主題

RFID/USN 환경에서의 정보보호 소고

한국전자통신연구원 정보보호연구단 정 병 호, 강 유 성, 김 신 효, 정 교 일
인하대학교 정보통신대학원 양 대 헌

차 례

Ⅰ. 서 론
Ⅱ. RFID/USN 네트워크 개요
Ⅲ. RFID/USN 정보보호
Ⅳ. 결론 및 시사점

요 약

IT 산업의 발전과 국가의 부 창출을 위하여 정부는 'IT 839 전략'에 따라 2010년까지 BcN·USN·IPv6 3대 IT 통신 인프라의 전국 상용망 구축을 추진하고 있다. u-센서 네트워크(USN)는 모든 사물에 전자태그(RFID)를 부착, 인터넷에 연결하여 정보를 인식 및 관리하는 네트워크를 말한다. USN 서비스는 RFID, 텔레메틱스, 그리고 지능형홈 분야 등에서 유통, 물류를 비롯하여 교통, 농축산물관리, 조달, 환경, 의료등 다양한 산업 전반에서 창출될 것으로 보인다. RFID 태그는 전자칩을 부착하고 무선통신 기술을 이용하여 리더와 통신한다.

본 고에서는 정보보호 관점에서 RFID/USN 네트워크가 인터넷 수준의 보안 서비스를 제공하기 위해서는 어떠한 점이 고려되어야하는지를 정리하였다. 현재 사회적으로 이슈가 되고 있는 RFID 정보보호 문제는 주로 프라이버시 측면에서 논의되어 왔다. 그러나 RFID/USN은 대규모의 RFID 태그(사물)들이 단말이 되고, IPV6, BcN 망과 연동되며, 새로이 구축되어야하는 네트워크임에도 불구하고, 아직 네트워크/서비스 정보보호 관점에서 고려해야할 것들이 무엇인가에 대한 논의가 활발하지 못했던 것으로 보인다.

이러한 논지를 가지고 본 고에서는 현재 논의되고 있는 RFID 정보보호 기술의 동향을 분석하고, 네트워크 정보보호 관점에서 RFID/USN 환경에 추가되어야 할 기술적 요구사항들을 정리해 보았다.

Ⅰ. 서 론

1988년 미국 제록스 팰로앨토 연구소의 마크

와이저 소장이 처음 이 용어를 사용함으로써 유명해진 유비쿼터스(Ubiquitous)란 단어는 라틴어로 '언제 어디서나 있는'이라는 의미로 시간과 장소에 구애 받지 않는 컴퓨팅 환경을 의미한다.

컴퓨팅 역사의 첫 번째 패러다임이 메인 프레임이었고 두 번째 패러다임은 PC였다. 현재 다가오고 있는 세 번째 패러다임은 과거 '일대다', '일대일'의 관계를 뛰어 넘어 컴퓨터와 인간의 관계가 '다대일'로 인간을 위해 존재하는 유비쿼터스 컴퓨팅 환경이 될 것이다. 현실세계를 모방하여 구성되었던 사이버공간이 아닌 실제에 컴퓨팅 환경이 구현되는 것이며, 이러한 변화의 첫걸음은 RFID 시스템으로부터 시작될 것으로 보인다.

RFID(Radio Frequency IDentification) 시스템은 그 편리함과 잠재적으로 큰 시장성에도 불구하고 보안 기능의 구현이 없을 경우 RFID의 정보가 쉽게 도청당할 가능성이 있기 때문에 프라이버시 문제가 이슈화되었던 것이 사실이다. 2005년부터 유럽 중앙은행은 유럽에서 사용하는 유로 화폐에 RFID 태그를 내장한다고 밝히고 있다[1]. 만약의 경우이긴 하지만 아무런 정보보호 대책을 세우지 않는다면 악의적인 사람이 길거리에 지나가는 사람들을 모니터링하여 누가 현금을 더 많이 가지고 다니는지 알 수 있으며 그는 범죄의 피해자가 될 수도 있다. 다른 예로 들 수 있는 것은 개인 정보에 관한 문제이다. 만약, 개인이 보유하고 있는 물품에 붙인 태그가 악의적인 사람의 물음에 자신의 정보를 가르쳐 준다면 이는 심각한 사회 문제가 될 것이다.

또한 RFID 태그의 정보노출 취약성뿐만 아니라 RFID/USN 네트워크의 DoS(Denial of Service) 취약성도 심각한 문제를 야기 시킬 수 있다. 만일 악의적인 공격자의 침입에 의해 네트워크 가용성이 훼손당한다거나 또는 네트워크로 유입되는 태그 정보의 비정상적인 폭주를 고려하지 못하여 DoS 공격에 취약하게 설계된다면 이는 네트워크 인프라 전체에게 영향을 끼치는 심각한 정보보호 결함이 될 것이다.

본 고는 RFID/USN 정보보호 기술의 현재 동향 분석과 추가 요구사항 제시를 위하여 다음과 같은 구성을 갖는다. Ⅱ장에서는 RFID/USN의 소개와 초기 활용 형태로 예상되는 EPCglobal 네트워크의 개요를 간략하게 설명한다. Ⅲ장에서는 RFID 기반의 EPCglobal 네트워크 구성 시 예상되는 정보보호 필요성을 분석하고, 이를 극복하기 위해 제시되고 있는 정보보호 요구사항 및 현재의 기술 동향을 항목별로 분석하며, 또한 네트워크 보호 관점에서 RFID/USN 환경에 추가되어야 할 기술적 요구사항을 제시한다. 끝으로 Ⅳ장에서 RFID/USN 환경에서의 정보보호 기술이 가지는 의미를 밝히면서 결론을 맺는다.

Ⅱ. RFID/USN 네트워크 개요

1. RFID/USN 소개

RFID란 "전자칩을 부착하고 무선통신 기술을 이용하여 사물의 정보를 확인하고, 주변 상황정보를 감지하는 센서 기술"로 정의할 수 있다[2].

