.
- Blocker Tag 방법[3] : blocker tag 방법은 binary tree-walking anticollision protocol에 기반하여 구성된 방법이다. binary tree-walking 방식의 태그 선택 알고리즘은 리더가 태그 ID의 첫번째 비트를 물어보고, 충돌이 없으면 다음 두 번째 비트를 질의하게 된다. 충돌이 생기면, 리더를 두 번째 비트가 1(또는 0)인 태그한테 응답할 것을 질의한다. 이러한 과정을 ID의 마지막 비트까지 진행하여 태그를 인식하게 된다. 이때, blocker tag는 자신이 보호하려는 영역의 비트 이후부터 모든 질의(1인 경우나 0인

경우)에 대해 계속 응답을 함으로써 충돌이 계속적으로 생기게 하여 어떤 한 영역에 대해서는 태그를 인식하지 못하도록 하는 방법이다. 그러나, blocker tag 방식을 이용하여 프라이버시 보호를 하기 위해서는 개인은 추가로 blocker tag를 물리적으로 가지고 다녀야 한다.

- Re-encryption 방법[4] : re-encryption 방법은 공개키 암호화 방식을 이용하는 방법으로, 무거운 공개키 방식 암호화 기법이 리더측에서 수행되어 태그에 저장되어야 한다. 그러나, 현재 제안된 re-encryption 방법은 화폐에 적용되며 화폐 내의 광학적인 데이터를 필수적으로 사용하여야 한다.

상기의 프라이버시 보호를 위한 방법들은 모두 태그와 리더 사이를 안전하게 함으로써 개인 프라이버시를 보호는 방법이다. 물론, 개인 추적성에 의한 프라이버시 침해를 막기 위해서는 태그 리더 사이에서의 해결책이 필수적으로 제공되어야 하지만, 태그의 ID에 결합되어 있는 네트워크 상의 정보 열람을 통한 프라이버시 침해 또한 고려되어야 한다. 네트워크 상에 유통되는 태그 ID에 결합된 정보의 무제한적인 유통을 막기 위해서는 태그 ID에 결합된 정보 열람을 제한하거나 보호하여야 한다. 현재, 개인 이동 단말에 RFID 리더 디바이스를 장착하는 모바일 RFID 기술이 개발 중이며[5,6], 이러한 환경에서 태그 ID에 결합된 네트워크 상의 정보를 보호하고 제한하는 방법을 사용한 개인 프라이버시 보호 방안에 대한 연구가 진행 중이며, 모바일 RFID 서비스를 위한 네트워크에 RPS(RFID user Privacy management Service) 시스템을 도입하여 개인 프라이버시 보호하려는 연구가 진행중이다(그림 7 참조). RPS의 기본적인 기능은 다음과 같다.



〔그림 7〕 RPS를 포함한 모바일 RFID 서비스 아키텍쳐

- 사용자별 프라이버시 보호 프로파일 생성 기능
- 사용자별 프라이버시 보호 프로파일 관린 기능
- 모바일 RFID 응용 서버의 요청에 따른 해당 프라이버시 보호 정책 전달 기능

RPS의 상기와 같은 기능을 이용한 대략적인 개인 프라이버시 보호 과정은 다음과 같다.

(1) 모바일 RFID 리더는 태그 ID를 읽어 태그 ID를 ODS(Object Directory Service) 리졸브 과정을 통해 태그 ID에 결합된 물품정보와 같은 다양한 정보의 네트워크 주소를 얻는다.
(2) 응용 서버에게 태그 ID 연결 물품 정보를 요청한다.
(3) 응용 서버는 물품 정보에 대한 개인 프라이버시 보호 정책을 RPS를 통해 전달받는다.
(4) 개인이 설정한 프라이버시 보호 정책에 알맞게 물품 정보가 보호되어 리더 측에 전달된다.

상기 과정을 통해 개인의 프라이버시 보호 정책이 반영된 태그 ID 연결 정보가 네트워크에 유통될 수 있어, 개인 프라이버시 침해 문제를 RFID 네트워크 인프라 측면에서 해결할 수 있을 것으로 기대된다.

V. 결 론

RFID 기술은 모든 사물에 RFID 태그를 부착하고, 자동으로 주변 환경 정보를 센싱 및 서로간 네트워크로 연결됨으로서, 지능형 유비쿼터스 환경으로 진화 될 것이다. 본 고에서는 최근 활발히 표준화 및 기술개발이 되고 있는 RFID 분야에서 능동형 RFID 보안기술과 수동형인 모바일 RFID 보안기술에 대하여 살펴보았다. 특히 RFID 기술은 악의적인 공격을 통하여 위변조, 위장, 도청, 위치추적 및 다양한 형태의 사생활 침해가 우려되므로 기술적인 보안 대책이 요구되는 기술이다. 따라서 개인의 프라이버시 침해에 민감한 소비자 보호 단체 모두가 만족할 수 있는 법과 제도의 제정과 더불어 이를 안심하고 모든 물품에 적용될 수 있는 보안 기술이 개발·적용되어야 할 것이다.

