RFID/USN 보안 기술 개발 동향

조현숙 · 정교일 ·
최두호 · 강유성
한국전자통신연구원
정보보호연구본부

요 약

RFID 기술은 ISO/IEC 18000 표준문서에서 정의한 규격에 기반하여 기술 개발이 진행되고 있으며, USN 기술은 IEEE 802.15.4에 기반한 Zigbee 표준문서를 따르는 센서 노드를 중심으로 기술이 발전하고 있다. 이러한 기본적인 통신 기능과 더불어 RFID/USN 정보 보호를 위한 보안 기술 논의도 활발하게 전개되고 있으며, 그 결과로서 RFID/USN 보안 취약점, 보안 필요성 및 보안 요구사항 등에 대한 분석 자료들은 지속적으로 발표되고 있다. 그러나 요구사항 분석 자료와 달리 기술적인 해결 방안을 제시하는 자료들은 단편적인 기능에 중점을 둔 학술적인 이론 분석에 머무르고 있을 뿐 실제 상용화 수준의 개발 내용들을 제공하는 발표는 미흡한 실정이다. 따라서 본 고에서는 기본적인 보안 요구사항 정리 수준을 넘어 보다 구체적인 RFID/USN 보안 기술의 개발 결과를 제시하고자 한다.

Ⅰ. 서 론

RFID(Radio Frequency Identification) 환경에서는 사물 단위의 정보화가 이루어져 보다 신뢰성 있는 정보 전달이 가능해질 것으로 예상되나, 현재의 RFID 기술은 보안 기능이 매우 취약하여 태그의 변조, 위장 리더, 서비스 거부 공격 등 수많은 위협에 노출된 상태이며, 특히 개인 프라이버시 문제가 가장 심각한 위협으로 지적되고 있다. 한때 유럽 중앙은행은 유럽에서 사용하는 유로 화폐에 RFID 태그를 내장하려고 계획한 적도 있으며[1], 일본에서도 10,000엔 지폐에 히다찌의 뮤칩을 부착할 계획을 세우기도 하였지만[2] 결국 실행에 옮기지는 못했다. 만약의 경우이긴 하지만 아무런 정보 보호 대책을 세우지 않은 채 실물 경제의 핵심인 지폐에 RFID 시스템이 적용된다면 악의적인 사람이 길거리에 지나가는 사람들을 모니터링하여 현금을 많이 가지고 다니는 사람을 찾아 범죄의 대상으로 삼을 수 있다. 이렇듯 개인이 보유하고 있는 물품에 붙인 태그가 악의적인 사람의 물음에 자신의 정보를 가르쳐 준다면 이는 심각한 사회 문제가 된다. 또한, RFID 태그의 정보 노출 취약성뿐만 아니라 RFID 시스템의 DoS(Denial of Service) 취약성도 심각한 문제를 야기시킬 수 있다. 만일 악의적인 공격자의 침입에 의해 네트워크 가용성이 훼손 당한다거나 또는 네트워크로 유입되는 태그 정보의 비정상적인 폭주를 고려하지 못하여 DoS 공격에 취약하게 설계된다면 이는 네트워크 인프라 전체에게 영향을 끼치는 심각한 정보보호 결함이 될 것이다.

RFID 태그의 지향점이라 할 수 있는 USN(Ubiquitous Sensor Network) 기술은 스스로 주변을 감지하고 정보를 유통시킬 수 있는 센서 네트워크 구성을 전제로 하며, 다양한 위치에 설치된 센서 노드들로부터 사람과 사물, 그리고 환경 정보를 인식하고, 인식한 정보를 통합 · 가공해 언제, 어디서나, 안전하고 자유롭게 이용할 수 있게 하는 정보 서비스 인프라를 제공한다. USN 환경에서는 수많은 센서 노드들이 감지한 정보를 베이스 스테이션으로 보내는데 있어, 각 센서 노드들의 제한된 전력은 빈번한 네트워크의 진

입과 탈퇴를 발생하여 잦은 토폴로지의 변화를 가져오며 이는 수집되는 정보의 신뢰성을 떨어뜨리는 결과를 가져온다. 이러한 가운데 악의적인 노드가 센서 노드로 가장하여 네트워크에 진입하게 되면 잘못된 정보를 전파하거나 라우팅 정보를 혼란시켜 센서 네트워크의 보안 취약점을 가중시킬 수 있다. 특히 센서 노드들이 배치된 물리적 환경이 공격에 그대로 노출되기 쉬우므로 전송되는 정보가 변경되거나 유출되어 정보의 기밀성 및 무결성을 쉽게 무너뜨릴 수 있다. 더욱이 이러한 공격의 파급 효과는 단순히 센서 노드만의 문제만이 아니라 USN 서비스를 사용하는 일상생활까지 확대 가능하여 그 파급 효과는 매우 클 것으로 예상된다. 이렇다 보니 보안을 강화하기 위한 방법으로 내부적으로 센서 노드의 보안 기능을 추가하는 것 이외에도 외부적으로 보안 위협으로부터 전체 네트워크를 보호하기 위해 네트워크의 모든 부분에 보안 기능을 도입하는 계층적 보안이 필요하다.

