안전한 모바일 RFID 리더를 위한 개방형 임베디드 소프트웨어 플랫폼 구현 방안

정회원 박 남 제*

The Implementation of Open Embedded S/W Platform for Secure Mobile RFID Reader

Namje Park* *Regular Member*

요 약

모바일 RFID 환경의 태그 및 모바일 리더에서는 높은 제약성 때문에 기존의 암호기술 및 프로토콜 기술의 적용이 불가하다. 모바일 RFID 환경에 맞는 정보보호기술 및 프라이버시 보호기술을 개발하기 위해서는 RFID 각 구성 요소별 특성과 각 요소의 전체 연동 관점에서 정보보호기술 및 프라이버시 보호기술을 개발해야 한다. 본 논문에서 제안된 모바일 RFID 단말 보안 S/W 플랫폼 시스템은 모바일 RFID 정보의 보호를 위한 보안 라이브러리를 이식 및 확장하여 RFID 리더부터 응용 서버까지 모든 데이터의 이동 경로에 보안을 적용하도록 지원한다.

Key Words : Mobile RFID, Terminal Platform, WIPI, Privacy, Security

ABSTRACT

The current excessive limitations to mobile RFID tags and readers make it impossible to apply present codes and protocols. The technology for information and privacy protection should be developed in terms of general interconnection among elements and their characteristics of mobile RFID in order to such technology that meets the RFID circumstances. In this paper, transplanting and extending security library for protecting mobile RFID information in secure mobile RFID terminal S/W platform system to support security application on the path of all data from RFID reader to application server.

Ⅰ. 서 론

최근 IT(Information Technology) 기술의 빠른 발전으로 휴대 단말은 다양한 정보서비스와 유비쿼터스 환경을 지원하기 위해 저전력·초경량화된 복합·지능형 단말기기로 진화되고 있으며, 현재의 서비스에서 더욱 발전된 모습으로 변화될 것이다. 이러한 모바일 단말기에 UHF(Ultrahigh Frequency) 대역의 RFID (Radio Frequency Identification) 리더를 장착해 RFID 태그를 인식할 수 있게 되면, 이는 우리 주위에 있는 물리적인 환경에 대한 인식능력을 갖게 됨을 의미한다. 또한, 이미 우리 생활의 일부가 된 모바일 단말기에 RFID 리더 기능을 추가함으로써 기존의 RFID 서비스를 유통, 물류 서비스와 같은 기업이 기업을 대상으로 각종 서비스나 물품을 판매하는 방식의 전자거래 형태인 B2B(Business to Busine ss) 모델에서 개인의 서비스와 관련 깊은 B2C(Busin ess-to-Consumer) 모델로 확대할 수 있게 된다. 기업 대 소비자간 전자상거래 형태인 B2C 모델은 국민들에게 더욱 다양한 서비스를 제공할 수 있음을 의미하며, 소규모 투자로

※ 본 연구는 2008년 정부(교육과학기술부)의 재원으로 한국학술진흥재단의 지원을 받아 수행된 연구임[KRF-2008-357-D00255].
* Arizona State University, Computer Science and Engineering (namjepark@asu.edu, namjepark@gmail.com)
논문번호 : KICS2009-11-538, 접수일자 : 2009년 11월 1일, 최종논문접수일자 : 2010년 4월 14일

부가가치가 높은 서비스가 가능하기 때문에 모바일 RFID 기술은 대형 업체들뿐만 아니라 소형 업체들에게도 많은 기회를 제공할 수 있을 것으로 보인다[3,5,10]. 하지만, RFID 태그가 모든 사물에 부착되어 보편화될 경우, 개인정보 침해 및 유출에 따른 보안 문제가 중요한 사회적 이슈로 대두될 것이 확실시된다. 모바일 RFID 보안 취약성은 사용자 프라이버시 침해와 기존의 가상공간 공격이 물리적인 공간으로 확대되어 가고 있다.

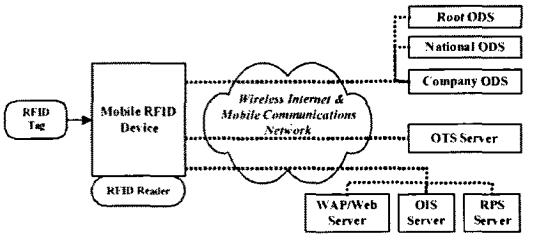
본 논문에서는 모바일 RFID와 보안 취약성을 분석하여 안전한 모바일 RFID 네트워크 서비스를 제공하기 위한 정보보호 구현방안과 개방형 단말 보안 플랫폼을 제안하고 분석하고자 한다. 본 논문의 구성은 II장에서 모바일 RFID 기술 및 보안취약성, 정보보호 구현 방안, III장에서 모바일 RFID 단말 보안 플랫폼의 구성 및 세부기능, IV장에서 제안된 단말 플랫폼의 구현 분석, V장에서 결론을 기술하였다.

II. 모바일 RFID와 보안 구현 방안

2.1 모바일 RFID 개요 및 보안 취약성

900MHz 주파수 대역의 모바일 RFID 서비스는 핸드폰에 RFID 리더(칩)을 내장함으로써 이동 중에도 무선 인터넷 네트워크를 통해 물품의 정보를 검색, 구매, 인증, 결제 절차를 즉시에 처리하는 등 개인화된 안전한 서비스를 제공하는 것으로 RFID 리더(칩), 휴대폰 단말, 통신망 구성 및 프로토콜, 정보보호, 응용서버, RFID 코드 해석, 콘텐츠 구축 등 서비스 인프라로 구성된다[3,5,10].

모바일 RFID의 구성 네트워크를 보면 크게 사물의 식별 정보를 가지고 있는 태그와 리더기가 장착된 휴대전화, 식별 코드와 관련 정보의 서버위치(URL: Uniform Resource Location)를 알려주는 ODS (Object Directory Service, 객체검색서비스), 태그의 실제 정보를 가지고 있는 OIS(Object Information Service, 객체정보서비스)로 구성된다[1]. 특정 제품에 설치 된 태그 정보를 읽은 후 리더기가 식별된 코드를 해당 ODS로부터 OIS 서버의 주소를 받아 콘텐츠를 제공하는 형태로 모바일 RFID 리더와 ODS, 콘텐츠 서버간의 통신은 이통망을 통해 이루어진다.