USN이란 "필요한 모든 것(사물)에 전자태그(RFID)를 부착하고 이를 통하여 사물의 인식정보를 기본으로 주변의 환경정보(온도, 습도, 오염정보, 균열정보 등)까지 탐지하여 이를 실시간으로 네트워크에 연결하여 정보를 관리하는 것"을 말하는 것으로 궁극적으로 모든 사물에 컴퓨팅 및 커뮤니케이션 기능을 부여하여 Anytime, Anywhere, Anything 통신이 가능한 환경을 구현하기 위한 것이다. USN 구축 기술의 발전 단계는 먼저 2005년까지 제 1단계로 인식정보를 제공하는 RFID 태그를 중심으로 발전하고, 제 2단계로 2007년경 센싱 기능이 추가될 것으로 예견

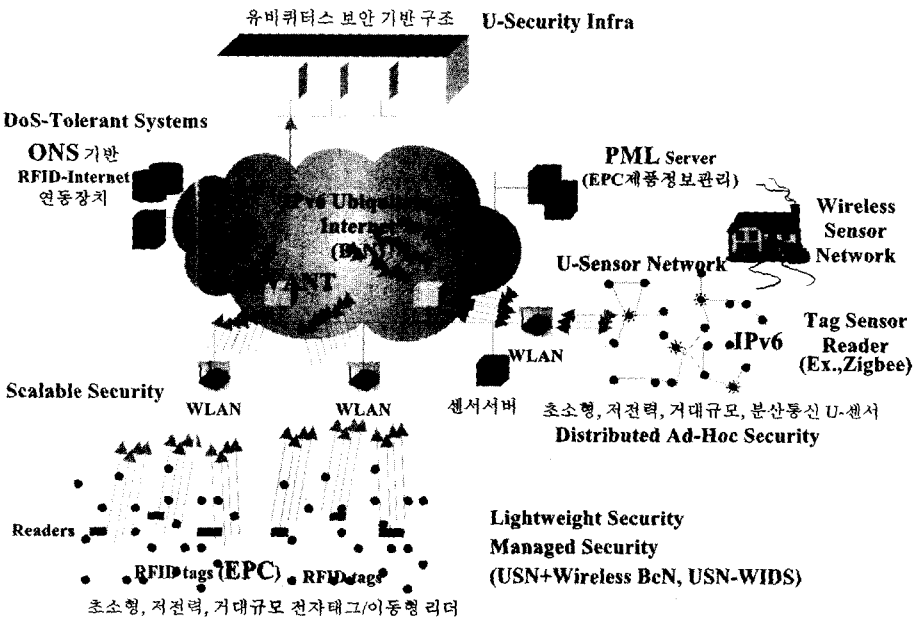

그림 1. RFID/USN 연동 인터넷 개념도

되며, 제 3단계 2010년 즈음에는 다기능 센싱 태그에 의한 상황인지처리 수준으로 진화하고 2010년 이후에는 개체 간 통신기능을 갖춘 지능형 네트워크로 발전될 전망이다[3].

2. EPCglobal 네트워크 개요

EPCglobal 네트워크는 RFID/USN 구축의 1단계에 해당하는 네트워크[1]의 모습으로 EPC 클래스 1과 클래스 2 형식의 태그를 부착한 RFID 사물이 단말로 인식되는 네트워크이다(표 1 참조).

IP 주소가 인터넷에 연결된 컴퓨터의 유일성을 나타낼 수 있는 정보 인 것처럼, RFID 태그는 자신의 유일성을 나타내기 위해 EPC(Electronic Product Code) 코드를 사용한다. EPC 코드는 "0011 0101" 값의 헤더를 가지며, 28 bits 관리자 번호(General Manager Number), 24 bits 물품 클래스(Object Class), 그리고 36 bits 일련번호(Serial Number)로 구성된다(그림 2 참조). 관리자 번호는 바로 다음에 이어지는 물품 클래스와 일련번호의 관리 책임을 맡고 있는 기업을 표시하며, 물품 클래스는 관리자 기업에서 정한 품목별 또는 형태별 분류 번호이며, 마지막의 일련번호는 각각의 물품 클래스 내에서 유일하게 부여받은 번호이다. 그림 2는 96 bits EPC 코드를 보이고 있으며, 이러한 형태의 EPC 코드는 IP 주소처럼 전세계적으로 특정 사물을 유일하게 식별하는 주소이다[7].

	Header	General Manager Number	Object Class	Serial Number
GID-96	8	28	24	36
	0011 0101 (Binary value)	268,435,456 (Decimal capacity)	16,777,216 (Decimal capacity)	68,719,476,736 (Decimal capacity)

그림 2. EPC 코드

1) 본 고에서는 EPCglobal네트워크와 RFID/USN 구축 1단계 네트워크가 동일한 것으로 보고 혼용해서 사용한다.

EPCglobal에서는 태그의 기능적 특성에 따라 RFID 시스템을 크게 5가지 클래스로 구분하고 있다. 표 1은 EPCglobal의 분류를 재구성한 것이다[4].

표 1. 태그의 기능적 특성 분류[4]

Class	Nickname	Memory	Power Source	Features
0	Anti-Shoplift Tags	None	Passive	Article Surveillance
1	EPC	Read-Only	Any	Identification Only
2	EPC	Read-Write	Any	Data Logging
3	Sensor Tags	Read-Write	Semi-Passive or Active	Environmental Sensors
4	Smart Dust	Read-Write	Active	Ad Hoc Networking

클래스 1은 읽기 전용 메모리를 가지고 있는 태그로 구성되며, EPC 코드를 응답하여 자신의 유일성을 보이는 ID 소자로써 동작한다. 클래스 2는 읽기와 쓰기가 가능한 메모리를 가진 수동형 또는 능동형 태그로 구성되며, 쓰기가 가능하기 때문에 클래스 1에 비해서 더욱더 다양한 환경에서 활용될 수 있는 장점이 있다. 그러나 공격자가 리더를 가장하여 태그의 정보를 덮어쓰려고 시도할 수 있기 때문에 쓰기 권한에 대한 인증이 반드시 필요하다. 클래스 3은 'Sensor Tags'라는 별칭에서도 알 수 있듯이 주변 정보를 스스로 읽을 수 있는 센서로 구성되며, 이러한 센서들은 세미-수동형 또는 능동형 소자이다. 클래스 4는 다른 태그들과 Ad-Hoc 무선 네트워크를 구성할 수 있는 태그로 구성되며, 이러한 태그들은 'Smart Dust'로 불리기도 한다[5]. 스마트 더스트는 스스로 통신을 시작할 수 있어야 하므로 반드시 능동형 소자여야 한다.

그림 1은 RFID 기반의 EPCglobal 네트워크 및 센서 연동 인터넷 개념을 보이고 있다. EPCglobal 네트워크는 다음과 같은 5개의 기본 시스템으로 구성되어 있다. EPC 코드, ID 시스템 (RFID 태그와 리더), ONS(Object Name Service)서버, PML(Physical Markup Language) 서버, 그리고 SAVANT서버가 그 핵심 구성요소이다[6]. EPCglobal 네트워크란 EPC 코드를 주소로 갖는 네트워크이며, 인터넷과 연동하기 위해서는 EPC 코드와 IP 주소를 상호 연결시켜야 하는데 이를 담당하는 장치가 ONS 서버이다. SAVANT 서버는 하나 또는 다수의 리더로부터 유입되는 태그 데이터의 수집, 카운팅, 또는 필터링 등을 처리하기 위해 설계된 미들웨어로써 분산 시스템으로 구현된다[8]. PML서버는 RFID EPC 제품 정보를 저장 관리하는 서버이다.