2004년에 국제표준으로 제정된 ISO/IEC 18000 시리즈 문서 및 EPCglobal의 UHF 통신 규격에 기반한 RFID 기술의 초기 목적은 제품 식별자의 자동인식이었으며, 기업의 물류 시스템 혁신 및 재고 관리 등 B2B(Business-to-Business) 서비스의 효율성과 신뢰성을 높이는데 기여할 것으로 기대되었다. USN 기술에 있어서는 주로 IEEE 802.15.4 기술에 기반한 Zigbee 표준문서가 핵심이 되는 기술을 제공하였으며, Zigbee 통신이 가능한 소형 모트가 대표적인 센서 노드가 되었다. 이러한 기본적인 통신 기능이 우선적으로 개발되어 왔으며 이와 더불어 RFID/USN 기술에 대한 본격적인 연구 개발 및 시범 서비스가 시작되었던 2004년 이후로 RFID/USN 정보 보호 기술에 대한 연구 역시 활발하게 진행되어 왔다. 그 결과로 국내에서는 2004년부터 최근에 이르기까지 참고문헌 [3]~[15]와 같이 RFID/USN 보안 취약점, RFID/USN 보안 필요성 및 RFID/USN 보안 요구사항 등에 대한 분석 자료들이 10여편 이상 발표되었다. 이 중 일부 자료들은 기술적인 접근을 포함하고 있지만 종합적인 고려가 아닌 단편적인 기능에 중점을 둔 학술적 분석에 머무르고 있는 수준이다.

본 고에서는 기본적인 보안 요구사항 정리 수준을 넘어 보다 구체적인 RFID/USN 보안기술의 개발 결과를 제시함으로써 RFID/USN 보안 응용 서비스 활성화에 기여하고자 한다. 이를 위하여 본 고는 다음과 같은 구성을 가진다. 제Ⅱ장에서는 RFID/USN 시스템의 보안 취약점과 보안 요구사항을 간략하게 정리한다. 일부 내용은 기존 자료들인 참고문헌 [3]~[15]의 분석을 인용하였다. 제Ⅲ장에서는 본 고에서 제시하고자 하는 RFID/USN 보안기술 개발 동향을 정리한다. 그리고 제 Ⅳ장에서 결론을 맺는다.

Ⅱ. RFID/USN 보안 취약성 및 보안 요구사항

2-1 RFID 보안 취약성

RFID 시스템을 공격하는 일반적인 RFID 공격기법을 살펴보면 다음과 같다[15].

2-1-1 도청 공격

RFID 시스템은 바코드 시스템과 달리, 효율성을 높이기 위해 수 미터 범위 내에서도 리더와 태그 간에 통신이 가능하도록 되어있는 무선 방식이기 때문에 누구든지 태그에 질의하여 태그의 응답 값을 얻을 수 있다. 도청 공격의 형태로는 공격자가 리더를 갖고 태그를 스캐닝(scanning)하는 적극적 공격과, 리더와 태그간 통신을 무선으로 수신하는 수동적 공격이 있다.

2-1-2 트래픽 분석

리더와 태그 간 통신 중 트래픽 분석을 통한 위협이 존재한다. 공격자가 어떤 특정 지역 또는 특정 태그에서 리더와 태그 간의 트래픽 분석에 의한 통계

기반의 식별 정보를 추적할 수 있다면, 공격자는 그 지역에서 어느 정도의 트래픽이 존재하는지 어느 정도의 물품이 존재하고 빠져 나가는지에 대해서 알 수 있다.

2-1-3 재전송 공격(Replay Attack)

RFID 시스템은 공격자가 도청으로 획득한 정보를 이용하여 정당한 태그로 가장하여 공격할 수 있다.

2-1-4 스푸핑(Spoofing) 공격

공격자가 정당한 리더로 가장하여 태그에 질의함으로써 태그로부터 인증 정보를 획득할 수 있거나, 공격자가 상품의 태그를 이용하여 유인 태그를 만든 후 실제 제품과 바꾸는 태그 스푸핑(Spoofing) 공격이 발생할 수 있다.

2-1-5 태그 복제

공격자는 도청한 데이터의 해독, 부채널 공격(SCA, Side Channel Attack) 등을 통해 태그의 정보를 복제할 수 있다.

2-1-6 메시지 유실

공격자에 의한 서비스 거부나 무선 통신에 방해가 되는 잡음 등의 문제로 인해 전송되는 데이터가 훼손, 유실될 수 있다.

2-1-7 서비스 거부(DoS, Denial of Service) 공격

공격자는 태그의 수를 급격히 늘리거나 전파 방해 등을 통해 서비스 거부 공격을 시도할 수 있다.

2-1-8 물리적인 공격 방법

단순전력분석(SPA, Simple Power Analysis) 및 차분전력분석(DPA, Differential Power Analysis), 칩 내부 공격(Chip Rewriting Attack), 메모리 잔류정보 분석 공격(Memory Remanence Attack) 등이 있다.

2-2 USN 보안 취약성

USN 시스템을 위협하는 대표적인 공격은 다음과 같이 정리될 수 있다[11].

2-2-1 도청

USN 시스템을 구성하는 각 센서 노드들은 일반적으로 IEEE 802.15.4와 같은 무선 통신을 구성한다. 따라서 무선 통신 상에서 주고받는 데이터에 대한 기밀성이 제공되지 않을 경우, 외부 공격자는 매우 손쉽게 도청을 할 수 있다. 따라서 데이터 기밀성 보장을 위한 암호화 기법의 사용이 요구된다.

2-2-2 데이터 위변조

센서 노드들은 무선으로 통신을 하기 때문에 공격자가 네트워크에 참여하기 위한 물리적인 제약이 없으므로, USN 시스템에서 공격자가 데이터 위변조 공격을 시도하는 것이 상대적으로 매우 쉽다.

2-2-3 서비스 거부 공격

USN 시스템에서 센서 노드들은 응용 서비스에 따라 매우 열악한 환경에 설치될 수 있으며, 굳이 공격이 일어나지 않더라도 배터리 소실, 홍수 등과 같은 자연/인공 재해에 의한 노드 유실 등의 가능성이 항상 존재한다. 여기에 공격자가 고의적으로 노드를 파괴할 가능성까지 생각한다면, 특정 노드들이 네트워크 상에서 탈락하더라도 라우팅 경로를 자동적으로 재설정하는 등 결함 감내(Fault Tolerance) 기능을 포함하고 있어야 할 것이다. 이러한 결함 감내 기능을 제대로 설계하기 위해서는 다양한 계층에서 이루어질 수 있는 서비스 거부 공격의 가능성을 충분히 고려하여야 한다.