* OTS(Object Traceability Service), ODS(Object Directory Service)
OIS(Object Info. Service), RPS(RFID user Privacy Mng. Server)

그림 1. 모바일 RFID 네트워크 기본 구조

새로운 모바일 RFID 서비스 환경에서 해를 가할 수 있는 방법은 여러 가지가 가능하며, 이는 더 이상 이론적으로만 가능한 것이 아니라 현실적인 문제이다. RFID 태그 및 리더에 대한 수동적인 신호 차단 공격, 권한이 없는 리더에 의한 RFID 태그 읽기, 왜곡된 태그 혹은 리더 인증, RFID 태그에 대한 공격 툴 사용, RFID 태그에 대한 무력화 공격, 암호학적인 해킹 기법을 동원한 정교한 RFID 태그 공격 등의 RFID 보안 취약성이 있으며, 모바일 RFID 환경에서도 유사한 보안 취약성과 프라이버시 침해 가능성이 존재하므로, 이에 대한 적절한 정보보호 기술이 필요로 하다[9,12]. 그리고, 현실적으로 기존의 RFID 규격 및 모바일 RFID 표준을 준수하며, 태그에서 암호 알고리즘을 사용하지 않는 상황에서 사업자 및 사업자에게 보안 기능 및 프라이버시 보호 / 관리 기능을 제공하는 새로운 정보보호 방안이 필요하다.

2.2 모바일 RFID 보안 구현에 대한 접근 방안

안전한 모바일 RFID 서비스 환경을 만들기 위해서 산학연 등에서 여러 가지 연구가 진행되고 있다. 정보보호 환경이 이뤄지기 위해서는 도메인 사이의 보안, 개인 프라이버시 보호, 인증, 단대단 보안, 위치 추적 방지 등과 같은 다양한 보안 이슈들을 해결할 수 있는 복합적인 보안 프레임워크를 필요로 한다[3,6,7]. 본 논문에서는 안전한 모바일 RFID 서비스 제공하기 위해 그림 2와 같이 다단계적인 모바일 RFID 보안기술 개발 전략을 수립하여 모바일 RFID 정보보호 서비스 방안을 구현해야 함을 제안한다. 구체적으로는 모바일 RFID 단말 플랫폼에서 대표적인 6가지의 표준 보안 기능을 개발하고, 이를 기반으로 주요 3가지의 보안 서비스 메커니즘을 적용하여, 응용 포털 서비스를 통해 안전한 모바일 RFID 응용 서비스를 실현함을 의미

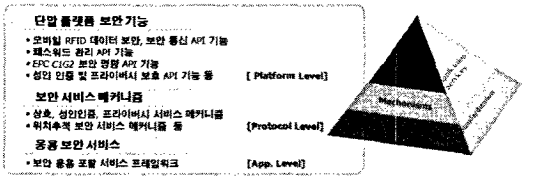


그림 2. 모바일 RFID 정보보호 구현 접근 방안

한다.

위의 통합형 모바일 RFID 보안 접근 방안에 근거하여 여러 가지의 보안 취약점을 해결하는 통합형 정보보호서비스 프레임워크 모델 구조를 살펴보면 그림 3과 같다[3,8].

모바일 RFID 통합 보안 프레임워크 기술의 주요 요소로는 응용 보안 수행을 위한 단말 플랫폼 암호 처리용 모바일 RFID 암호 라이브러리기술, 사용자가 이동통신망에서 UHF 대역의 리더기가 장착된 단말기를 사용하여 안전하게 응용서비스를 이용하도록 지원하는 무선인터넷 표준플랫폼(WIPI, Wireless Internet Platform for Interoperability) 확장 단말 보안 플랫폼 기술, 유무선 통합 환경의 RFID 응용 서비스 구축을 위해 다양한 보안 서비스를 손쉽게 구축할 수 있는 보안 응용 게이트웨이 기술, 동적 프로파일 기반의 맞춤형 RFID 개인 프라이버시 보호기술 등이 있다. 그림 3의 세부 지원 보안기능을 살펴보면 다음과 같다. 제안된 모바일 RFID 정보보호 서비스의 주요 기능은 RFID 태그부문에서 태그 인증 및 태그 불추적성, 태그와 리더 구간에서 리더 인증, 단말 플랫폼에서 WIPI 기반의 RFID 보안 플랫폼, 단말 플랫폼과 네트워크 시스템 구간 사이의 정보 메시지 종단간 보안, 응용서비스를 위한 성인인증, 위치추적 방지, 프로파일 기반의 동적 프라이버시 보호 등이다. 각 서비스 구간별 개별적인 보안기능들이 통합 프레임워크 형태로 제공되어져 서비스 연동을 통하여 모바일 RFID 서비스 이용자가 안전하게 정보를 제공할 수 있게 되어진다. 본 논문에서는 위에서 제안하는 통합 프레임워크 기술들 중 단말 보안 플랫폼을 중심으로 모바일 RFID 정보보호를 위해 제공될 수 있는 여러 방안들을 세밀히 분석한다.

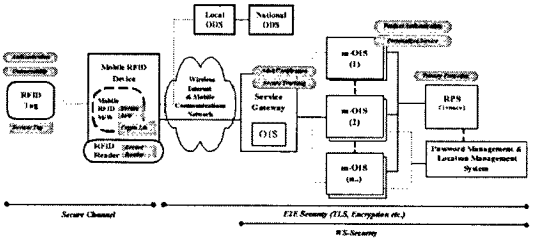


그림 3. 모바일 RFID 통합 보안 프레임워크 모델

Ⅲ. 모바일 RFID 단말 보안 플랫폼 설계 및 구현

3.1 단말 보안 S/W 플랫폼 구성

WIPI 확장된 모바일 RFID 단말 보안 S/W 플랫폼은 RFID 리더(칩)를 핸드폰에 연동하여 RFID 리더를 제어하고 리더를 통해서 인지된 태그에 대한 다양한 연산 기능 및 필터링 기능, ODS 질의 관련 처리 기능 등을 모바일 RFID 응용 시스템에게 안전하게 제공함으로써, 사용자가 원하는 객체에 대한 정보를 이동통신망을 통해서 획득할 수 있게 하는 시스템을 뜻한다.