EPC 코드는 RFID 태그에 저장되고, 리더가 RFID 태그로부터 EPC 코드를 읽는 역할을 한다. 리더로부터 EPC코드를 전달받은 SAVANT는 ONS 서버에게 EPC 코드의 제품정보를 가지고 있는 PLM서버의 인터넷 위치 정보(인터넷 주소)를 받아 온다. 그 후 SAVANT는 PML 서버로부터 제품정보를 가져와서 제품정보 응용 서버에게 전달해 줌으로써 RFID 응용 서비스가 제공되게 된다. 이 때 EPCglobal에서 정의한 시스템 간의 통신 프로토콜로 PML과 SOAP-RPC/XML-RPC 이 활용되고 있다.

앞서 언급한 바와 같이, EPCglobal 네트워크 시스템이 인터넷과 연동되어 동작하고, 전세계적 글로벌 네트워크로부터 인터넷으로 유입되는 RFID/USN 트래픽양 또한 대규모일 것으로 판단된다. 따라서 RFID/USN네트워크 인프라는 가용성, 안정성, 보안성 등 여러 가지 기능적, 성능적 요소들을 만족할 수 있는 시스템들이 배치되어 운용되어야 할 것으로 본다. 따라서 시큐어 RFID/USN 인프라 구축을 위해서는 컨트롤 plane, 데이터 plane, 메니지먼트 plane을 어떻게 설계하고 구성할 것이 좋은지에 대해서도 고민할 필요가 있다고 본다. 예를 들면 USN으로부터 DoS성격이 있는 비정상 트래픽의 인터넷 유입을 조기 차단하기 위하여 USN 보안 관리를 적용하는 방안이 고려될 수 있다. 또는 RFID/USN 서비스 환경에서 위조/복사 태그로 인한 문제를 원

천적으로 차단하겠다고 한다면, 이러한 태그를 이용한 통신 서비스가 이루어지기 전에, RFID/USN 액세스 컨트롤 단계에서 정품 인증이 선행되어야하고, 이러한 정품 인증 서비스를 제공하기 위해서는 정보보호 인프라를 어떻게 가져가야하는 것이 좋은지를 검토해야 할 것으로 본다.

본 고에서는 3장에서 이러한 문제를 정보보호 요구사항 수준에서 접근해 보았다.

Ⅲ. RFID/USN 정보보호

1. 정보보호 필요성

RFID/USN 네트워크 정보보호의 필요성에 대해서는 다양한 견해가 존재할 수 있다. 저가의 물품에 부착된 RFID 태그 정보의 도청을 심각한 위협으로 여기지 않을 수도 있으며, RFID 태그의 전파 도달거리가 매우 작아서 도청 시도 자체가 근접거리에서만 가능할 것이므로 쉽게 알아낼 수 있을 거라는 의견도 있다. 그러나 RFID의 활용이 저가의 물품에만 한정된 것이 아니고 개인의 사생활 영역에 깊숙이 파고들 것이며, 기업 및 공공기관에서의 활용범위도 커져 갈 것이다. 따라서 RFID 사용자의 프라이버시 보호 문제는 반드시 해결되어야 하며 또한 네트워크 가용성을 훼손하는 일 없이 안정적인 망 구축이 되어야 할 것이다. 이에 본 고에서는 RFID 사용자의 프라이버시 보호와 EPCglobal 네트워크 보호 관점에서 정보보호 필요성을 밝힌다.

첫 번째는 프라이버시 보호의 필요성이다. 프라이버시 훼손이라 함은 정보 유출 또는 정보 위변조에 따른 피해로 볼 수 있으며, 이러한 피해를 사전에 예방하는 것이 프라이버시 보호이다. 여기서 정보유출이라 함은 RFID 태그에 저장된 정보, 태그를 소유한 소유자의 개인 정보 그리고 특정 소유자의 RFID 소유물에 대한 정보를 모두 포함한다. 프라이버시 보호의 범주에는 첫째 엿듣기를 방어하는 도청 방지, 둘째 도청된다 하더라도 그 정보가 정확히 무슨 내용인지 모르도록 하는 비밀성 보장, 셋째 고가의 상품에 저가의 태그를 부착하는 위조 태그 방지, 넷째 불법 복제 태그 방지, 다섯째 불법적 정보 수집을 행하는 위장 리더 방지가 포함될 수 있다.

사회/문화적 흐름이 점차 개인의 정보가 보호되어야 한다는 인식으로 발전해감에 따라 무방비적으로 노출될 수 있는 RFID 태그의 실생활 활용은 소비자 보호단체의 반대에 부딪힐 가능성이 높아지고 있다. 개인에게 있어서 RFID 태그 정보의 노출은 개인의 물품 보유현황 노출, 위치정보 노출, 구매 패턴 및 선호도 노출 등으로 이어질 수 있으며, 이는 이러한 정보를 원하는 기업이 있는 경우 개인의 의사와 무관하게 불법적인 거래가 이루어질 수 있다. 이러한 이유에 근거하여 소비자 보호단체에서는 RFID 태그의 전면적인 시행을 위해서는 프라이버시 보호가 선결되어야 한다는 의견을 제시하고 있다. 실례로 미국의 CASPIAN(Consumers Against Supermarket Privacy Invasion and Numbering)이라는 소비자 보호단체는 베네통의 RFID 태그 도입을 저지하는데 일조하기도 했다[9]. 또한 일부에서는 법률 제정을 통한 총체적인 개인 정보보호를 주장하며 정보보호 기술 개발을 견인하고 있다[10].

또 다른 사례로, 기업 역시 프라이버시 훼손에 의해 피해를 볼 수 있다. 예를 들어 대형 할인점에서 10만원에 해당하는 제품에 60원의 RFID 태그가 부착되어 있다고 가정하자. 만일 누군가가 몰래 태그 정보를 덮어쓰거나 또는 태그를 교체하여 계산 시 3만원으로 나타나게 한다면 손실비용은 7만원으로 볼 수 있다. 따라서 이러한 프라이버시 훼손 행위를 방지할 수 있다면

태그 가격이, 300원으로 높아지더라도 정보보호 기술이 추가된 태그를 사용해야 할 것이다. 즉, 비용 상승의 측면이 있기는 하지만 프라이버시 훼손 행위를 방어함으로써 얻어지는 이익(ROI)이 더 큰 경우에는 반드시 정보보호 기술의 도입이 필요하다. 이를 위한 방안으로, RFID/USN환경에서의 도입되고 있는 다양한 서비스를 태그비용, 정보보호 비용, 제품비용 그리고 프라이버시 침해비용 관점에서 분석함으로써 ROI개념이 고려된 정보보호 솔루션 마련이 필요하다고 본다.