2-2-4 라우팅 공격

USN 시스템에서 이루어지는 라우팅 공격은 메시지가 정상적인 경로를 통하여 싱크 노드에게 전달되

는 것을 방해하고자 하는 것이다. 공격자는 라우팅 공격을 이용하여 응용 서비스가 정상적으로 이루어지지 않도록 할 수 있으며, 또한 다른 종류의 공격을 시도하기 위한 준비 단계로서의 공격 효과도 가능하다. 일반적인 USN 라우팅 기법들은 제한된 능력을 가진 노드들이 센싱된 데이터를 얼마나 효율적으로 보내는가에 초점을 맞추고 있으나, 보안을 고려하지는 않았기 때문에 여러 종류의 라우팅 공격에 취약할 수밖에 없다.

2-2-5 물리적 공격

물리적으로 센서 노드를 탈취하여 노드 내부의 중요한 정보를 획득하는 경우는 심각한 위협이 될 수 있다. 예를 들어, 기초적인 수준의 보안성을 제공하기 위하여 어떤 USN 시스템에서는 모든 노드들이 동일한 암호 키를 사용하고 있다고 가정하면 단지 하나의 노드를 탈취하여 키 정보를 획득하는 것만으로도 전체 네트워크를 손쉽게 도청할 수 있는 효과가 있으며, 또한 공격용 코드를 삽입하여 내부자 공격에 이용할 수도 있다. 또 다른 형태의 물리적 공격으로 노드가 동작하고 있을 때 사용하는 소비 전력 혹은 방사되는 전자파 정보 등을 이용하여 노드 내부에 있는 암호 키와 같은 중요한 정보를 알아내는 부채널 공격이 있다.

2-3 RFID/USN 보안 요구 사항

〈표 1〉은 RFID/USN 시스템에서 제공하고자 하는 보안 서비스 및 보안 서비스별 주요 보안 요구사항을 정의하고 있다[15].

Ⅲ. RFID/USN 보안기술 개발 동향

RFID/USN 보안 기술 개발의 목표는 RFID 및 모바일 RFID 환경에서 태그와 리더, 미들웨어 등 제반 환경에 대한 보안 및 프라이버시 보호 기술을 제공하며, 센서 노드와 네트워크, 베이스 스테이션 등

〈표 1〉 RFID/USN의 보안 요구 사항

구분	RFID/USN의 보안 요구 사항
기밀성	· 태그 데이터를 암호화할 수 있어야 한다. · 태그의 설계 또는 구조의 간섭 없이 암호화된 데이터를 읽고 쓸 수 있어야 한다. 이러한 특성은 사용자가 선택할 수 있어야 한다. · 센서 노드의 정보는 암호화되어 전달되어야 한다. 이는 도청의 위협을 극복하기 위함이다.
익명성	· 태그 데이터 또는 별도의 식별 정보에 대한 익명성이 보장되어야 한다. · 정보를 이용한 사물 및 개인에 대한 위치추적 경로 추적 및 감시가 이루어지지 않도록 인증된 적법한 사용자가 제어할 수 있다.
무결성	· 태그는 데이터의 변경이나 삭제를 막을 수 있어야 한다. · 태그 제조사들은 특정 데이터를 잠글 수 있는 기능을 가져야 한다. · 센서 노드의 전달 정보는 전송 중 훼손되지 않았음을 보장해야 한다. 이는 데이터 위변조 공격을 방지해야 함을 의미한다.
인증성	· 태그 데이터의 저장소와 전송 프로토콜은 태그 데이터를 읽기에 앞서 인증이 선행되어야 한다. · 센서 노드의 통신은 상호 인증이 선행되어야 한다.
침해 대응성	· 서비스 거부 공격 대응 · 네트워크 보호 제공 · 해킹 바이러스 침입 공격 등에 대한 대응

USN 제반 기술에 대한 보안 및 프라이버시 보호 기술을 제공함으로써, 사물의 자동 식별, 이력 추적 등 RFID/USN 서비스를 안전하고 신뢰할 수 있도록 하는 보안기 술을 제공하는 것이다. 이를 위하여 현재까지 개발된 주요 RFID 보안 기술과 USN 보안 기술이 개발되어 왔으며, 본 고에서는 다양한 기술적인 해결책을 담은 국내의 개발 결과를 요약 정리한다[16].

3-1 RFID 보안 기술

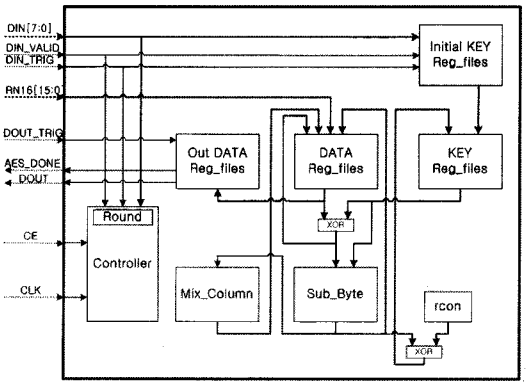
RFID 보안 기술 개발의 대표적인 결과는 수동형 RFID 태그용 보안 모듈, 보안 미들웨어와 정보 서버의 통합 보안 플랫폼, 태그와 리더 간 보안 프로토콜을 들 수 있으며, 모바일 RFID 보안을 위한 모바일 RFID 보안 미들웨어, 보안 라이브러리도 대표적인 개발 내용이다. 그리고 이러한 보안 플랫폼을 활용하는 보안 응용 서비스로는 제품 유통 이력 보증을 위한 전자 계보(e-Pedigree) 서비스, 전자 봉인 데이터 보호 서비스 등이 있다.