이 플랫폼은 휴대폰 내장 RFID 리더칩에 대한 인식 거리, 송신 전력, 주파수, 간섭, PIN 규격, UART (Universal Asynchronous Receiver/Transmitter) 통신 인터페이스 등에 대한 내용과 리더(칩)를 제어하기 위해 WIPI 무선인터넷 표준 플랫폼의 확장 규격으로 구성된다. 이중 UHF 대역 RFID 리더 H/W 칩은 UART를 이용한 시리얼 통신으로 모바일 RFID 디바이스 드라이버를 통해 인터페이스되며, 이는 WIPI HAL (Handset Adaptation Layer)을 통해 WIPI API (Application Program Interface)에 의해 연결된다.

모바일 RFID 단말 보안 플랫폼 시스템은 RFID WIPI API 서브시스템과 RFID HAL API 서브시스템으로 구성되며, 모바일 RFID용 경량형 암호 라이브러리를 이용해 각종 보안 기능을 제공한다. RFID WIPI API 서브시스템은 RFID를 위해서 확장된 WIPI API와 확장된 WIPI 실행엔진 부분을 포함하며, RFID HAL API 서브시스템은 RFID를 위해서 확장된 HAL API를 포함한다. 그림 5는 WIPI 플랫폼에서의 모바일 RFID 확장 부분과 주요 모바일 RFID 확장 API의 기능 구조를 나타내고 있으며, 이러한 WIPI 플랫폼을 확장한 모바일 RFID 단말 보안 플랫폼 시스템의 세부 기능을 나타내고 있다[1,2,3].

주요 보안 기능은 RFID 태그 데이터 및 응용정보의 데이터 보안을 지원하는 응용 데이터 보안, 모바일 RFID 단말에서 서비스 네트워크 서버와의 통신시 안전한 보안통신을 지원하는 통신 보안, RFID 태그에서의 보안 패스워드 키 설정과 보안서버에서 지원하는 보안키 설정 및 관리에 대한 단말 보안키 관리[4], 모바

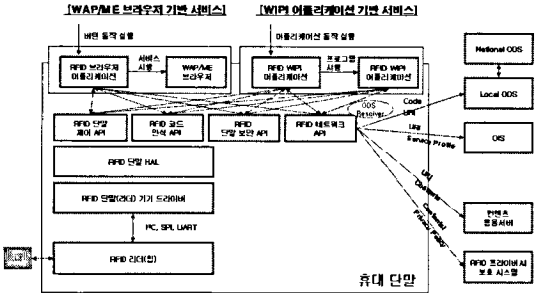


그림 4. 단말 보안 S/W 플랫폼의 참조 모델

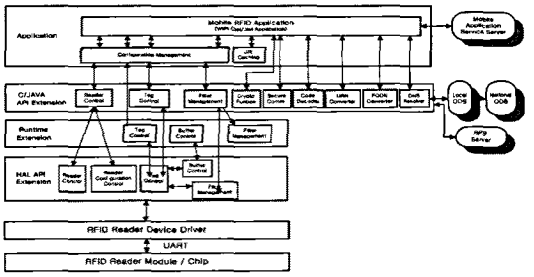


그림 5. 단말 보안 S/W 플랫폼의 세부 기능도

일 RFID 서비스에서 성인 서비스에 대한 성인 인증, 모바일 RFID 서비스 네트워크 환경에서 개인 프라이버시 보호를 위한 단말 프라이버시 에이전트 기능 등으로 구성된다.

3.2 단말 보안 S/W 플랫폼 세부 기능 설계

3.2.1 리더 및 태그 제어 기능

WIPI 기본 및 HAL 계층에서 RFID 리더를 제어하고, ISO 18000-6 Type A, B, C의 표준을 따르는 RFID 태그를 조작하기 위한 기능을 지원한다. 그리고, WIPI 확장 API 계층에서 RFID 리더기 제어 및 RFID 태그 정보 수집 기능이 지원하고 리더기 관련 설정 정보를 제공할 수 있다. 본 기능은 RFID 리더(칩)를 통해 인지된 태그에 대해서 다양한 연산 기능을 제공하는 것으로 태그 ID 쓰기/읽기, 사용자 데이터의 쓰기/읽기, 태그의 특정필드(ID, 접근 및 무효화 패스워드, User Data 등) 혹은 모든 필드에 대한 Lock/Unlock, 특정 태그에 대한 무효화 기능 등이 있다. 이러한 기능들은 하부 HAL API 확장에서 단말기 기본 S/W 및 H/W에 의해서 구현 가능하도록 맵핑되어 구현된다. 그리고, WIPI API 확장 및 HAL API 확장은 필요한 이벤트를 수신하고, 처리하기 위해서 WIPI 실행 엔진과 연동하여 구현한다.

3.2.2 태그 데이터 관리 및 보안 필터링 기능

응용 프로그램의 효과적인 서비스를 지원하기 위해서 중복 제거, 응용이 원치 않는 정보 삭제 등의 필터링 규칙을 정의하고, 필터링을 처리하는 모듈에 해당 규칙을 전달해야한다. 그리고, 보안 필터링 규칙을 정의하고, 정의된 필터링 규칙은 WIPI 실행 엔진 에서 처리되도록 지원한다.

모바일 RFID 리더는 태그의 정보를 읽고 버퍼에 저장하는 과정에서 필터링을 하여 저장하도록 필터를 추가한다. 필터는 태그의 정보에 대해 mask에 set된 비트에 대하여, value 값과 AND 연산을 한 결과가 value 값과 동일한 지 확인하여, 그 결과가 true이면 inclusive 값에 따라 태그의 정보를 저장하도록 한다. 추가된 필터는 기본적으로 enable 상태이다. 모바일 RFID 리더가 태그를 읽었을 때의 필터링 및 버퍼링의 진행과정을 살펴보면 그림 6과 같다.