두 번째는 네트워크 보호의 필요성이다. 태그와 리더사이의 도청 및 방해 전파보다 더욱 더 심각한 보안 위협은 네트워크 전체에 대한 DoS 공격이다. 지난 1.25 인터넷 침해사고에서 경험하였듯이 이러한 위협은 광범위한 사용자들에게 영향을 주게 된다. 전달매체 사이에서의 정보수집과는 달리 취약 지점을 집중 공격하는 DoS 공격(예를 들면, 리더가 자신에게 유입되는 모든 데이터를 Savant로 보내고, Savant는 어떤 필터링 없이 그대로 ONS 서버에게 ONS 쿼리를 요청하는 경우) 또는 불법 복제 태그의 대량 유통을 통한 비정상적인 데이터 폭주 등은 네트워크 가용성을 파괴하기 때문에 전체 사용자들의 통신을 불통시키는 막대한 영향을 끼칠 수 있다. 악의적인 행위로써 금전적 가치를 획득하기 위한 공격과는 다소 차이가 있지만 대다수 사용자에게 영향을 끼치는 대규모 피해 가능성이 있기 때문에 EPCglobal 네트워크의 각 시스템들은 DoS 공격을 감내할 수 있는 정보보호 기술을 지니고 있어야 한다. 또한 네트워크에 대한 능동적 공격으로써 ONS 쿼리 또는 PML 데이터 등을 EPCglobal 네트워크 내부에서 가로채거나 변경할 수도 있으므로 당연히 데이터의 비밀성 보장도 필요하다

2. 정보보호 요구사항

일반적인 정보보호 요구사항으로는 첫째 악의적인 공격자가 태그의 정보를 얻고자 시도하는 공격을 막는 인증 기술, 둘째 정상적인 리더와 태그 사이의 데이터를 공격자가 엿듣는 경우를 방어하는 도청 방지 기술, 셋째 공격자가 정상적인 데이터를 위조하여 리더 또는 태그를 혼란시키는 공격을 방어하는 데이터 기밀성과 무결성 보장기술 등이 있다.

이러한 일반적인 요구사항과 더불어 무엇보다 중요한 기술적 요구사항은 RFID/USN의 각 시스템들이 DoS-Tolerant 네트워크 구성을 유지해야 한다는 것이다.

RFID/USN은 새롭게 등장한 네트워크로써 기존의 IPv4 인터넷 또는 IPv6 기반의 BcN 네트워크와 연동될 것이다. BcN 네트워크가 안전하다하더라도 USN 네트워크가 DoS 공격에 취약하여 인증되지 않은 비정상적 데이터 트래픽을 대량으로 BcN 네트워크로 유입시킨다면 이는 BcN 네트워크의 취약성으로 이어지게 된다. RFID/USN 네트워크를 DoS-Tolerant하게 유지하는 것은 인터넷과의 연동에 있어서 반드시 해결되어야 할 정보보호 요구사항이다. 예를 들면, 악의적인 공격자가 복제된 불법 태그를 대량으로 여러 장소에서 유통시킨다거나 고의적인 DoS 공격을 시도할 경우 리더 또는 Savant 미들웨어 및 ONS 서버에서 이를 판별하고 적절하게 처리하여 네트워크 불통 상황을 방어해야 하며, 각 시스템 사이의 상호 인증 및 데이터 보호도 보장되어야 한다. 이 외에도 방해 전파 또는 금속 박막과 같은 물리적인 공격으로 태그와 리더의 통신을 원천적으로 차단하는 악의적인 행동에 대한 감지 기능도 있어야 하며, 예기치 못한 상황이 발생할 때 이를 기록에 남기고 보고할 수 있는 보안관리 기능 등도 요구된다.

구체적으로 RFID 시스템에 대한 정보보호 요구사항을 고민하고 있는 곳 중의 하나가 미국의

EFF(Electronic Frontier Foundation)라는 비영리 단체이다[12]. EFF의 Lee Tien 변호사는 미국 국방부(Department of Defense, DoD)와 국토안보부(Department of Homeland Security, DHS)의 RFID 사용 계획과 월마트와 같은 일반 기업의 RFID 사용 의지에 대해 걱정하면서 RFID 정보보호 측면에서 'Kill Tag' 방법을 주장하고 있다. 그리고 'Kill Tag' 방법을 적용해서는 안 되는 스마트 RFID 태그의 접근 제어에 대한 정책을 누가 설정할 것이며 소유권이 바뀌는 RFID 태그를 누가 제어할 것인가와 같은 디지털 권한 관리에 대한 논의가 필요하다고 주장하고 있다[13].

일본 정부에서는 RFID 시스템의 데이터 보호를 위한 가이드라인을 준비하고 있는데, RFID 태그에는 프라이버시 데이터를 직접 담지 말 것과 고객의 희망에 의해 선택적으로 RFID 태그를 Lock/Unlock 시킬 수 있어야 한다는 것을 권고하고 있다[14].

그리고 국내에서는 RFID 프라이버시 개념으로 첫째 RFID 태그가 부착되어 있는지 알 권리, 둘째 구매 후 소비자가 RFID 태그를 제거할 수 있는 권리, 셋째 ID 추적 또는 비인가 리더로부터 사생활 침해를 받지 않을 권리, 넷째 자신 소유의 RFID 부착 제품에 대한 정보의 조회 및 삭제 권리, 다섯째 자신 소유의 RFID의 정보가 언제 어디서 판독되었는지 알 권리 등이 고려되고 있다[15].

본 절에서는 상기와 같은 정보보호 요구사항을 만족시키기 위하여 RFID/USN 네트워크에 적용할 기술적 요소를 다음과 같이 5가지로 재구성한다. 이와 같은 기술적 요구사항은 RFID/USN 네트워크 초기 설계 시 동시에 반영되어야 한다.

(1) 인증(Authentication)

RFID 태그와 리더 사이의 상호 인증은 태그를 잠그는 Lock 동작이나 해제시키는 Unlock 동작이 요구되는 상황에서 반드시 선행되어야 하는 요구사항이다. RFID 태그는 기본적으로 저성능의 독립된 개체로써 태그가 리더를 인증하기 위해서 신뢰할 수 있는 외부 서버에 접근하기가 어렵다. 그러므로 RFID 태그는 리더를 완벽히 안전하게 인증할 수는 없으며, 일정 수준에서 태그와 리더가 서로를 신뢰할 수 있는 방법이 연구되어야만 한다. 이러한 방법 중에 하나는 태그에 내장된 비밀키를 이용하는 방법인데, 비밀키를 알고 있는 리더가 있다면 이를 신뢰할 수 있는 리더로 인정하는 것이다. 이는 기존의 기술에 비하면 보안성과 안전성이 상당히 결여된 방식이며 이를 뒷받침하기 위해서 이를 충분히 지원해줄 수 있는 백엔드 시스템(Back-end system)이 필요할 것으로 보인다. 또한 EPCglobal 네트워크를 구성하는 콤포넌트 사이의 상호 인증도 보장되어야 한다.