3-1-1 수동형 RFID 태그용 보안 모듈

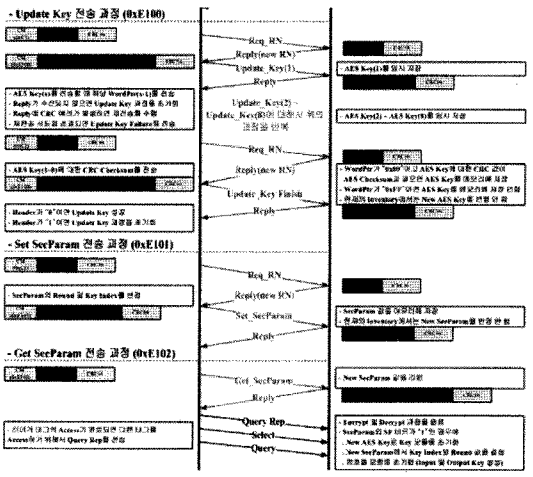
수동형 RFID 태그는 리더로부터 전원을 공급받아 동작하는 자원 제약이 심한 장치이다. 이러한 환경에서 태그와 리더간의 프라이버시 보호 및 데이터 보안을 보장하기 위하여 수동형 태그에 적용 가능한 저전력 AES 모듈을 설계하고, 이를 기반으로 태그-리더 간의 보안 프로토콜을 구현하였다. 저전력 AES 보안 모듈은 저전력 동작을 위하여 하나의 8비트 S-box 만을 반복 사용하며, 연산 효율을 높이기 위하여 ByteSub 연산과 Mixcloumn 연산을 최적화 하여 구현하였다. [그림 1]은 이러한 AES 보안 모듈의 구조이다. AES 보안 모듈은 태그-리더간의 보안 통신에 필요한 키 스트림을 생성하며, 이를 이용하여 태그-리더간 인증 및 데이터 보안을 수행한다. 이러한 보안 모듈이 적용된 수동형 보안 태그는 호환성을 고려하여 ISO/IEC 18000-6 타입 C 동작되다가 보안 동작을 위한 파라미터가 설정되면 보안 프로토콜을 수행하도록 구현되었다. 보안 프로토콜 절차는 [그림 2]와 같다.

3-1-2 보안 RFID 통합 서비스

SRIS(Secure RFID Integration Services)는 EPCglobal의 ALE(Application Level Events) 서비스 계층과 정보 서비스 계층을 통합한 시스템이다. 설정에 의해 RFID 미들웨어 및 정보 서버의 역할을 수행한다. SRIS는 EPCglobal ALE v1.0 표준 준용, EPCIS v1.0



[그림 1] 수동형 태그용 보안 모듈 구조



[그림 2] 보안 프로토콜 절차

표준 준용, EPC 코드 및 모바일 RFID 코드 처리, Gen2 태그의 user memory/kill/lock 기능 지원, SOAP 메시지 보안, 안전한 리포트 전달, 서비스 자원에 대한 접근 제어를 포함한 보안 기능 지원, 분산 구조로서 고성능 데이터 처리율과 높은 확장성 지원, 규칙 기반 상황인지 정보를 간략화 하여 응용 서비스에 제공, 응용에 대한 인가 기능 제공, 전자 계보의 생성, 검색, 검증 기능 제공의 특징을 가지고 있으며, [그림 3]과 같은 구조로 구현되어 있다.

3-1-3 전자계보(e-Pedigree) 기술

전자 계보는 물품에 대한 제조업체의 판매부터 도매상의 취득 및 판매, 소매점에서의 최종 판매에 이르기까지의 소유권 변화에 대한 전자 기록으로 물품에 대한 공급, 관리 및 유통 등의 정보를 포함하며, 하나의 계보는 한 물품에 대해 각 유통 단계별 관리 정보와 이에 대한 인증 체인을 포함한다. PDS(e-Pedigree Discovery Service)는 물품에 대해 제조업체, 유통업체 및 소매점 등의 SRIS 및 응용 등에서 생성, 갱신 및 서명하는 모든 전자 계보를 안전하게 관리하여 물품에 대한 신뢰성 있는 유통 정보를 제공한다. 전자 계보 서비스는 전자계보 문서 생성 및 검증, 전자 계보 문서 관리 및 조회 서비스 제공, 전자 계보 문서에 대한 보안 기능(접근 제어, 프라이버시 보호, 인증 등), 모바일 RFID 단말을 이용한 전자 계보 문서 조회 및 검증 등의 서비스를 제공한다. [그림 4]는 SRIS와 PDS의 연동 구조이다.

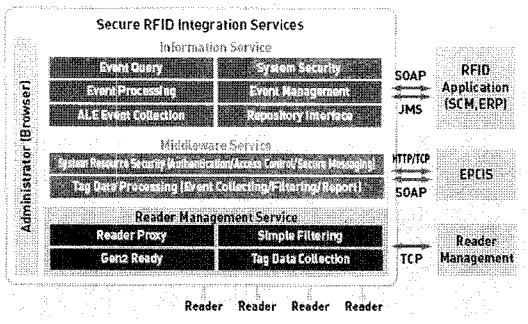
3-1-4 전자봉인(eSeal) 보안 프로토콜

전자봉인(eSeal, Electronic Seal)은 433 MHz/2.4 GHz 주파수 대역을 사용하는 능동형 RFID 기술의 대표적인 응용이며, ISO TC 104/SC 4/WG 2 표준화를 통해 ISO 18185 국제표준으로 제정된 기술이다. 능동형 RFID 태그와 리더 간 데이터 보호를 위한 전자봉인 보안 프로토콜은 ISO 18185-1 통신 프로토콜과 ISO 18185-5 물리계층 특성과 호환성을 유지하며, 태그와 리더에 대한 상호 인증 지원, 데이터 기밀성 지원, 데이터 무결성 지원, ECDSA 전자 서명을 사용하여 저장 데이터의 부인 방지 지원, 비인가 메시지의 DoS 공격 감지 방법 제공, Replay 공격의 감지 방법 제공, 고유의 마스터 키 관리를 통한 복제품 검출 방법 제공 등의 서비스가 가능하다. [그림 5]는 전자봉인 보안 프로토콜의 동작 영역을 보이고 있으며, 태그와 리더 사이의 데이터 보호를 위한 마스터 키를 분배하고 관리하기 위한 키 관리 서버와의 동작 메커니즘도 포함한다.