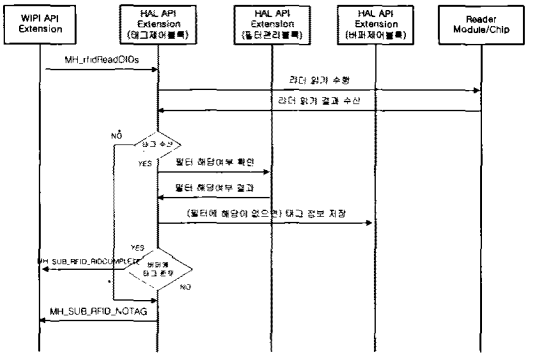


그림 6. 리더 API의 필터링, 버퍼링 상태 흐름도

3.2.3 단말 데이터 및 통신 보안 기능

RFID 태그나 모바일 RFID 서비스 네트워크상의 서버와 통신시 필요한 데이터 및 통신 보호를 위한 데이터 및 통신 보안 기능을 제공한다. 응용 프로그램에서 보안 기능이 필요할 때마다 해당 암호 알고리즘 API를 이용하여 보안 기능을 지원하는 것으로 응용에서 처리된 데이터의 정보들을 설정된 규칙에 따라 모바일 RFID 서비스 네트워크를 이용하여 응용 서버에게 안전하게 정보들을 전송한다. 주요 지원 기능은 경량형 무선 암호 연산 컴포넌트, 대칭키/공개키, 메시지 다이제스트 및 서명, 고성능 타원곡선 고속 연산 및 암호, 국산 KCDSA(Korean Certificate -based Digital Signature Algorithm) 전자서명, SEED 대칭암호, ARIA, AES(Advanced Encryption Standard) 표준형 경량 알고리즘, 표준 보안통신 프로토콜 (SSL/TLS), ASN.1 및 PKCS #5/8, 이동통신 3사별 표준 인터페이스 컴포넌트 등이 있다. 보안통신 프로토콜은 국제 표준을 준수하여 SSL(secure sockets layer) 버전 3.0 및 TLS(Transport Layer Security) 버전 1.0(3.1)을 지원하며 통신 메시지들을 안전하게 응용 서버 등의 네트워크 서버 시스템에게 전송한다. 보안 라이브러리에 대한 전체 WIPI 플랫폼의 개념적 계층 구조에서의 위치와 모듈 운용 구조는 그림 7과 같다.

모바일 RFID용 경량형 보안 라이브러리는 WIPI 기반 플랫폼에서 응용 프로그램을 위해 설계된 것으로서 응용 프로그램의 관점에서 보았을 때에는 기본 계층 API 와 같은 위치의 기능을 갖게 된다. 그러나

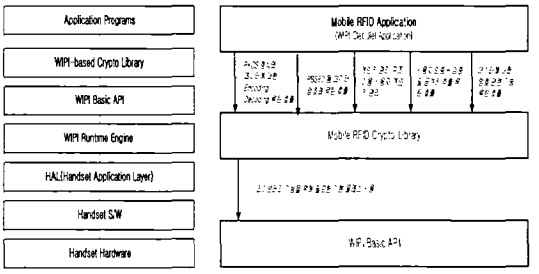


그림 7. WIPI 개념적 계층에서의 보안 지원 방안

플랫폼의 관점에서 보았을 경우, 본 보안 라이브러리는 플랫폼의 기본 API를 이용하여 설계 개발된 것으로 볼 수 있으므로 응용 프로그램 계층의 라이브러리라 생각할 수 있다. 개발된 라이브러리는 응용에서 사용할 수 있는 기본 타입의 변수를 이용하여 차례로 라이브러리 구현을 위한 기본적인 클래스만을 사용하였으므로 WIPI 뿐만 아니라 J2ME(Java 2 Micro Edition)등 유사한 플랫폼에서도 최소한의 변형을 통해서 같은 기능을 수행할 수 있는 장점이 있다.

3.2.4 단말 보안키 설정 및 관리 기능

태그 데이터의 종단간 보안을 위한 단말 보안키(패스워드) 설정 및 관리 기능을 제공한다[9,20]. 태그의 접근 통제나 기능 정지를 위한 패스워드 전송 시 원타임 패스워드 방식 등의 패스워드 메커니즘 등의 안전한 기능 방법을 지원한다. 태그제어 및 리더제어 중 쓰기/잠그기/무효화(Kill) 등 보안이 요구되는 민감한 명령을 수행할 경우 패스워드를 통한 접근 인가 기능을 지원하는 것으로, 태그의 기능을 정지하거나, 태그에 접근 제어를 위해서 패스워드를 사용해야 하는 모바일 RFID 응용 서비스의 경우, 이러한 보안키를 안전하게 관리하고, 리더 단말에게 안전하게 패스워드를 위임할 수 있어야 하며, 이러한 기능이 모바일 RFID 응용 서비스 인프라에서 제공된다.

태그 패스워드 관리 API는 태그 패스워드를 저장할 때, 단말기에 설정된 비밀번호를 태그 패스워드와 함께 함수 파라미터로 입력 받는다. 이후, 태그 기능 정지 혹은 태그 접근 제어 명령을 위해서 태그 패스워드를 질의할 때, 올바른 비밀번호를 지정할 때만 태그 패스워드 관리 API는 정상적으로 태그 패스워드를 출력한다. 이러한 태그 패스워드는 단말 리소스로 관리되는 것으로 정의하며, 본 리소스는 WIPI HAL에서 제공하는 단말 리소스 보안 API를 사용하여 단말기에 설정된 비밀번호로 본 리소스에 대해 잠금 설정하여 안전하게 관리되어야 한다.