(2) 키 관리(Key Management)

RFID 태그와 리더의 경우 RFID 태그의 제한적인 컴퓨팅 환경 때문에 공개키 암호화 방식을 사용하여 리더와 태그 사이에 안전한 키 교환은 불가능하다. 그러므로 대칭키를 리더와 태그가 미리 공유하고 대칭키 암호화 방식을 사용하여 데이터를 암호화하여 리더와 태그가 주고받는 방법이 한 가지 방법인데, 이런 대칭키는 노출될 가능성이 높기 때문에 그다지 안전하지 못하다. 다른 한 가지 방법은 신호 전달거리가 짧은 태그가 대칭키를 랜덤하게 생성하여 리더에게 전해주는 방법이 있다. 그러나 신호 전달거리는 물리적으로 정확하게 제어되는 것이 아니기 때문에 예기치 않게 신호 전달거리가 길어질 경우라면 이는 전혀 안전하지 못하다. 리더 뒷단의 네트워크 보호를 위해서는 네트워크 토폴로지에 따라 대칭키 방식 또는 공개키 방식을 적절하게 운용할 필요가 있다.

(3) 암호 알고리즘(Cipher Algorithm)

효율적인 비밀키 암호 알고리즘으로 알려진 TEA(Tiny Encryption Algorithm)도 200~2000개의 게이트를 사용하여 하드웨어적으로 구현하기 어렵다. 그러므로 RFID 태그와 리더는 기존의 거의 모든 암호화 알고리즘이나 기존의 암호학적인 방법을 그대로 사용하기란 어려움이 있으며 이를 위해서는 굉장히 제한적인 환경 아래에서도 충분한 보안성을 가져야 하며 충분히 효율적인 알고리즘이 필요하다.

(4) 보안 프로토콜(Security Protocol)

기존의 보안 프로토콜은 데이터를 주고받는 측에서 안전하게 공유된 키를 사용하여 데이터를 서로 암호화하여 주고받는 방법을 사용한다. 또한 디지털 서명 기법을 이용하여 중간자 공격(Man-in-the-middle)에 대비하였다. 그러나 데이터를 암호화한다거나 디지털 서명 기법을 적용하는 것은 RFID 태그와 리더 사이에서는 쉬운 문제가 아니며 안전하게 공유된 키를 리더와 태그 사이에 갖는 것도 쉬운 일이 아니다.

그런 까닭에 이와는 조금 다른 보안 프로토콜들이 제안되었는데, 바로 고요한 트리워킹(Silent Tree-walking)과 랜덤 트리워킹(Randomized Tree-walking)이 바로 그것들이다. 이는 리더가 보내는 신호의 전달거리와 태그가 보내는 신호의 전달거리가 서로 차이가 난다는 것에 기초한 방법으로 태그가 보내는 신호의 전달범위는 충분히 좁아서 도청하려고 하는 제 3자에게 들리지 않는다는 것을 가정한다.

(5) DoS(서비스 거부) 대응

DoS 공격을 막기 위해서 인터넷 웹서버에서 사용하는 방식은 서버가 공격에 대해서 충분히 견딜 수 있도록 공격 트래픽을 분산시키거나 공격을 하는 특정 IP 대역을 차단하여 서버를 지키는 방식을 사용한다.

RFID 기반 EPCglobal 네트워크의 DoS 공격은 두 가지 부분에서 생각해 볼 수 있다. 하나는 태그의 데이터를 읽어 들이는 리더에 대한 공격이고 다른 하나는 RFID의 시스템을 뒷받침하는 백엔드 EPC 시스템에 대한 공격이다. 리더에 대한 DoS 공격은 불법적인 태그가 합법적인 태그를 가정하여 리더에게 리더가 처리할 수 없을 정도의 데이터를 보냄으로서 이루어진다. 리더가 데이터를 모두 처리한다고 하더라도 그 대부분은 잘못된 정보이며 속도 또한 정당한 태그들에 대한 데이터의 처리와는 비교할 수 없을 정도로 지연될 것이다. 그러나 리더는 이러한 DoS 공격에 대해서 쉽게 알아차릴 수 있으며 보안관리 정책을 통하여 리더를 안전하게 지킬 수 있을 것이다. 백엔드 시스템에 대한 공격은 인터넷 상의 웹서버와 비슷하게 발생할 것이지만 이와 다른 점은 웹서버처럼 자신을 지키기 위해서 IP 대역을 차단하듯 리더를 차단할 수 없다는 점이다. RFID의 백엔드 시스템은 항상 합법적인 리더가 요구하는 모든 데이터를 처리해 줄 수 있어야 한다. 따라서 EPCglobal 네트워크 설계 시 정상적인 데이터 처리와 비정상적인 데이터 처리를 구분할 수 있는 DoS-Tolerant 정보보호 기술을 추가하여 자체적인 USN 네트워크 보호뿐만 아니라 BcN 네트워크와 연동 시 BcN 네트워크에 DoS 공격의 영향을 줄 수 있는 취약성을 원천적으로 차단하여야 한다.

지금까지 분석된 내용을 기반으로 RFID/USN 네트워크에 대한 정보보호 필요성과 정보보호 요구사항 또는 고려사항을 표 2로 정리하였다.

3. 현재의 정보보호 기술 동향

고가의 물품이나 장비의 경우 RFID 태그 정보가 높은 부가가치를 가질 수 있는 경우가 많을 것이며 이를 보호해야 하는 것은 당연한 일이다. 그러므로 허가받지 않은 제 3자에 의하여 RFID

표 2. RFID/USN 정보보호 필요성에 따른 고려사항

고려대상	정보보호 필요성	정보보호 요구사항
프라이버시 보호	- 개인 사용자 및 소비자 보호단체의 정보보호 요구 또는 법적/제도적 장치로써 강제하는 프라이버시 보호 필요 - 정보 유출 또는 정보 위변조 등의 프라이버시 훼손 공격에 따른 손실을 방지하기 위해서 프라이버시 보호 필요	- 태그의 정보를 제 3자가 엿들어서는 안 된다. - 설령 엿듣는다 하더라도 정확히 무슨 정보인지 알 수 없어야 한다. - 소유자가 태그를 선택적으로 제거할 수 있어야 한다. - 소유자가 자신 소유의 태그를 제어(Lock/Unlock, activate/deactivate) 할 수 있어야 한다. - 소유자의 위치 정보가 노출되어서는 안 된다. - 태그에 접근 제어 정책, 태그에 대한 디지털 권한 관리를 누가 책임질 것인가에 대한 논의가 필요하다. - 공격자가 태그 정보를 덮어 쓸 수 없어야 한다. - 위조 태그의 동작이 프라이버시를 훼손해서는 안 된다. - 복제 태그의 동작이 프라이버시를 훼손해서는 안 된다. - 위장 리더의 불법적인 정보수집이 허용되면 안 된다. - 태그 정보의 재전송 공격이 허용되면 안 된다.
네트워크 보호	- DoS 공격 또는 비정상적인 데이터 폭주는 네트워크 불통 사고를 유발할 수 있기 때문에 이를 방어하기 위한 네트워크 보호 필요	- 태그와 리더가 서로 신뢰하는 경우에만 통신이 보장되어야 한다. - DoS-Tolerant 리더 기능이 요구된다. - DoS-Tolerant ONS 서버 기능이 요구된다. - DoS-Tolerant PML 서버 기능이 요구된다. - Savant는 비정상적인 데이터 트래픽에 대한 필터링이 요구된다. - EPCglobal 네트워크 내부(ONS 쿼리 또는 PML 데이터)에서의 도청이나 위변조가 방어되어야 한다. - ONS 서버 접근에 대한 인증이 요구된다. - PML 서버 접근에 대한 인증이 요구된다. - RFID/USN에 대한 네트워크 보안관리가 요구된다.