3-1-5 모바일 RFID 보안 라이브러리

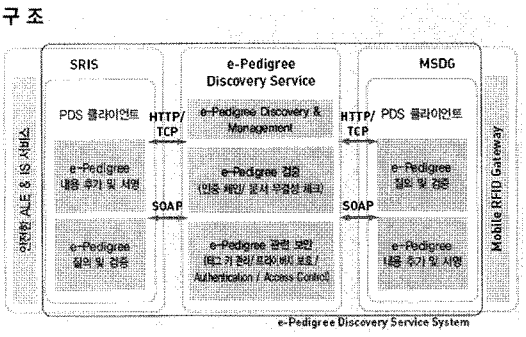
모바일 RFID 보안 라이브러리 기술은 무선 인터

구조

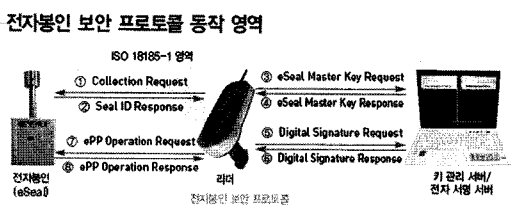


[그림 3] SRIS 구조

구조



[그림 4] 전자 계보 서비스 구조



[그림 5] 전자 봉인 보안 프로토콜 동작 영역

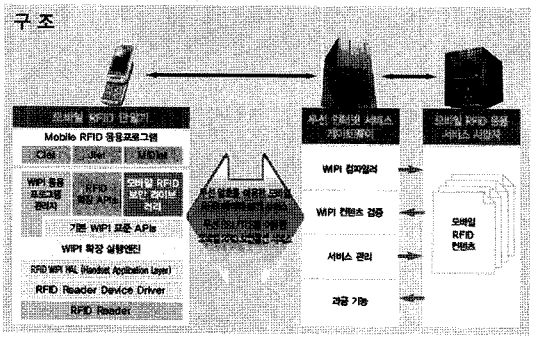
넷 표준 플랫폼인 위피(WIPI) 환경 기반의 모바일 RFID 응용 보안 수행을 위한 WIPI/C-JAVA 언어로 작성된 모바일 RFID 단말 플랫폼 암호 처리용 API 기술이다. 이 기술은 모바일 RFID 서비스 업체 및 무선 컨텐츠 산업체에서 단기간에 저렴한 비용으로 모바일 RFID 보안 응용을 개발할 수 있도록 지원한다. 이 기술은 대칭키/공개키 주요 표준 암호 알고리즘(AES, DES, 3DES, SHA-1, HMAC) 지원, 고성능 국가 표준 암호 알고리즘 및 전자 서명(SEED, KCDSA, ARIA) 지원, X.509 인증서 처리를 위한 ASN.1 지원, 개인 키 암복호 처리를 위한 PKCS #5, PKCS #8 지원 등의 특징을 가진다. [그림 6]은 모바일 RFID 보안 라이브러리의 구조이다.

3-1-6 모바일 RFID 보안 미들웨어

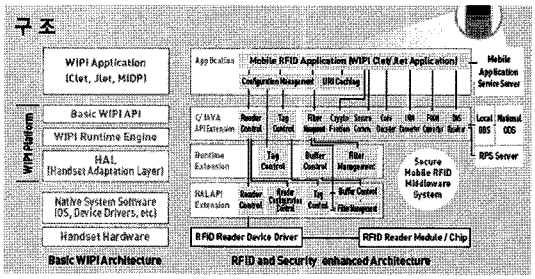
모바일 RFID 보안 미들웨어란 900 MHz 대역의 RFID 리더기를 핸드폰에 장착하여 RFID 리더를 제어하고 리더를 통해 인지된 태그에 대한 다양한 연산 기능 및 필터링 기능, ODS 질의 관련 처리 기능 등을 모바일 RFID 응용 시스템에게 안전하게 제공함으로써, 사용자가 원하는 객체에 대한 정보를 이동통신망을 통해서 획득할 수 있게 하는 시스템을 뜻한다. 이 시스템에서 모바일 RFID 정보의 보호를 위한 보안 라이브러리를 이식 및 확장하여 RFID 리더부터 응용 서버까지 모든 데이터의 이동 경로에 보안을 적용하도록 지원한다. 이 기술은 모바일 RFID 리더를 위한 WIPI API 기능(RFID 리더 제어, 태그 제어, 필터링, 코드 디코딩, URN/FQDN 변환, ODS 리졸빙, 무선 컨텐츠 서비스) 지원, 모바일 RFID 보안 API 기능(패스워드 관리, 성인 인증, 프라이버시 보호, Gen2 보안 명령) 지원, 모바일 RFID 리더를 위한 HAL API 기능(리더 제어, 버퍼 제어, 태그 제어, 필터링, 로컬 ODS 주소 설정) 지원, 모바일 RFID 포럼의 미들웨어 표준 규격 지원 등의 특징을 가진다. [그림 7]은 모바일 RFID 보안 미들웨어의 구조를 보인 것이다.