3.2.5 단말 성인 인증 기능

모바일 RFID 서비스 중 성인 등급 표시가 필요한 서비스의 경우, 태그의 사용자 데이터 영역에는 성인 등급 표시가 포함되어, 성인물 등급에 따라 사용자의 서비스 접근을 제어하기 위한 성인 인증 처리 기능이 지원된다. 모바일 RFID 태그 정보 기반의 성인등급 인증 절차를 살펴보면 그림 8과 같다. 그림 8에서 모바일 RFID 응용 프로그램은 성인인증 API 를 이용해서 태그의 사용자 데이터 영역의 성인등급을 요청한다. 성인인증 API 는 다시 태그제어 API 를 이용해서 태그의 사용자 데이터를 요청하고, 태그제어 API는 엔진에 콜백 함수를 등록한다. 그리고, 태그제어 API 는 HAL API 를 이용해서 사용자 데이터를 요청한다. HAL API는 태그에서 사용자 데이터를 읽어서 이벤트를 엔진에 전달하고, 엔진은 버퍼안의 데이터 유효성을 검사한 후 버퍼안의 사용자데이터를 읽고, 등록된 해당 콜백 함수를 호출 해 준다. 이후 가져온 사용자데이터 안의 성인등급이 현재 단말기에 저장된 성인정보(예, 생년월일)에 부합되는 지 검사한다. 이 과정에서 성인인증이 되면 코드 변환 요청을 하게 되어 해당 응용 정보를 단말기로 수신하게 된다.

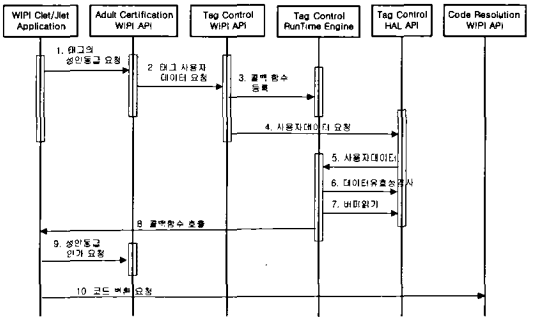


그림 8. RFID 태그 성인등급 인증 절차

3.2.6 단말 프라이버시 에이전트 기능

안전한 개인 프라이버시 보호를 위해 RFID 프라이버시 보호 시스템과 송수신할 수 있는 안전한 프로토콜을 지원하는 단말 프라이버시 에이전트 기능을 지원한다. 모바일 RFID 서비스 프라이버시 영향 평가 시 부여받은 기본 프라이버시 등급 정보를 태그의 사용자 데이터 영역에 저장하고, 해당 기능을 지원한다. 모바일 RFID 태그 접근 인증을 통한 위치 프라이버시 보호 기능은 RFID 태그 잠금 패스워드 설정 및 RFID 태그 잠금 기능을 이용하여 동작되는데, 주요 RFID 태그정보 프라이버시 보호 기능 흐름은 다음 그림 9와 같다.

모바일 RFID 응용 프로그램은 WIPI API 를 이용해서 태그의 사용자 데이터 영역의 프라이버시 레벨을 요청한다. 단말 플랫폼의 프라이버시 API 는 다시 태그제어 API 를 이용해서 태그의 사용자 데이터를 요청한다. 태그제어 API는 엔진에 콜백 함수를 등록하고, HAL API 를 이용해서 사용자 데이터를 요청한다. HAL API는 태그에서 사용자 데이터를 읽어서 이벤트를 엔진에 전달하고, 엔진은 버퍼안의 데이터 유효성을 검사한 이후 버퍼안의 사용자데이터를 읽어오고, 등록된 해당 콜백 함수를 호출 해 준다. 그리고, RFID 코드 변환 요청을 한다. 이후 단말 플랫폼에서 응용서버에 접근 시 프라이버시 레벨을 제시한다. 응용서버는 단말에게 프라이버시 정책을 내려주고, 단말 플랫폼은 GUI(Graphical User Interface)를 통해서 사용자가 프라이버시 레벨을 설정할 수 있도록 한다. 마지막으로 단말 플랫폼이 UPP(User Privacy Policy) 설정정보를 응용서버에게 전송하여 해당 프라이버시 등급에 맞는 정보를 수신하게 된다. 아래의 그림 10은 서비스 적용 메커니즘을 나타내고 있으며, 사용자의 UPP 정보 없으면 사용자에게 프라이버시 보호 정책 고시 및 레벨설정 요청하고, 사용자의 UPP 정보가 있으면 사용자의 UPP를 OIS 시스템에 맞게 가공하여 전달하는 순서로 동작된다.

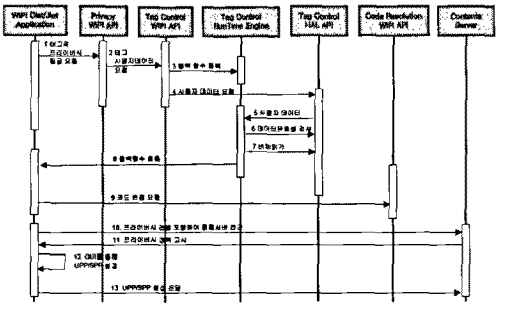


그림 9. RFID 프라이버시 보호 기능 절차

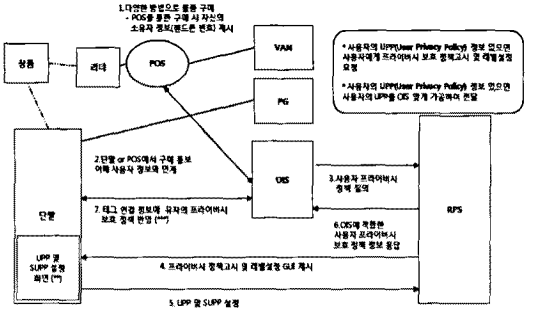


그림 10. 개인 프라이버시 보호 적용 메커니즘

3.2.7 단말 플랫폼 접근 보안 등급 기능 적용

모바일 RFID 단말 플랫폼 시스템에 대한 안전성을 보장하기 위해, WIPI에서 각 자원마다 정의된 보안 수준별 접근 정책을 지정하고, 이에 따른 서비스 접근 통제를 기반으로 하는 보안 정책을 적용한다[3,4]. 즉, 단말 플랫폼의 각 자원 별로 보안 수준에 따라 접근 허용여부 지정하는 것으로 해당 기능 API별 자원을 분류하여 해당 그룹에 대한 접근인가 등급을 구성하여 적용한다.