태그의 정보가 유출되어서는 안 되며 정보가 유출되었다 하더라도 그 정보가 제 3자에 의해서 사용될 수 있는 유용한 정보가 되어서는 안 된다. 현재 논의되고 있는 RFID 정보보호 기술은 이러한 태그 정보 유출에 따른 위협에 대해 중점적으로 연구되고 있는 것이 사실이다. 본 절에서는 현재 논의되거나 제안된 기술을 인증 및 접근 제어, 도청 방지, 그리고 정보차단의 3가지 항목으로 분류하여 설명한다.

(1) 인증 및 접근 제어

태그와 리더는 서로를 인증하여 서로를 신뢰하는 경우에만 올바른 동작을 보장해야 한다. 이는 접근 제어와도 동일한 개념이다. 정당한 사용자만이 태그에 접근 할 수 있으며 태그를 잠그거나(Lock) 해제(Unlock)할 수 있어야 한다. 잠긴 태그는 어떠한 리더의 신호에도 응답하지 않으며 해제된 태그는 정당한 사용자에 한하여 자신의 정보를 전송해야 한다. 현재 논의되고 있는 기술로는 '해쉬 기반(Hash-Based) 접근 제어'나 '랜덤(Randomized) 접근 제어'와 같은 방법이다.

■ 해쉬 기반 Lock/Unlock 제어[16]

태그를 잠그기 위하여, 리더는 랜덤한 키를 해쉬하여 데이터베이스에 저장하고 이를 태그의 메타 ID로 사용한다. 그리고 리더는 태그에게 메타 ID를 보내고 태그는 이를 저장하고 잠김 상태가 된다. 태그를 풀기 위하여, 리더는 태그에게 잠김을 풀려고 한다는 쿼리를 보낸다. 태그는 자신이 저장했던 메타 ID를 리더에게 보내고 리더는 데이터베이스에서 메타 ID에 해당하는 ID와 자신이 생성했던 키를 가져온다. 리더는 태그에게 키를 보내고 태그는 이 키를 해쉬해서 나온 값이

자신의 메타 ID와 동일하다면 태그는 잠김 상태에서 빠져나와 주위의 리더에게 반응하게 된다.

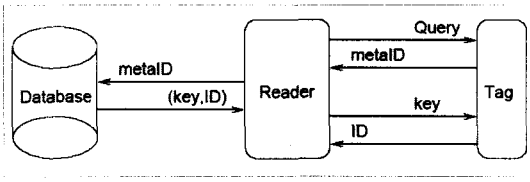

그림 14. 해쉬 기반 접근 제어: 풀기 과정

■ 랜덤 Lock/Unlock 제어[16]

랜덤 접근 제어의 태그를 잠그는 방법은 위의 해쉬 기반 접근 제어와 동일하다. 잠겨 있는 태그를 풀기 위해서는 리더가 태그에게 쿼리를 보내고, 태그는 난수 R을 생성하여 자신의 메타 ID와 R의 해쉬를 계산하고 R과 함께 리더에게 보낸다. 리더는 데이터베이스에게 모든 ID를 줄 것을 요구한 뒤 모든 ID를 뒤져 ID와 R을 해쉬한 것과 동일한 ID를 찾아 태그에게 보낸다. 만약 자신의 메타 ID와 동일한 ID를 받게 되면 태그는 잠김 상태를 풀고 주위의 리더에게 반응한다. 이 방법은 리더가 자신이 잠갔던 태그가 많으면 많을수록 태그를 해제하는 데 걸리는 시간이 늘어난다는 문제점이 있다.

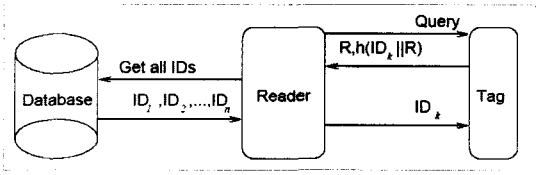

그림 16. 랜덤 접근 제어: 풀기 과정

(2) 도청 방지

정당한 사용자에 의하여 전송된 태그의 정보는 제 3자가 엿들을 수 없어야 하며 설령 엿듣는다 하더라도 정확히 무슨 정보인지 알 수 없어야 한다. 이를 위한 방법으로는 바이너리 트리워킹 충돌 방지 기법 상에서 작동하는 '고요한 트리워킹(Silent Tree-walking)'이나 '랜덤 트리워킹(Randomized Tree-walking)' 같은 방법이 있다. 그 외 암호학적인 방법 중에 '비밀키 암호화 방식'을 사용하여 암호화된 데이터를 전송하는 방법이나 공개키 암호화 방식을 사용하여 암호화된 정보를 태그에 기록하는 '재암호화(Re-Encryption)' 방법 등이 있다.

■ 고요한 트리워킹(Silent Tree-walking)[16]

일반적인 바이너리 트리워킹으로 태그를 읽어들일 경우 리더는 도청자에게 태그에 대한 정보를 말해주게 된다. 그래서 제시된 고요한 트리워킹은 태그가 리더에게 보내는 데이터는 도청자가 직접 들을 수 없다는 데에 착안하여 리더가 태그의 정보를 부르지만 태그가 리더에게 보낸 마지막 데이터와 리더가 태그에게 보내고 싶은 데이터를 XOR하는 방식으로 이루어지게 된다.

■ 랜덤 트리워킹(Randomized Tree-walking)

랜덤 트리워킹은 태그가 랜덤한 수를 생성하여 이를 리더에 보내고 이를 기초로 하여 트리워킹을 시도하는 방식이다. 태그는 반드시 자신이 생성했던 랜덤한 수를 기억하고 있어야 하며, 난수 생성기를 가지고 있고 전원이 끊어지지 않도록 해야 한다는 제약 사항이 있다.

■ 재암호화(Re-Encryption)[17]

RSA 연구소에서 제시한 재암호화(Re-Encryption) 기법은 공개키 암호화 시스템을 사용하여 암호화한 고유 번호를 태그에 덮어 쓰는 방식으로 이루어진다. 공개키 암호화 시스템을 태그 안에 구현할 수 없기 때문에 믿을 수 있는 외부 계산기가 필요하다.

(3) 정보 차단(Blocking)

어느 누구도 태그의 정보를 알 수 없도록 태그의 정보를 막는 방법이다. 물리적인 방법으로 '킬 태그(Kill Tag)' 방법이나 '패러데이 우리(Faraday Cage)', '방해 전파(Active Jamming)'을

쓰는 방법과 '차단자 태그(Blocker Tag)'를 사용하는 방법이 있다.

