RFID/USN 정보보호 기술

김광조 | 한국정보통신대학교(ICU) 공학부 교수

유비쿼터스 환경을 완성하기 위한 RFID/USN은 전파식별(RFID) 칩의 저가화와 소형화, 지능화 추세에 따라 조달, 국방, 우편, 교육, 문화, 엔터테인먼트, 교통 및 환경 등의 다양한 분야에 적용되고 결국 지능형 유비쿼터스 센서 네트워크(USN)로 진화될 것이다. 이에 유비쿼터스 강국으로 도약하기 위해 지금까지 이룩한 IT 강국으로의 노하우를 접목하고 우리의 핵심 역량을 집중시킬 수 있도록 하고, RFID/USN 기술 및 시장동향을 살펴봄으로써 세계시장 개척을 위한 초석이 되고자 한다(편집자주).

RFID/USN 특집 순서 ●●●●
- □ RFID 기술 및 표준화 동향
- □ RFID 산업동향 및 전망
- □ RFID 시범사업 현황 및 추진방향
- □ 멀티코드 지원 객체 검색 시스템
- ■ **RFID/USN 정보보호 기술**
- □ 유비쿼터스 센서 네트워킹 기술

요약

자동화되고 손쉽게 정보를 얻을 수 있는 RFID/USN 환경에서는 보안에 심각한 위협을 가져오며, 반대로 RFID 등의 제약된 자원에 의해 기존 정보보호 기법을 그대로 사용하기 어렵게 된다. 따라서 새로운 경량화 정보보호 기법이 연구되고 있으며, 또한 QoSS(Quality of Security Service)를 통해 제약된 자원의 활용도를 최대화 시키고자 하는 연구가 진행 중이다. 본고에서는 이러한 연구 동향에 대해 소개한다.

I. 서론

RFID/USN(Radio Frequency Identification/Ubiquitous Sensor Network)란 필요한 모든 것(곳)에 RFID를 부착하고 이를 통하여 사물의 인식정보를 기본으로 주변의 모든 정보를 탐지하여 이를 실시간으로 네트워크에 연결하여 정보를 관리하는 것을 말하는 것으로 먼저 인식정보를 제공하는 RFID를 중심으로 발전하고 이에 감지기능이 추가되고 이들간의 네트워크가 구축되는 USN 형태로 발전할 것으로 전망되고 있다. 그러나 이러한 자동화되고 손쉽게 정보를 얻을 수 있는 환경에서는 보안에 있어 심각한 결과를 초래할 수 있다.

RFID 태그의 사용에 있어서 사용자 개인의 프라이버시 문제(위치정보 또는 구매이력 노출 등)가 심각하게 인식하여야 하며, RFID 태그의 ID는 쉽게 식별되며, 태그는 사용자가 알지 못하는 사이에 모든 리더에게 자동적으로 응답한다. 이러한 우려들이 RFID의 상용화에 걸림돌이 되며, 성공적인 산업화를 위해서는 제반 프라이버시 문제를 해결해야 하는 것이 선결 과제로 되고 있다.

또한, 현재 단계에서 USN 환경에서의 공격의 형태나 공격자에 대한 명확한 추정은 아직까지 센서 네트워크 자체가 미성숙한 단계에 있기 때문에 어렵지만,

현재의 공격보다는 광범위한 범위와 대상을 목표로 하는 것으로 예상되고 있다. USN 환경에서의 공격(침해) 대상은 기존 환경의 컴퓨터에 저장된 정보 또는 통신 정보만이 아닌, 사물이나 신체 등 개인의 모든 정보가 되며 공격 범위는 기존의 개인의 컴퓨터에 국한되지 않고, 개인의 사적인 모든 공간이 된다. 따라서 공격에 대한 피해 범위는 이러한 공격범위 확대 및 공격의 용이함에 의해 매우 확대될 것이다.