Ⅳ. 모바일 RFID 단말 보안 플랫폼 구현 분석

4.1 구현 시스템 테스팅

본 논문의 연구개발 결과물에 대한 서비스 테스트 베드는 ETRI 연구과제[12]로 구축되었으며, 결과 기준은 모바일 RFID 포럼 표준[1,2]을 통해 검증되었다. 구현된 단말 보안 S/W 플랫폼 시스템은 외장형 모바일 RFID 리더와 표준형 시리얼 통신으로 연결된 실제 상용화된 핸드폰에 적용되었다. 전체적인 H/W시스템 모형은 그림 11처럼 외장형 모바일 RFID 시스템으로, RFID 리더는 외부에 RFID 안테나와 RFID 리더 모듈로 구성되어 있다.

그림 12는 모바일 RFID 단말 보안 S/W 플랫폼을 실제 환경에서 시연한 화면이다. (a)는 모바일 RFID 단말 플랫폼에서 필터링을 수행한 LCD 창 화면이며, (b, c)는 무선인터넷으로 연결된 모바일 단말기 실행 화면을 캡쳐한 것이다.

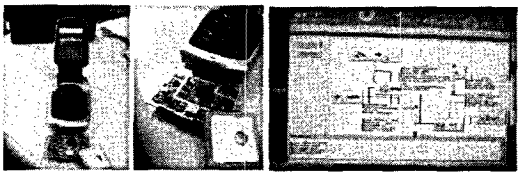


그림 11. 구현된 모바일 RFID 서비스 시스템 모습

그림 12. 모바일 RFID 단말의 시연 화면 (a,b,c)

4.2 구현 결과 분석

모바일 RFID 단말 플랫폼은 제한된 단말의 하드웨어 기능과 이동성으로 인해 전용 RFID 리더기에서만 태그 데이터를 수집하게 되며, 따라서 동시에 읽어드리는 태그 개수도 제한적일 수밖에 없다. 구현된 모바일 RFID 단말 보안 플랫폼 시스템으로 단말 플랫폼의 여러 기능이 동작되어 태그 정보를 읽고, 해당 응용 서비스 서버로 접속하여 정보를 가져오는 서비스 과정에 따른 데이터 전송의 수행시간 결과는 다음 표 1과 같다.

표 1. 모바일 RFID 기능별 주요 응용 수행시간 결과

(단위 : 초)

서비스과정	상태 (R/W)	평균 수행시간			
		전체 시간	통신 시간	주요 API 연산	내부연산 (주요 API 단계)
리더 오픈 상태 요청	R	0.12	-	ISOPENREADER	3
리더 실행 상태 요청	R	0.09	-	ISBUSYREADER	3
리더 인증	-	0.14	-	SecureReaderAuth	4
보안키 설정 및 인가	-	0.17	-	SecureKey	2
태그 읽기	R	0.15	-	STARTTRIGGERDATA	5
태그 읽기 중지	R	0.13	-	STOPTRIGGERDATA	5
태그 읽기 (User Data 읽기)	R	0.25	-	REQUSERDATATYPEC	7
서버 URL 접속 요청	-	-	0.5	-	-
정보 데이터 획득	-	-	0.6	-	-
전체 소요시간	-	1.05	0	-	29

4.2.1 데이터 전송 성능 평가

본 논문에서는 단말 보안 S/W 플랫폼의 기능을 이용하여 외장형 RFID 리더기를 통해 태그 데이터를 미리 읽어 저장한 후에 데이터 보안 API 기능을 이용한 보안 필터링속도와 필터링 결과를 모바일 클라이언트로의 전송하는 속도를 측정하였다. 단말 보안 플랫폼의 데이터 보안기능에 대한 필터링 성능 분석을 위해 다중 접속 서버형이므로 동시에 오픈 가능한 모바일 RFID 단말기 수는 1~4개까지의 동시 접속을 기준으로 하였으며[8,9,10], 필터링 조건은 태그 정보에 대한 AES 데이터 암호화 조건을 적용하였다. 모바일 H/W 리더기는 900MHz 대역의 국내 N사 외장형 모바일 RFID 리더 및 자체 개발된 리더기를 기반으로 하였으며, 실제 이동통신사의 무선 인터넷 환경에서 테스트를 진행하였다. 구현된 모바일 RFID 단말 보안 S/W 플랫폼의 성능을 분석하기 위해 사용된 성능척도는 태그 개수, 모바일 RFID 단말기 수, 필터링 수행시간과의 관계를 측정하였다.

그림 13에서 태그 개수는 5개부터 150개, 동시 오픈 가능한 모바일 RFID 단말기 수는 1~5개까지를 가정하였다. 그래프는 보안 API 기능의 필터링 기능을 이용하지 않고 수집된 태그 데이터를 클라이언트로 직접 전송하는 경우 에 대한 전송시간 측정 결과이다. 측정 결과는 전체적으로 태그 수와 오픈된 클라이언트 수에 따라 필터링속도가 약간 증가 되었지만 1~3초 이내에 수행이 완료되는 것을 확인하였다.