참 고 문 헌

〔1〕 ISO/IEC 18000-7, *"Information technology - Radio frequency identification for item management - Part 7: Parameters*

for active air interface communications at 433 MHz", ISO/IEC International Standard, 2004.8.15
[2] ISO 18185-7, "*Freight containers - Electronic seals - Part 7: Physical Layer*", ISO Working Draft, 2005.4.28.
[3] ISO 18185-4, "*Freight containers - Identification and Communication, Electronic seals - Part 4: Data Protection*", ISO Working Draft, 2004.8.20.
[4] S. A. Weis, S. E. Sarma, R. L. Rivest, D. W. Engels, "*Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems,*" First International Conference on Security in Pervasive Computing(SPC), 2003.
[5] D. Henrici, P. Muller, "*Tackling Security and Privacy Issues in Radio Frequency Identification Devices,*" PERVASIVE 2004. LNCS 3001, pp. 219-224, 2004.
[6] A. Juels, R. L. Rivest, M. Szydlo, "*The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy,*" CCS'03, October 2003.
[7] A. Juels, R. Pappu, "*Squealing euros: Privacy protection in RFID-enabled banknotes,*" Proceedings of Financial Cryptography FC'03, 2003.
[8] 모바일 RFID 포럼, http://www.mrf.or.kr
[9] 노키아, "Nokia Mobile RFID Kit," http://www.nokia.com

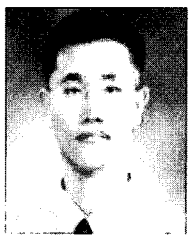
〈著 者 紹 介〉

이 병 길 (Lee Byung Gil)

1991년 2월 : 경북대학교 전자공학과 졸업
1993년 2월 : 경북대학교 전자공학과 석사
2003년 2월 : 경북대학교 전자공학과 박사(공학박사)
1993년 1월~2001년 7월 : 데이콤종합연구소 선임연구원
2001년 7월~현재 : 한국전자통신연구원 선임연구원
〈관심분야〉 무선통신보안, RFID/USN 정보보호

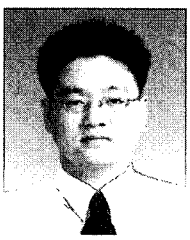
강 유 성 (Kang You Sung)

1997년 2월 : 전남대학교 전자공학과 졸업
1999년 8월 : 전남대학교 전자공학과 석사
2005년 3월~현재 : 한국과학기술원 전기 및 전자공학 박사과정
1999년 11월~현재: 한국전자통신연구원 선임연구원
〈관심분야〉 무선랜보안, RFID/USN 정보보호



박 남 제 (Park Nam Je)

2000년 8월 : 동국대학교 정보산업학과 졸업
2003년 8월 : 성균관대학교 정보통신대학원 정보보호학과 석사
2003년 4월~현재 : 한국전자통신연구원 연구원
〈관심분야〉 XML보안, RFID/USN 정보보호



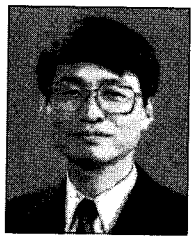
최 두 호 (Choi, Doo Ho)

1994년 2월 : 성균관대학교 수학과 졸업
1996년 2월 : 한국과학기술원 수학과 석사
2002년 2월 : 한국과학기술원 수

학과 박사
2002년 1월~현재 : 한국전자통신연구원 선임연구원
〈관심분야〉 무선 보안, 암호프로토콜 설계, RFID 보안

김 호 원 (Kim Ho Won)

1993년 2월 : 경북대학교 전자공학과 졸업
1995년 2월 : 포항공과대학교 전자전기공학과 석사
1999년 2월 : 포항공과대학교 전자전기공학과 (공학박사)
1998년 12월~2003년 6월 : 한국전자통신연구원 선임연구원
2003년 7월~2004년 6월 : Ruhr University Bochum Post Doc. (Germany)
2004년 7월~현재: 한국전자통신연구원 선임연구원/팀장
〈관심분야〉 암호학, RFID/USN 정보보호, 암호칩 설계



정 교 일 (Chung Kyo IL)

1981년 2월 : 한양대학교 전자공학과 졸업
1983년 8월 : 한양대학교 전자공학과 석사
1997년 8월 : 한양대학교 전자공학과(공학박사)
1980년 12월~1981년 11월 : 엠시스템즈 사원
1981년 12월~1982년 2월 : 한국전기통신연구소 위촉연구원
1982년 2월~현재 : 한국전자통신연구원 정보보호연구단 정보보호기반그룹/그룹장
〈관심분야〉 RFID/USN정보보호, IC카드보안, 생체인식, 정보전