3-1-7 모바일 RFID 프라이버시 보호 서비스

RPS(RFID user Privacy management Service) 서비스는 모바일 RFID 환경에서 개인화된 태그에 연결된 정보에 대한 개인 프라이버시를 보호하는 서비스이다. 태그가 개인화되는 순간부터 태그에 연결된 다양한 정보를 소유자 개인이 RPS 서비스를 통해 직



[그림 6] 모바일 RFID 보안 라이브러리



[그림 7] 모바일 RFID 보안 미들웨어

접 통제할 수 있다. RPS 서비스는 소유자의 프라이버시 보호 정책 설정 및 관리 기능, 소유자의 프라이버시 정책에 따른 개인화된 태그에 연결된 정보 접근 제어 기능, 소유자가 설정한 의무 사항 집행 결과 통지 기능, 감사 로그 관리를 통한 프라이버시 감사 기능 등을 제공한다. [그림 8]은 일반적인 모바일 RFID 서비스 아키텍처에 RPS 서버가 함께 연동되는 RPS 서비스 시나리오를 나타낸 그림이다.

3-2 USN 보안 기술

USN 보안 기술 개발의 대표적인 결과는 센서 네트워크에서 안전한 인증 및 키 관리, 접근 제어, 프라이버시 보호 기능을 제공하는 USN 보안 플랫폼 구축 기술과 USN 보안 관리 시스템 및 센서 노드용 저전력 하드웨어 보안 모듈 구현 기술이다. 이러한 USN 보안 기술을 기반으로 구축된 안전한 USN 네트워크는 물류, 교통, 의료 등의 다양한 보안 응용 서비스에 활용될 수 있다.

3-2-1 안전한 USN 보안 플랫폼(esPlatform)

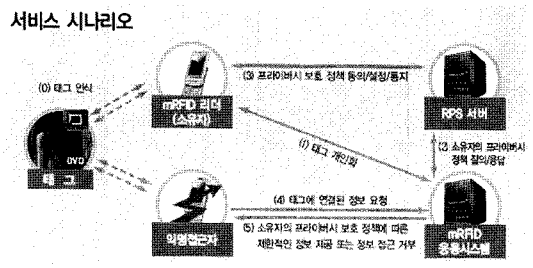
USN 환경에서 센싱되어 전달되는 데이터들은 개인의 프라이버시나 기업의 비밀 정보와 관련된 경우가 많으며, 이러한 데이터들에 대한 도청 혹은 위변조는 중대한 침해가 될 수 있다. 이러한 침해에 대응하기 위하여 센싱 데이터에 대한 보안 기능이 반드시 필요하다. [그림 9]는 USN 보안 플랫폼을 구성하는 구성 요소를 보인 그림이다. esNode로 표현된 센서 노드는 센싱 정보 및 보안 정보 감지 후 esGate로 전달하고 안전한 멀티홉 라우팅, AES 기반 MAC 메시지 생성, 응용 메시지 보안 및 공개키(ECC) 기반 노드 인증과 키 교환을 수행한다. esGate는 안전한 보안 게이트웨이 시스템으로써 센싱 정보와 보안 정보를 수집하여 esCenter로 전달하고, 센서 노드 및 esCenter에 대한 접근 제어, 센서 노드에 대한 키 전달 등의 보안 기능을 수행한다. 그리고 보안 관리 시스템인 esCenter는 보안 정보와 센서 네트워크 정보 모니터링, 저장 및 관리 기능, 그리고 센서 노드 초기화와 보안 정보 입력 기능을 수행한다.

3-2-2 저전력 HW/SW 보안 모듈

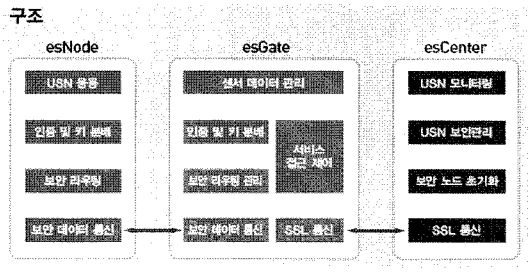
센서 노드는 공개된 환경에서 사용되므로 다양한 보안 위협이 존재하며, 에너지와 연산 능력 등의 자원 제약으로 인하여 암호화 기능을 수행하기 위해서는 효율적인 보안 모듈 구현이 필요하다. USN에서 사용하기 위한 저전력 대칭 키 하드웨어 암호 모듈(AES, 해쉬함수), TinyOS용 경량 보안 소프트웨어 모듈, USN 시스템을 위한 공개 키 보안 모듈(ECC) 및 [그림 10]과 같은 이러한 세부 기술을 집약시킨 저전력 보안 센서 노드 구현의 결과가 있다.

3-2-3 USN 보안 관리 시스템(esCenter)