본고를 통하여 현재 RFID/USN의 보안 이슈를 소개하고 그 문제들의 해결 방안을 위한 연구 동향들을 살펴보기로 한다. 본고는 다음과 같이 구성되어있다. Ⅱ장에서는 RFID/USN의 보안 문제점 및 보안 목표에 관하여 살펴보고 Ⅲ장에서는 RFID 관련 보안문제 해결을 위한 연구동향을 살펴본다. Ⅳ장에서는 국내의 RFID/USN 연구활동을 간략히 살펴본 후, 끝으로 Ⅴ장에서 결론 및 향후 연구방향을 제시한다.

Ⅱ. RFID/USN의 보안 문제점 및 목표

1. RFID 보안 문제

RFID의 보안 문제는 다음과 같이 정리된다[5][6][8][9].

- 도청 : RFID 시스템은 바코드 시스템과 달리, 효율성을 높이기 위해 수 미터의 범위 내에서도 리더와 태그간에 통신이 가능하도록 되어 있다. 이러한 특징은 악의적인 사용에 의해 보안 문제점을 노출시킨다. 공격자가 리더를 갖고 태그를 스캐닝하는 적극적 공격과, 리더와 태그간 통신을 RF 수신하는 수동적 공격이 있다.
- 트래픽 분석 : 리더와 태그간 통신중 트래픽 분석을 통한 위협이 존재한다. 공격자가 어떤 특정 지역 내지 특정 태그에서 리더와 태그간의 트래픽을 분석할 수 있다면, 그 지역에서 어느 정도의 트래픽이 존재하는지, 어느 정도의 물품이 존재하고, 빠져나가는지에 대해서 알 수 있다. 또한, 트래픽 분석을 통해서 위치 추적이 가능하다. 아무리 패킷내용이 암호화되어 있을지라도 같은 비트(bit) 패턴의 태그가 이동하는 것을 알 수 있기 때문에 개인의 움직임을 알 수 있다. 더 나아가 개인의 신상정보까지 노출될 수 있는 위험이 존재한다.
- 위조 : 태그에는 메모리에 데이터 항목이 존재한다. 이 항목은 항상 공격자의 대상이 될 수 있다. 공격자는 데이터 항목을 지우거나 대신할 수 있는 방법을 사용할 수 있다. 이것은 리더와 태그간의 통신에 잘못된 데이터를 서로 교환가능하게 되므로 치명적인 위험이 존재한다. 또한, 리더의 위조는 태그의 데이터 항목을 읽히는 위험이 있다.
- 서비스 거부(DoS, Denial of Service) 공격 : 리더가 태그간에 질의와 반응의 메커니즘이 존재한다. 이러한 특징을 이용하여 공격자가 리더를 가지고 수많은 질의를 리더 및 태그에게 보낸다면 리더와 태그는 많은 질의에 대해서 일일이 반응해야 된다. 이는 너무 많은 계산이 요구되고, 리더와 태그가 정상적인 기능을 못하게 만드는 결과를 초래한다. 서비스 거부 공격은 RFID 시스템이 작동을 못하도록 하는 위협이다.

2. 보안 요구 사항

위에서 살펴본 RFID/USN 보안 문제들을 해결하기 위하여 RFID는 RF 태그와 보유자 및 리더 등 구성 환경에 대해 다음과 같은 사항을 고려해 보안 목표를 설

정 [7] 할 수 있고, USN의 경우 서비스되는 상용 시스템이 존재하지 않아 보안 요구 사항은 논의 중에 있다.