그림 14의 그래프는 단말 플랫폼의 AES 암호 알고리즘을 사용한 보안 필터링 기능을 이용하여 수집된 태그 데이터를 클라이언트로 직접 전송하는 경우 에 대한 전송시간 측정 결과이다. 이 경우는 필터링 기능을 수행하는 경우의 그래프와 동일한 조건으로, 태그 개수는 1~150개, 클라이언트 수는 1~5개를 적용하여 측정하였다. 태그 데이터는 각 클라이언트에 모두 도착 완료되는 시간을 기준으로 하였다. 그림 14의 그래프 결과로 보면 보안 필터링을 수행하고 전송하는 경우 단말 플랫폼에서의 필터링 시간은 거의 소요되지 않지만 서버 플랫폼으로의 전송 데이터 양이 상대

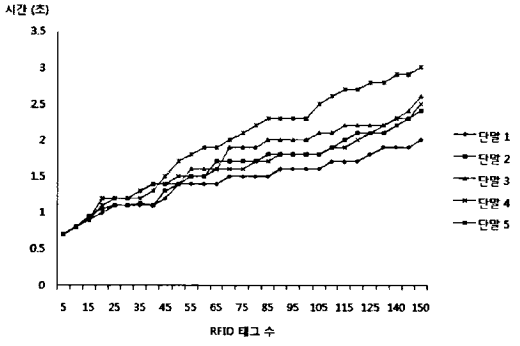


그림 13. 보안 API의 필터링이 적용되지 않은 경우의 전송 시간

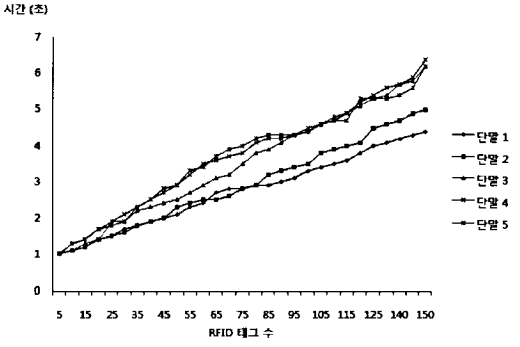


그림 14. 보안 API의 필터링이 적용된 경우의 전송 시간

적으로 많아 전송시간은 약간 높아진 4~8초까지의 전송 시간을 확인할 수 있었다. 이 시간은 보안이 적용된 테스트의 경우 단말 플랫폼에서 암호화와 복호화가 각각 일어남으로 인해 소비되는 오버헤드로 생각되어질 수 있으며, 이때 무선 네트워크 전송 이후의 시간은 전체 송수신 시간에 큰 영향을 미치니 않기 때문에 비슷하게 측정되어지는 것으로 나타났다. 위의 분석 내용에서 무선인터넷 환경과 소용량 데이터 처리를 위한 이러한 성능 결과는 열, 먼지, 전자파, 제한된 단말 성능, 서버가 놓여있기 어려운 환경 등 열악한 여러 서비스 환경에서 모바일 RFID 보안 기능을 적용하면서, 해당 비즈니스 프로세스를 처리하는데 필요한 서비스를 정확하게 수행할 수 있음을 보여준다.

4.2.2 보안 세션 요청에 따른 지연시간 및 임계치

단말에서 네트워크 정보 서버로의 보안 세션 생성 요청률에 따른 지연시간 증가와 세션 처리가 가능한 임계치를 측정한다. 단말 플랫폼에서 보안키의 암/복호화 처리와 네트워크 전송 처리에 따른 세션 생성 지연 및 성능을 비교 분석한다. 하나의 모바일 RFID 단말기에서 OIS 등의 네트워크 정보로 여러 개의 세션 연결을 시도하도록 하며, 이러한 모바일 RFID 단말기를 여러개로 이용하여 실제 단말기가 세션 연결을 하는 것과 동일한 환경을 구성한다.

평균 보안 서비스 세션지연 시간 측정결과는 그림 15와 같다. 보안 서비스 세션 요청의 경우 세션의 개수가 증가할수록 세션 생성까지의 시간은 계속적으로 증가되며, 요청률이 40개로 증가하면 1000~1500msec의 지연시간을 보였다. 요청률이 50개가 되면 1800msec까지 지연되며, 60개의 요청부터는 세션 에러가 발생한다.

그림 16의 서버에서 측정한 초당 세션 요청개수에 따른 처리를 살펴보면, 50개까지 세션에 대한 모든 처리가 가능하지만 60개의 요청부터 세션 처리가 감소

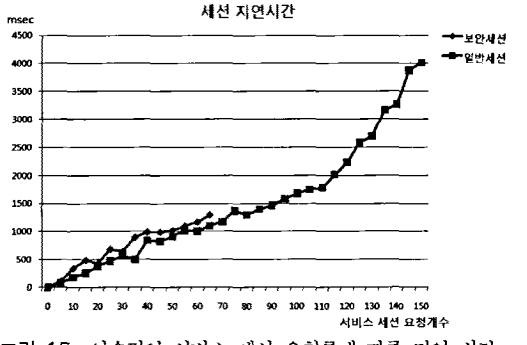


그림 15. 연속적인 서비스 세션 요청률에 따른 지연 시간

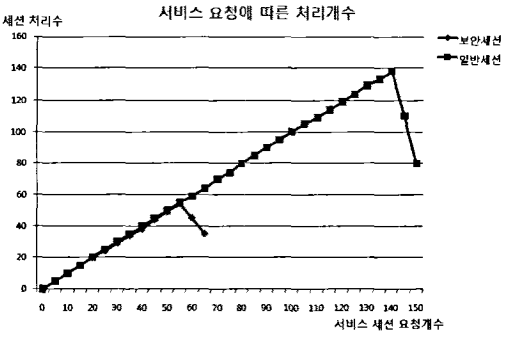


그림 16. 보안 서비스 요청률에 따른 처리 개수

한다. 때문에 시험 시스템, 네트워크 정보 서버에서의 동시 처리 가능한 보안 세션 수는 60여개까지 가능한 것으로 측정되어진다. 일반 서비스 세션의 경우 초당 요청되는 세션의 개수가 120개까지 증가할수록 증가하는 시간은 약 2000~2500msec까지 증가하며, 120개의 요청부터 세션 지연시간이 급격히 증가하며 140개의 요청부터는 세션 에러가 발생하게 된다. 서버에서 측정한 초당 서비스 세션 요청개수에 따른 처리별 처리수를 살펴보면, 동시에 130개까지 요청된 세션에 대든 처리가 가능하지만 140개의 요청의 요청부터는 세션 처리가 급격하게 감소하게 된다. 때문에 시험 단말기, 서버에서의 동시에 처리 가능한 서비스 세션 수는 140개까지 가능한 것으로 측정되어 진다.