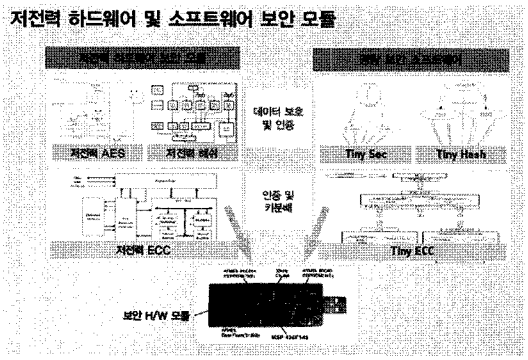
USN 보안 관리 시스템은 사용자나 네트워크 관



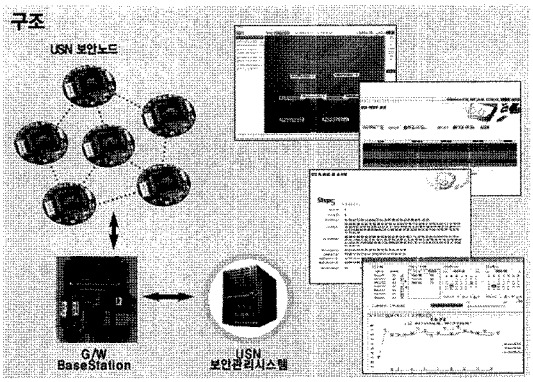
[그림 8] RPS 서비스 시나리오



[그림 9] USN 보안 플랫폼



[그림 10] 저전력 하드웨어/소프트웨어 보안 모듈 및 저전력 보안 센서 노드

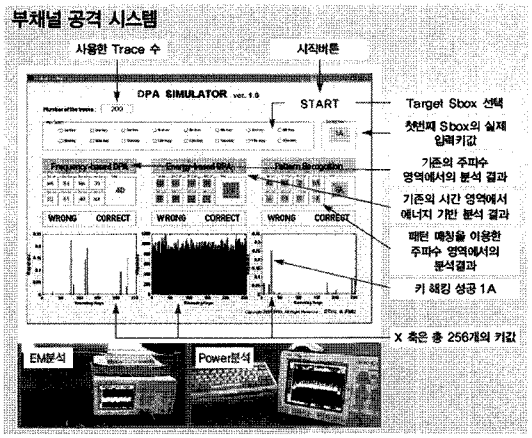


[그림 11] USN 보안 관리 시스템

리자에게 센서 노드와 게이트웨이로 구성된 센서 네트워크를 보다 쉽고 용이하게 관리할 수 있을 뿐 아니라 응용 환경에서 보안 관리 및 보안 예방 서비스 등을 제공하기 위한 통합 관리 시스템이다. 주요 기능으로는 센서 네트워크 보안(침입) 상태 관리, 센서 네트워크 모니터링, 센서 노드 및 네트워크의 보안 이벤트 관리, USN 보안을 위한 키 생성 및 배치, 센서 노드 초기화, 특정 노드에 대한 질의 요청 및 보안상태 관리, 센서 노드별 실시간 데이터 모니터링, 센서 노드로부터 수집된 정보의 분석 및 통계, 그래프 제공, 센서 네트워크의 토폴로지 및 노드의 전원 소모 관리, 사용자 웹 인터페이스 제공 등이 있다. [그림 11]은 USN 보안 관리 시스템의 개념 및 사용자 인터페이스 결과를 표현한 그림이다.

3-2-4 센서 노드 부채널 공격 시스템 및 방어 기술

부채널 공격(SCA, Side Channel Analysis)은 암호학적으로 안전성이 검증된 보안 알고리즘이 보안 하드웨어(예를 들어 스마트 카드 또는 센서 노드)에서 동작할 때, 회로에서 소비하는 전력이나 전자기장 등의 물리적인 특성을 이용하여 비밀 키 또는 데이터를 분석하는 공격 방법이다. 따라서 부채널 공격에 대한 연구 및 이를 방어하기 위한 연구가 진행되었으며, 그 결과로 센서 노드에서 NesC로 구현된 DES,



[그림 12] 부채널 공격 시스템 및 DPA 분석 시뮬레이터

ARIA, AES 암호에 대한 DPA 분석 및 이에 대한 방지 기법, 센서 노드에서 NesC로 구현된 ECC 공개키 암호에 대한 SPA 분석 및 이에 대한 방지 기법 그리고 저전력 하드웨어 보안 모듈에 대한 SPA, DPA 분석 등의 결과가 도출되었다. [그림 12]는 부채널 공격 중 하나인 DPA 분석을 통한 비밀 키 검출을 수행하는 시뮬레이터 그림이다.

Ⅳ. 결 론

RFID/USN 기술은 유비쿼터스 세상을 향한 핵심

기술로서 그동안 수년간의 연구가 진행되었음에도 불구하고 피부에 와닿는 응용 서비스가 등장하지 못하고 있는 저변에는 보안 및 프라이버시 문제가 해결되지 못한 상황도 포함된다. RFID/USN 보안 문제를 해결하기 위하여 많은 분석 자료들이 RFID 보안 요구사항 또는 USN 보안 요구사항을 일목요연하게 정리하고 있으며, 일부 자료에서는 기술적 접근 방안도 제시하고 있다.

그러나 보다 구체적이고 상용화 가능한 수준의 연구 결과 정리가 미흡하였기 때문에 본 고에서는 단순한 보안 요구사항 분석과 아이디어 차원의 기술 소개를 넘어 응용 서비스를 염두에 둔 RFID/USN 보안 기술의 연구 결과를 소개하고자 하였다. RFID/USN 환경에 대한 보안 요구사항과 개별 요구사항을 만족하는 단편적인 기술이 일차원적인 일대일 연결을 통해 한꺼번에 해결되는 것이 아니기 때문에 본 고에서 소개한 개발 결과들은 요소 구현 기술, 플랫폼 구축 기술, 보안 응용 서비스 기술 등이 다양하게 열거되는 구성이 되었다.

RFID/USN 기술은 그 활용 범위가 다양하기 때문에 단편적인 기술로 모든 RFID/USN 보안 문제를 해결하려고 할 것이 아니라 분야별, 대상별 또는 수직적, 수평적인 환경을 모두 고려하여 산업체, 연구소, 학계, 정부기관이 모두 참여하여 종합 대책을 수립하고, 특성에 적합한 해결책을 찾고자 노력해야 할 것이다. 본 고에서 소개한 기술 개발 결과, 내용이 향후 다양한 응용 서비스 구축시 보안 대책을 수립할 때 참조되기를 기대한다.

참 고 문 헌

[1] Junko Yoshida, Euro bank notes to embed RFID chips by 2005, http://www.eetimes.com/story/OEG20011219S0016, Dec. 2001.