- 태그는 태그 소유자의 프라이버시를 손상 또는 위협하지 말아야만 한다.
- 정보는 인증이 되지 않은 리더로 유출이 되서는 안되며, 태그와 그 소유자 사이에 긴 기간 동안의 추적(long-term tracking)이 불가능해야만 한다.
- 추적을 막기 위해서 소유자는 그들이 보유한 태그를 감지하거나 사용불가로 만들 수 있어야만 한다.
- 공개적으로 사용 가능한 태그의 결과는 랜덤화 되거나 태그와 소유자 사이의 장기간 관련성(long-term association)을 회피하기 위해 쉽게 수정이 가능해야만 한다.
- 비공개적인 태그의 내용은 접근제한기법(access control)에 의해 질의채널(interrogation channel)이 안전하지 않다고 예상된다면 암호화 되어야 한다.
- 태그와 리더는 모두 상호 신뢰해야만 한다.
- 태그와 리더 어느 쪽이든 스푸핑이 어려워야 한다.
- 접근제한 기법의 제공 이외에도 태그와 리더 사이에는 상호인증(mutual authentication)이 신뢰의 척도로서 제공된다 [5].
- 전원의 중단이 프로토콜을 손상시키거나 가로채기공격(hijack) 시도에 대한 창구를 열어놓지 말아야만 한다.
- 태그와 리더 모두 재생공격(replay attack) 및 공격자 중간 공격(man-in-the-middle attack)에 저항력이 있어야만 한다.

Ⅲ. RFID 보안문제 해결을 위한 연구동향

RFID/USN 환경에 적합한 공개키 알고리즘의 하드웨어적인 구현은, 2004년 Rabin, NTRU, ECC등의 공개키 알고리즘에 대한 구현 결과 제시에 의해 NTRU의 경우 20μW의 저전력에 3000개의 게이트만 필요하며, 경량화 된 센서 노드에 탑재 가능한 것으로 알려져 있다[15]. 그러나 현재는 기존의 알고리즘을 개선하여 사용하고 있으며 향후에는 새로운 알고리즘 개발이 요구된다.

USN 환경의 그룹키 관리의 경우 대칭키 방식은 RFID의 경우 리더와 태그간의 키를 공유해야 하며, 각 태그마다의 유일한 키를 관리하는 등의 많은 계산양 때문에 사용하기 어려우며, 또한 키의 유출에 의한 태그 무력화, 또한 장기간의 사용에 대한 노출 가능성 증가 등의 문제가 있다. 또한, 센서 노드에 암호키를 탑재하는 방식은 에칭(etching), 탐침, TEMPEST 등의 물리적 공격에 취약하며 암호키의 노출 가능성이 있다. 버클리 대학의 SmartDust 프로젝트에서 채택한 센서 네트워크의 보안 프로토콜인 SPIN(Security Protocols for Sensor Network)[16]은 μTESLA와 SNEP로 구성되어 있으며 메시지 인증, 무결성, 기밀성, 적시성 등의 서비스를 제공하고 있다. 랜덤키 사전분배방식은 키 DB을 선택하고 무작위로 키를 선택하여 센서 노드에 할당하며, 두 개의 노드는 자신의 키 DB을 탐색하여 상대방이 같은 공통키를 소유하고 있으면 이 키를 세션키로 사용하는 방식이다.

RFID 시스템에서 사용자 프라이버시의 보호를 위한 많은 연구들이 진행되어 오고 있다. 이 절에서는 현재 진행되어 왔던 연구결과 중, Kill 명령어의 접근법, Blocker 태그 기법[4], 해쉬-락(Hash-Lock) 기법[10], 랜더마이즈드 해쉬-락 기법[10], XOR 기반 원타임 패드 기법[1], 외부 재암호화 기법[3], 해쉬 체인

(Hash-Chain) 기반 기법[13] 등이 있다.

RFID는 USN에 비해 좀 더 경량화되고, 저비용의 기법이 요구된다[2]. 따라서, 위에 제시된 기법들은 용도에 따라 선택적으로 사용되는 것을 방법으로 하며, 성능 및 용도에 따라 사용되는 기법들에 대한 정량적인 구분을 위해 보안서비스를 미리 정의된 기준으로 평가하여 나타나는 보안서비스 품질인 QoSS(Quality of Security Service) 및 등급 분석을 하게 된다[12]. QoSS를 통해 다음과 같은 기대효과를 얻을 수 있다.