■ 킬 태그(Kill Tag)[18]

Kill Tag 방법은 Auto-ID 센터에서 제안한 방법으로 태그의 설계에 8-bit의 패스워드를 포함하고 태그가 이 패스워드와 'Kill' 명령을 받을 경우 태그가 비활성화 되는 방식이다. 태그는 내부에 단락회로가 있기 때문에 이를 끊음으로서 Kill 명령을 실행하게 되는데 한 번 죽은 태그는 다시 살릴 수 있는 방법이 없다. 이런 경우 태그를 재사용할 필요가 있는 분야에서는 사용이 불가능하다. 아주 간단한 예로 반품이 가능한 물건에 붙어 있는 태그의 경우 이런 Kill Tag 명령 방식을 사용할 수 없다.

물론, 읽기/쓰기가 가능하도록 설계된 태그의 경우 플래그(Flag) 비트를 이용하여 태그를 죽였다 다시 살릴 수도 있을 것이다. 하지만, 이 경우 또한 여전히 태그에 사용하는 8-bit 암호에 대한 문제가 남는다. 수많은 제품에 사용될 태그라는 것을 감안하고 보안을 생각한다면 128-bit 이상을 암호로 사용해야 하지만 이는 태그에 상당한 부담이 된다. 태그마다 다른 암호를 사용한다면 이를 저장하는 것도 문제이다.

■ 페러데이 우리(Faraday Cage)[18]

무선 주파수가 침투하지 못하도록 하는 방법으로 금속성의 그물이나 박막을 입히는 방법이다. 실제로 RSA 연구소는 2005년 유로화의 RFID 시스템의 도입에 대비하여 돈 봉투에 그물을 입힌 상품을 제시하였다. 그러나 이 경우도 사용 범위가 극히 제한적이 될 것이다.

■ 방해 전파(Active Jamming)[18]

리더가 제품을 읽지 못하도록 방해 신호를 보내는 물건을 소비자가 들고 다니자는 것인데, 불법적으로 이용할 소지가 크고 오히려 방해 신호에 의해 다른 RFID 시스템이 손상될 수 있기 때문에 이를 회피하는 연구를 해야 할 상황이기도 하다.

■ 차단자 태그(Blocker Tag)[18]

차단자 태그는 모든 질문 메시지에 대해서 '그렇다' 또는 '아니다'라는 일관적인 응답만 하는 태그를 말한다. 모든 질문 메시지에 응답하기 때문에 바이너리 트리워킹을 사용하여 태그를 읽어들이는 방식에서는 바이너리 트리의 모든 영역을 검색하게 만드는 결과를 가져온다. 태그의 고유번호가 길어지면 길어질수록 리더는 리더의 용량을 초과하는 개수의 태그를 찾기 위해 시도할 것이고 이는 리더에게 치명적인 결과를 가져올 것이다.

차단자 태그를 조금 더 유용하게 사용하는 방법은 자신이 비밀을 지키고자 의도하는 태그들의 비트에 맞춰 처음 비트들을 제어함으로서 비밀 구역(Privacy Zone)을 만드는 것이다. 차단자 태그와 동일한 시작 비트를 갖는 태그들은 차단자 태그가 만드는 비밀 구역 안에서 안전하게 보호될 수 있다.

이상에서 살펴 본 바와 같이 현재까지의 기술들은 주로 태그와 리더 사이의 인증 및 도청 방지에 중점을 두었기 때문에 Savant 미들웨어, ONS 서버 등 백엔드 시스템을 보호하기 위한 기술의 제안이 미흡한 상태이다. 따라서 네트워크 보호 관점에서 RFID/USN 보호를 위한 기술적 요구사항을 정리할 필요가 있다.

4. 네트워크 보호를 위한 정보보호 기술

그림 5는 RFID 기반 EPCglobal 네트워크의 각 영역에서 요구되는 정보보호 기능을 간략하게 보인 그림으로써, 안전한 RFID/USN 구축을 위해서는 여기서 요구하는 기술적 사항을 만족해야 한다.

구체적인 내용은 그림 5에 기술되어 있으며, 각 구성요소별로 간략하게 정리하면, 첫째 태그와 리더 사이의 인증 및 도청방지 그리고 선택적

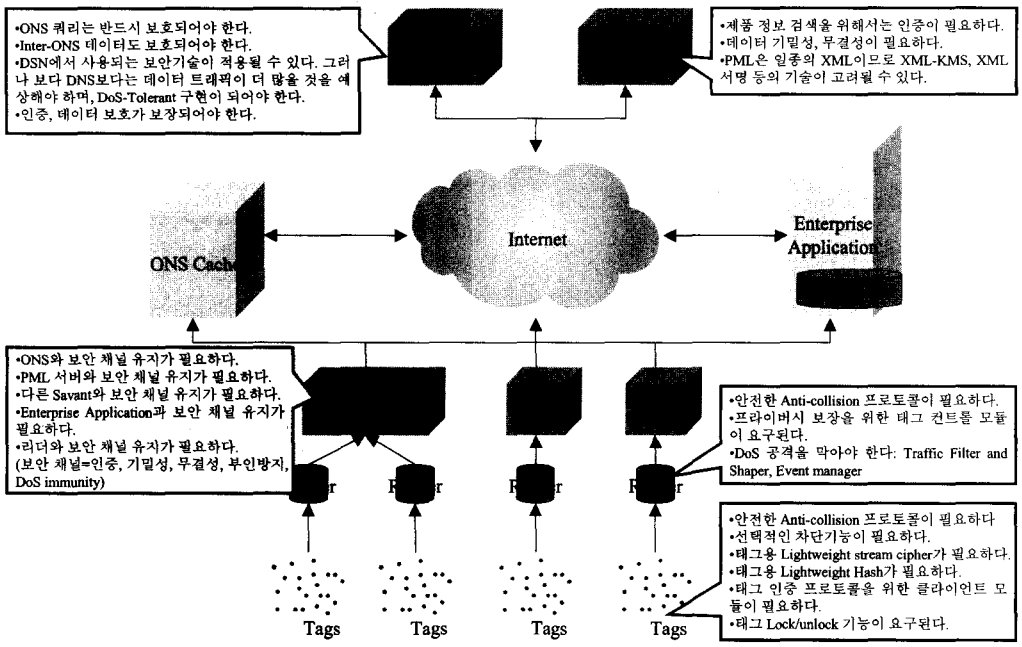

그림 18. 안전한 RFID/USN 구축을 위한 기술적 요구사항

Lock/Unlock에 대한 요구사항과 더불어 리더에서 DoS 공격을 감지하고 방어해야 하는 요구사항이 추가된다. 둘째 Savant 미들웨어는 각 구성요소와 통신 채널을 유지함에 있어서 상호인증이 보장되고, 데이터 보호가 필요하다. 또한 비정상적인 데이터 폭주를 제어하여 DoS 공격에 대응할 수 있어야 한다. 셋째 ONS 서버는 ONS 쿼리의 보호가 필요하며, DNS 보호를 위한 정보보호 기술의 적용이 고려될 수 있다. 끝으로 PML 서버에서는 제품 정보 검색을 위해서는 인증 절차를 통과하도록 구현되어야 하며, PML이 일종의 XML이므로 XML-KMS, XML 서명 등의 정보보호 기술이 고려될 수 있다.