[2] Kim Yong-Young, Radio ID chips may track bank-notes, http://news.com.com/2100-1017-1009155.html. May 2003.

[3] 정병호, 강유성, 김신효, 정교일, 양대헌, "RFID/USN 환경에서의 정보보호 소고", 한국통신학회지, 21(6), pp. 102-115, 2004년 6월.

[4] 김신효, 강유성, 정병호, 정교일, "u-센서 네트워크 보안 기술 동향", 전자통신동향분석, 20(1), pp. 93-99, 2005년 2월.

[5] 이병길, 강유성, 박남제, 최두호, 김호원, 정교일, "능동 및 모바일 RFID 서비스 환경에서의 정보보호 기술", 15(3), pp. 40-47, 2005년 6월.

[6] 오경희, 김호원, "RFID 환경에서의 프라이버시 보호 기술", 한국통신학회지, 2(9), pp. 103-112, 2006년 9월.

[7] 강유성, 김호원, 정교일, "화물 컨테이너 보호를 위한 RFID 보안장치 기술 동향", 한국통신학회지, 24(11), pp. 43-50, 2007년 11월.

[8] 강유성, 이석준, 김호원, "RFID 기반 유가증권 보호 기술 동향", 전자통신동향분석, 22(6), pp. 150-157, 2007년 12월.

[9] 박남제, 강유성, "모바일 RFID 보안기술", TTA Journal, no. 115, pp. 108-114, 2008년 2월.

[10] 김태성, 김호원, "RFID 시스템의 미들웨어를 위한 접근제어", 한국방송공학회 동계 학술대회, pp. 201-204, 2008년 2월.

[11] 이석준, 오경희, 김호원, 정병호, "USN 공격 기법 및 보안 기술 동향", 한국인터넷정보학회지, 9(1), pp. 34-43, 2008년 3월.

[12] 김호원, 이석준, 오경희, "센서네트워크 보안 기술 개발 동향", 한국정보보호학회지, 18(2), pp. 33-39, 2008년 4월.

[13] 강유성, 최두호, 김호원, "모바일 RFID 보안기술 표준화 동향 및 표준화 추진 전략", 전자통신동향분석, 23(2), pp. 142-152, 2008년 4월.

[14] 이신경, 이해동, 정교일, 최두호, "안전한 USN을

위한 정보보호 기술 동향", 전자통신동향분석, 23 (4), pp. 72-79, 2008년 8월.
[15] 최두호, 박남제, 강유성, 김태성, 김주한, "RFID 보안 및 주요 응용 서비스", 월간 정보보호 21C, 게제 예정, 2008년.
[16] 한국전자통신연구원 RFID/USN보안연구팀, "안전한 유비쿼터스 세상을 위한 RFID & USN 보안 기술", RFID/USN KOREA 2008 국제전시회 홍보책자, 2008년 11월.

≡ 필자소개 ≡

조 현 숙

1979년: 전남대학교 수학교육과 (이학사)
1989년: 충북대학교 전산학과 (이학석사)
2001년: 충북대학교 전산학과 (이학박사)
2000년~2001년: 인터넷안전마크위원회 위원(정통부)
2000년~2005년: 대한여성과학기술인회 부회장
2001년~2004년: 한국통신학회 이사 및 정보통신여성위원장
2001년~2003년: 국가과학기술위원회 연구개발전문위원
2002년~2007년: 국가연구개발사업 평가위원(과학기술부)
2005년~2006년: 한국통신학회 부회장
1982년~현재: 한국전자통신연구원 정보보호연구본부장
현재: 민군겸용기술위원회 위원(과학기술부)
서울시 정보화추진위원회 위원(서울시)
정부통합전산센터추진위원회 위원(정통부)
국방부자체평가위원회 위원
과기부 미래전략자문위원회 위원
산업기술보호전문위원(산자부)
한국정보보호학회 이사
여성벤처인협회 자문위원
[주 관심분야] 산업보안, 콘텐츠보안, 시스템보안

정 교 일

1981년: 한양대학교 전자공학과 (공학사)
1983년: 한양대학교 전자공학과 (공학석사)
1997년: 한양대학교 전자공학과 (공학박사)
1982년~현재: 한국전자통신연구원 책임연구원, 마케팅기술위원
현재: 국가정보원 정보보호시스템 인증위원
ITU-T(국제전기통신연합) SG17 연구위원
TTA(한국정보통신기술협회) 국제표준화전문가
한국전자지불산업협회 IC카드포럼 의장
Asia IC Forum 표준화위원장
행정자치부 전자주민증 자문위원
ISO TC215 전문위원
TTA(한국정보통신기술협회) TC1 의장
IC카드연구센터 전자여권표준기술개발단 단장
모바일RFID포럼 정보보호분과위원장
홈네트워크시큐리티포럼 의장
대검찰청 디지털수사 자문위원
대한전자공학회 상임이사
한국정보보호학회 부회장
한국디지털포렌식학회 부회장
한국인터넷정보학회 이사
[주 관심분야] 정보보호, Biometrics, 국가기반보호, 신호처리

최 두 호

1994년: 성균관대학교 수학과 (이학사)
1996년: 한국과학기술원 수학과 (이학석사)
2002년: 한국과학기술원 수학과 (이학박사)
2002년~2007년: 한국전자통신연구원 선임연구원, 팀장
2006년 9월~현재: ITU-T X.1171(X.nidsec-1) 에디터
[주 관심분야] RFID/USN, 정보보호, 위상수학

강 유 성

1997년: 전남대학교 전자공학과 (공학사)
1999년: 전남대학교 전자공학과 (공학석사)
2005년~현재: 한국과학기술원 전자전산학부 전기및전자공학 전공 박사과정
1999년~현재: 한국전자통신연구원 선임연구원
[주 관심분야] RFID/USN, 정보보호, 통신시스템