- USN 환경내 개별 개체의 상이한 보안 요구사항에 부합되는 다양한 등급의 보안서비스 제공 가능
- 보안을 통해 효율적인 자원의 스케줄링으로 장비 효율성 증가
- 상황에 따른 선택으로 개체의 서비스 사용비용 감소
- 기존 QoS가 제공할 수 있는 가용성, 예측 가능성, 효율성을 더욱 향상시키고, 더불어 보안성을 제공

〈표 1〉은 RFID 시스템에서 제공하고자 하는 보안 서비스 및 보안 서비스별 정보보호 요구사항을 정의하고 있다. 이러한 서비스에 대한 요구 사항에 맞추기 위해 가변 보안이 사용된다. 〈표 2〉의 예와 같이 보안 서비스별 적절한 보안 메커니즘을 구성한다. 이에 대해 〈표 3〉과 같은 태그 분류와 함께, 제공하고자 하는 보안 서비스에 따라 제공되는 보안도구를 통해, 사용자(USN의 개체)는 적절한 보안수준을 선택할 수 있게 된다.

QoSS를 통해 RFID/USN 환경에서 사용자의 선택적인 보안 요구사항을 실제 메커니즘으로 할당하는 할당표를 작성하고, 이를 보안 정책 서버나 RMS (Resource Management System) 내부 관리 테이블

〈표 1〉 보안 서비스의 정의 [14]

보안서비스	요구사항
기밀성	• 태그 유저는 권한이 있는 유저에 의해서만 태그가 읽히길 요구하며, 태그 유저는 태그에 쓰여진 데이터를 암호화 할 수 있어야 한다. • 태그는 태그의 설계 또는 구조의 간섭없이 암호화된 데이터를 읽고 쓸 수 있어야 한다. 이러한 특성은 유저가 선택할 수 있어야 한다.
익명성	• 태그 내의 정보 또는 정보와 별도의 태그 식별 정보에 대한 익명성이 보장되어야 한다. • 정보를 이용한 사물 및 개인에 대한 위치추적, 경로추적 및 감시가 이루어 지지 않도록 인증된 적법한 사용자가 제어할 수 있다.
무결성	• 태그는 잠김 데이터를 알려진 데이터의 변경이나 삭제를 막을 수 있어야 한다. • 태그 제조사들은 사용자에 관련되지 않는 제조사와 관련된 데이터의 저장소와 식별에 대한 태그 데이터를 잠글 수 있는 기능을 가져야 한다.
인증성	• 태그 데이터의 저장소와 전송 프로토콜은 태그 데이터를 읽기에 앞서 결의자의 권한에 대한 인증의 요구에 대해서 사용자가 제어 가능한 옵션을 제공한다. • 태그 아이디를 읽는 것만으로 인증을 요구하지 않는다.
침해대응성	• 서비스 거부공격 대응 • 시스템 보호 제공 • 네트워크 보호 제공 • 해킹, 바이러스, 침입 공격 등에 대한 대응

〈표 2〉 보안 서비스 및 태그 유형별 보안 도구(예시)

보안 서비스	공격 유형		위협 사례	보안 도구										
보안 서비스	능동	수동		Hash	대칭키	비대칭키	전자서명	인증 프로토콜	키 관리	기능정지		기타	물리적 보안
										영구	일시		
기밀성		○	도청 가로채기		○	○			○	○	○		○
익명성	○	○	트래픽 분석 태그추적 스캐닝	○		○			○	○	○	재암호화, 난수 생성 등	
무결성	○		내용변조	○	○	○	○		○			DES-CBC 등	○
인증성	○	○	코드위장 코드변조 인증부인 순서수정	○	○	○	○	○	○			원타임 패드, DES-CBC, 상호 인증 등	
DoS 방지	○	○	DoS 시간수정	○	○	○	○	○	○			방화벽, IDS, IPSec 등	

로 보관하여 사용자가 요청시 해당 메커니즘을 수행하도록 한다. 〈표 3〉과 〈표 4〉는 RFID 시스템에서 제공하고자 하는 보안 서비스에 따라서 임의 등급의 태그를 선택했을 경우 제공 가능한 서비스의 등급을 분류하고, 고려되는 가변 보안요소(Variable Security Factor)로써 보안 벡터의 암호학적 보안 도구의 상세 할당을 보여 준다. 실제 시스템 구성에서는 각각에 맞는 설정이 필요하다.