Ⅳ. 결론 및 시사점

최근 정부는 8대 신규 서비스와 3대 첨단 인프라 및 9대 신성장 동력을 포함하는 국민소득 2만불로 가는 IT 839 전략을 발표하였다. 이 IT 839 전략에 따르면 USN은 IPv6 , BcN과 같이 새로운 인프라로 정의하고 있으며 RFID, 텔레매틱스, 홈네트워크 등의 서비스에서 활용될 것이다. RFID/USN은 큰 규모의 전략 사업으로 진행되어 오고 있으며 국민 생활과 산업 전반에 파급효과가 큰 조달/물류/텔레매틱스 등의 분야에서 시범사업 추진을 계획하고 있다.

본 고에서는 RFID/USN 환경에서의 정보보호에 대한 고찰을 진행함에 있어 u-센서 네트워크에 대한 개념 정리와 RFID 기반 EPCglobal 네트워크에서의 정보보호 기술동향을 살펴보고 정보보호의 필요성 및 정보보호 요구사항을 도출하였다.

RFID/USN 정보보호 기술과 관련하여 지금까지는 RFID 태그와 리더에서의 정보보호 위협 이슈가 집중적으로 제기되었고 이와 관련된 솔루션에 대한 언급이 이루어진 반면에, USN과 인터넷

이 연동되는 백엔드 시스템 보호를 어떻게 할 것인가에 대한 논의는 거의 이루어지고 있지 않은 상태이다. 또한 USN 네트워크 안전성 및 서비스 안정성을 포함하는 RFID/USN 정보보호 요구사항에 대하여 구체적으로 정해진 바가 없다. RFID 및 홈네트워크, 텔레매틱스 서비스를 촉진시키기 위해서는 서비스 관점에서 사업자와 이를 활용하는 국민 그리고 개인의 프라이버시 침해에 민감한 소비자 보호 단체 모두가 만족할 수 있는 안전한 USN 인프라 구축이 선행되어야 하며, 우선적으로 USN에서의 정보보호 마스터 플랜이 마련되어야 한다고 본다. 특히 법과 제도, 기술 개발 그리고 RFID 응용 서비스가 상호 연계된 상태에서 USN 정보보호 서비스가 고려되어야 하고, 이를 바탕으로 우리 실정과 응용에 맞는 정보보호 기술이 마련되어야 할 것이다.

참 고 문 헌

[1] Junko Yoshida, 'Euro bank notes to embed RFID chips by 2005', EE Times, December 19th 2001, http://www.eetimes.com/story/OEG20011219S0016.

[2] 정보통신부, '국민소득 2만불로 가는길 IT 839 전략', 2004.

[3] 김동석, 'u-센서 네트워크 구축을 위한 정책 추진 방향', 전파 제 116호, 2004년 1월~2월호, 2004.

[4] Stephen August Weis, 'Security and Privacy in Radio-Frequency Identification Devices', Masters's thesis, M.I.T, May 2003.

[5] J. M. Kahn, R. H. Katz, and K. S. J. Pister. 'Next Century Challenges: Mobile Networking for "Smart Dust"', Mobicom, 1999.

[6] EPCglobal Homepage FAQs, http://www.epcglobalinc.org/about/faqs.html

[7] EPCglobal, 'EPC™ Tag Data Standards Version 1.1 Rev1.24', EPCglobal, April 2004. Available at http://www.epcglobalinc.org

[8] Sean Clark, Ken Traub, Dipan Anarkat, Ted Osinski, 'Auto-ID Savant Specification 1.0', Auto-ID Center, September 2003.

[9] Stephen A. Weis, 'RFID Privacy Workshop: Concerns, Consensus, and Questions', IEEE Security and Privacy, pp.48-50, March 2004.

[10] Australia, 'National Privacy Principles (Extracted from the Privacy Amendment (Private Sector) Act 2000)', Available at http://www.privacy.gov.au/publications/npps01.html

[11] Sanjay Sarma, 'Towards the five-cent Tag', White Paper MIT-AUTOID-WH-006, MIT Auto-ID Center, November 2001. Available at http://www.epcglobalinc.org

[12] EFF, http://www.eff.org/

[13] Lee Tien, 'RFID: Government Use + Economic and Security Issues', Electronic Frontier Foundation, April 2004.

[14] RFID Privacy Workshop @ MIT, http://www.rfidprivacy.org/blog/archives/2003_10.html

[15] KIEI 교육자료, '네트워크와 RFID 기술 및 비즈니스 전략', 산업교육연구소, March 2004.

[16] Stephen A. Weis, Sanjay E. Sarma, Ronald L. Rivest and Daniel W. Engels, 'Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems', First International Conference on Security in Pervasive Computing, 2003.

[17] Ari Juels and Ravikanth Pappu, 'Squealing Euros: Privacy Protection in RFID-Enabled Banknotes', Finalcial Cryptography '03, Springer-Verlag, 2003.

[18] Ari Juels, Ronald L. Rivest, and Michael Szydlo, 'The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy', 8th ACM Conference on Computer and Communications Security, pp.103-111, ACM Press, 2003.

정 병 호

1988년 전남대학교 전산통계학과 학사

2000년 충남대학교 컴퓨터과학과 석사

2000년 3월 - 현재 충남대학교 컴퓨터과학과 박사수료

1998년 2월 - 2000년 6월 국방과학연구소 선임연구원

2000년 6월 - 현재 한국전자통신연구원 무선LAN보안연구팀 팀장

강 유 성

1997년 전남대학교 전자공학과 학사

1999년 전남대학교 전자공학과 석사

1999년 11월 - 현재 한국전자통신연구원 무선LAN보안연구팀 선임연구원

김 신 효

1990년 전남대학교 전산학과 학사

2000년 충남대학교 컴퓨터과학과 석사

1990년~현재 한국전자통신연구원 무선LAN보안연구팀 선임연구원

정 교 일

1981년 한양대학교 전자공학과 학사

1983년 한양대학교 산업대학원 전자계산학과 석사

1997년 한양대학교 대학원 전자공학과 박사

1980년 12월 - 1981년 11월 : 엠시스템즈 사원

1981년 12월 - 1982년 2월 : 한국전기통신연구소 위촉연구원

1982년 3월 - 현재 : 한국전자통신연구원 정보보호기반그룹장/책임연구원

양 대 헌

1994년 한국과학기술원 과학기술대학 전기및전자공학과 학사

1996년 연세대학교 컴퓨터과학과 석사

2000년 연세대학교 컴퓨터과학과 박사

2000년 9월 - 2003년 2월 한국전자통신연구원 정보보호연구본부 선임연구원

2003년 3월 - 현재 인하대학교 정보통신대학원 전임강사