성능 측정 결과를 비교해 보면 보안 기능을 지원하는 것과 미지원의 세션 지연시간은 비슷한 값으로 증가되어진다. 하지만 보안 기능의 오버헤드가 약 2배정도 있다는 것으로 측정되어진다. 이는 단말기 내부에서 요청된 보안 서비스 세션에 대한 처리 시 필요한 자원 할당으로 생기는 문제에 발생되는 것으로 예상되어 진다. 이에 비해 일반적인 모바일 RFID 단말기의 비 보안 서비스 경우 세션에 대한 정보처리가 간단한 RFID 태그 정보 데이터가 이루어지기 때문에 세션 처리 능력이 높을 것으로 예상된다.

V. 결 론

모바일 RFID 서비스는 기존의 RFID 시스템과 모바일 시스템이 접목되어 만들어 일상생활에 넓게 이용되게 될 것이다. 이에, 모바일 기기가 많은 사람들이 보편적으로 사용하는 만큼 모바일 리더 또한 보편적인 기기가 되어 사용자들의 프라이버시 침해 문제를 발생시킬 것이다. 이에, 본 논문에서는 최근 각광을 받고 있는 안전한 모바일 RFID 응용 서비스를 제

공하기 위해 모바일 RFID 기술과 이의 여러 가지 보안 취약성을 분석해보고, 이를 위한 다각적인 정보보호 서비스 모델의 제안과 그 기술에 대해 살펴보았다. 그리고, 세계 최초로 개발된 UHF 900MHz 모바일 RFID 서비스 환경에 대한 단말 임베디드 보안 S/W 플랫폼의 실제적인 구현을 통해 기술적으로 규명함으로써 안전한 모바일 RFID 서비스 인프라가 갖춰야 할 정보보호의 기능적 목표를 제시할 수 있도록 하였다. 앞으로 모바일 RFID 기술을 이용한 안전한 유비쿼터스 서비스 환경을 이용하기 위해서는 서비스 이용자의 의식 개혁, 프라이버시 법안, 해킹 대응 기술 및 서비스를 위한 보안 서비스 모델을 수립하여 모두에게 필요한 프라이버시 보호를 제공해야 할 것이다[3,5]. 서비스 활성화를 위한 법/제도 차원에서 보안기술 및 프라이버시 보호를 위한 노력을 해야 하지만, 이와 더불어, 기술적인 차원에서의 기술을 개발해야 한다. 그리고, 우리는 모바일 RFID 기술의 목표, 계획 및 사용에 대한 분명한 기준을 통해 프라이버시에 대한 시민들의 권리를 보존하는 한편 서비스를 활성화 시킬 수 있는 최선책을 앞서 생각해야 한다고 본다.

참 고 문 헌

[1] 김말희, "모바일 RFID 리더를 위한 WIPI C API", *모바일 RFID포럼 표준*, MRFS-1-04, 2006.

[2] 박경호, "모바일 RFID리더를 위한 HAL API", *모바일 RFID포럼 표준*, MRFS-1-03, 2006.

[3] 박남제, 곽진, 김호원, 김승주, 원동호, "WIPI Mobile Platform with Secure Service for Mobile RFID Network Environment," *LNCS*, Vol 3842, pp.741-748, January 2006.

[4] 박남제, 강유성, "모바일 RFID 보안기술", *TTA 저널*, 제115호, pp.108-114, 2008.

[5] 강전일, 박주성, 양대현, "RFID 시스템에서의 프라이버시 보호기술", *정보보호학회지*, 제14권 제6호, 2004.

[6] 김일중, 최은영, 이동훈, "모바일 기반의 RFID 프라이버시 보호 기법", *정보보호학회 논문지*, 제17권 제1호, pp.89-96, 2007.

[7] 정윤선, 김일중, 최은영, 이동훈, "모바일 RFID 시스템에서의 보안 위협과 대안", *한국방송공학회 학술발표 논문집*, pp.93-96, 2007.

[8] Namje Park, Seungjoo Kim, and Dongho Won, "Privacy Preserving Enhanced Service Mechanism in Mobile RFID Network," *ASC Series*, Vol.43, pp.151-156, 2007.

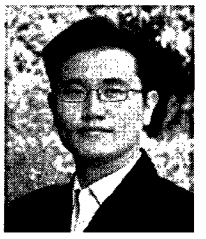
[9] 박병섭, "모바일 환경을 위한 모바일 RFID 미들웨어 모듈 설계 및 구현", *한국콘텐츠학회논문지*, 제8권 제9호, pp.10-18, 2008.

[10] Feldhofer, M., Dominikus, S. Wolkerstorfer, J., "Strong authentication for RFID systems using the AES algorithm," *CHES 2004, LNCS*, Vol.3156, pp.357 - 370. 2004.

[11] 박남제, "RFID 가상 태그를 활용한 개인화된 광고 및 정보 응용 서비스 개발", *한국 IT서비스학회지*, 제8권, 제4호, pp.151-163, 2009.

[12] 정교일 외, "안전한 RFID/USN을 위한 정보보호 기술개발에 관한 연구", *ETRI연구보고서*, 지식경제부, 2009.

박 남 제 (Namje Park) 정회원



2000년 8월 동국대학교 정보산업학과

2003년 8월 성균관대학교 정보보호학과 석사

2008년 3월 성균관대학교 컴퓨터공학과 박사

2003년 4월~2008년 12월 한국전자통신연구원 정보보호연구단 선임연구원

2009년 1월~2009년 12월 UCLA대학교 공과대학 Post-Doc.

2009년 3월~2009년 12월 UCLA대학교 WINMEC 연구센터 Staff Researcher

2010년 1월~현재 Arizona State University 컴퓨터공학과 Research Scientist

<관심분야> 암호이론, 융합기술보안, 모바일컴퓨팅, RFID/USN, 스마트 그리드 등