〈표 3〉 EPC Global의 태그 등급

규격		방식	메모리	주요 특징
0	EPC0	수동	읽기 전용 EPC:64bit	사물인식 Kill 코드 24bit
1	EPC1	수동	읽기 전용(한번 입력 가능) EPC : 64bit	사물인식 Password 8비트
2	EPC2	수동 능동	읽기/쓰기	Data Logging
3	Sensor Tag	능동	읽기/쓰기	환경정보 센싱
4	Comm. Tag	능동	읽기/쓰기	Ad-Hoc 네트워킹
5	Reader형 Tag	능동	읽기/쓰기	리더 기능을 갖는 태그

〈표 4〉 보안 선택 범위별 할당(예시)

보안서비스	태그 유형	보안 요구 수준		
		하	중	고
기밀성	0	무결성	Kill Command	Blocker Tag
	1	Kill Command	Blocker Tag	Blocker Tag
	2	Blocker Tag	DES-64	DES-64
	3	DES-64	DES-64	AES-128
	4	AES-128	AES-128	AES-128/RSA-1024
	5	AES-256/RSA-2048	AES-256/RSA-2048	AES-256/RSA-2048

Ⅳ. 국내 RFID/USN 보안기술 연구 동향

국내에서는 TTA가 활동을 지원하는 USN표준화포럼 내에 4개의 분과(기술, 응용, 네트워크, 정보보호)가 구성되어 있으며, 이중 정보보호 분과는 RFID 보안 W/G, USN 보안 W/G의 2개의 W/G로 구성되어 있다. RFID 보안 W/G은 RFID 태그 등 초경량 환경에 적합한 암호 프리미티브(블럭암호, 스트림 암호, 해쉬함수), RFID 태그/리더간 상호인증을 위한 경량화된 인증기술, RFID 사용자의 개인정보 및 위치정보 프라이버시 침해방지를 위한 기술을 개발하여 국내표준 제정 및 국제표준을 제안한다. USN 보안 W/G은 USN 환경에서의 라우팅 프로토콜 보호 메커니즘, Ad-hoc 네트워크, USN 등에서의 인증을 위한 기술을 마련하여 국내표준 제정 및 국제 표준을 제안한다[11].

Ⅴ. 결론 및 향후 전망

RFID/USN의 정보 활용의 유용성은 반대급부로 정보의 노출이라는 보안 취약점을 야기시키며, RFID/USN 환경에서의 정보노출은 기존의 컴퓨터 정보의 유출만이 아닌 위치, 건강상태, 활동방식 등 우리의 전반적인 생활정보의 유출을 의미하게 된다.

RFID 관련 프라이버시 보호에 대한 핵심 연구주제 중 하나는 낮은 비용으로 암호화 프로세스가 가능한 RFID를 개발하고 구현하는 것이다. 여기에는 해쉬함수, 난수 생성기 그리고 대칭키 암호, 비대칭키 암호(공개키 암호) 등의 경량화 연구가 포함된다. 최근 Crypto2004 암호학회에서는 RFID 프라이버시 보호용으로 널리 알려진 해쉬함수(Haval, MD4, MD5) 등이 해독되는 사례[17]가 발표되어 새로운 해쉬함수의 설계가 요구된다.

현재 RFID의 보안 요구 사항으로 태그 정보의 보호, 임의의 태그에 대한 추적방지 등이 제시되고 있다. 가장 최근에 연구되고 있는 프라이버시 보호를 위한 해쉬체인 기법 등의 연구는 RFID의 보안 요구사항을 어느 정도 만족하고 있다. 그러나 연산량의 줄이는 방법, 초경량 해쉬함수의 구현문제 사항들이 더욱 연구되어야만 한다. 또한, 재기록이 가능한 태그(rewritable tag)에 대한 무결성 보장 등도 연구주제로 진행되고 있다.

아직까지는 표준화된 RFID의 보안 요구사항에 대한 정의 및 정형화된 기법은 존재하지 않고 있다. 따라서 보안에 대한 기술적 접근과 더불어 RFID 보안 연

구에 있어 표준화 작업도 다각적으로 전개될 전망이다. 또한, RFID/USN의 정보보호는 현재 USN의 미성숙한 단계에서는 가시적으로 정의하기 어렵다. 그러나 매우 가변적인 네트워크에 대한 보호를 위한 라우팅 보호 프로토콜, 부채널 공격에 대한 RFID 칩 보안 기술 등의 연구가 활발하게 진행되고 있다.

참고문헌

[1] A. Juels, "Privacy and authentication in low-cost RFID tags", In submission, Available at http://www.rsasecurity.com/rsalabs/staff/bios/ajuels/

[2] A. Juels, "Minimalist Cryptography for Low-Cost RFID Tags", Available at http://www.rsasecurity.com/rsalabs/staff/bios/ajuels/publications/index.html

[3] A. Juels, R. Pappu, "Squealing Euros: Privacy protection in RFID-Enabled Banknotes", In Proceedings of Financial Cryptography FC'03, 2003.

[4] A. Juels, R.L. Rivest and M. Szydlo, "The Blocker Tag : Selective Blocking of RFID Tags for Consumer Privacy", In Proceedings of 10th ACM Conference on Computer and Communications Security (CCS 2003), Oct. 2003.

[5] K. Romer, T. Schoch, F. Mattern, and T. Dubendorfer, "Smart Identification Frameworks for Ubiquitous Computing Applications", PerCom03, pp.253-262, 2003. 3.

[6] R.L. Rivest, "Approaches to RFID Privacy", RSA Japan Conference 2003

[7] S. Sarma, S. Weis, and D. Engels, "RFID Systems, Security & Privacy Implications", Auto-ID Center. White paper. 2002. 11. 1.

[8] S. Sarma, S. Weis, and D. Engels, "Radio-Frequency Identification : Security Risks and Challenges", CryptoBytes, 2003.

[9] S. Weis, "Security and Privacy in Radio-Frequency Identification Devices", Master's thesis, MIT. 2003.

[10] S. Weis, S. Sarma, R. Rivest, and D. Engels, "Security and privacy aspects of low-cost radio frequency identification systems", In Proceedings of the 1st Security in Pervasive Computing, 2003.

[11] RFID/USN표준화포럼, 2004.

[12] 함우석 외 "QoSS의 연구 동향과 적용" 2002년도 한국정보보호학회 학술대회, pp. 352-355, 항공대, 2002. 11. 16, 한국.

[13] M. Ohkubo, K. Suzuki, and S. Kinoshita, "Forward-secure RFID Privacy Protection using Hash Chain", NTT Laboratorie, 2003.

[14] ISO/WD 17367, AutoID.

[15] G. Gaubatz, J. Kaps, B. Sunar, "Public Keys Cryptography in Sensor Networks - Revisited", to appear in the Proceedings of the 1st European Workshop on Security in Ad-Hoc and Sensor Networks (ESAS 2004).

[16] A. Perrig, et al., "SPINS : Security Protocols for Sensor Networks", Mobile

Computing and Networking 2001, Rome, Italy.

[17] Xiaoyun Wang and Xuejia Lai, "Collisions for Hash Functions MD4, MD5, HAVAL-128 and RIPEMD", Crypto2004, Rump Session, UCSB, 2004. USA.