RFID/USN 서비스 환경에서의 정보보안 동향에 관한 연구

고준영, 이근호
백석대학교 정보보호학과
no5ship@naver.com, root1004@bu.ac.kr

A Study of Information Security Trends in RFID/USN Service Environment

Jun-Young Go, Keun-Ho Lee
Div. of Information and Communication, Baekseok University

요 약

IT기술의 발달과 더불어 손쉽게 정보를 얻을 수 있는 RFID/USN 환경을 구축하여 편리하게 사용하고 있는 것이 사실이다. 그에 반해 개인정보 침해문제가 RFID 서비스에서 더욱 이슈화되고 있어 정보보호 문제는 RFID/USN 서비스를 사용함에 있어 해결해야 할 문제가 되었다. 본고에서는 기존의 RFID/USN의 정보보안 위협과 향후 그 대응방안에 대한 동향을 분석해 보고자 한다.

1. 서론

최근들어 기술발전에 의해 우리의 생활은 더욱 편리하게 바뀌고 있다. 여러 개발된 기술 중 대표적인 기술이 RFID(Radio Frequency Identification)/USN(Ubiquitous Sensor Network)기술이다. USN은 필요한 모든 것에 RFID 태그를 부착하고 이를 통하여 사물의 인식정보를 기본으로 주변의 환경정보까지 탐지하여 이를 실시간으로 네트워크에 연결하여 생성된 정보들을 관리하는 통신망으로 정의할 수 있으며, RFID는 태그 리더기를 사용하여 사물에 부착된 태그로부터 사물의 정보 및 주변 환경정보를 수신하고 이를 분석·처리하여 사물에 대한 원격처리·관리 및 사물 간 정보교환 등 다양한 서비스를 제공할 수 있는 기술이다[1,2].

RFID/USN은 현재도 다양한 분야에서 사용 중이고, 앞으로도 사용될 것으로 예측되지만 보안위협에 있어서는 많은 취약점을 나타내고 있다. 이에 본 고 에서는 RFID/USN의 서비스에서 발생이 예상되는 정보보호 이슈와 개선방향에 대한 동향을 알아보고자 한다.

2. RFID/USN의 보안 문제점

RFID의 보안 문제는 도청, 트래픽 분석, 위조, 서비스 거부(DoS, Denial of Service) 공격으로 정리된다.

- 도청 : RFID 시스템은 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 태그 간 통신을 RF 수신하는 수동적 공격이 있다[3].

- 트래픽 분석 : 공격자가 어떤 특정지역의 트래픽을 분석을 하고 있다면, 그 지역의 물품과 유통에 대해 알 수 있으며, 개인의 움직임을 알 수 있다. 이러한 것을 통한 위치 추적 및 개인의 신상정보까지 노출될 수 있는 위험이 존재한다[4].

- 위조 : 메모리에 데이터 항목이 존재하여 공격자는 데이터 항목을 지우거나 대신할 수 있는 방법을 사용할 수 있다. 이것은 리더와 태그간의 통신에 잘못된 데이터를 서로 교환가능하게 함으로 치명적인 위험이 존재한다[5].

- DoS : 공격자가 리더를 가지고 수많은 질의를 리더 및 태그에게 보낸다면 리더와 태그는 많은 질의에 대해서 일일이 반응해야 한다[6].

다음 표는 RFID/USN의 순기능과 그에 반한 역기능에 대한 내용이다.

<표 1> RFID/USN의 순기능과 역기능

RFID/USN 서비스	내용	역기능
동물관리	가축에 전자태그를 부착	폐기될 가축의 이력을 바꿔 유통
홈 네트워크	가전제품에 전자태그를 부착하여 이를 홈 네트워크에 연결	가전제품의 이상 발생을 탐지하지 못하거나 오류정보 전송으로 안전사고 발생
의료 약품	u-healthcare를 통한 진료의 효율화 및 편리성	응급환자 발생 시 환자의 의료정보를 즉시에 전달하지 못하도록 방해
자동차 교통	차량의 중요 부품에 태그를 장착하여 차량 이상 사전에 감지	차량 결함 및 열악한 도로조건 등에 정보전송 오류 및 고의로 정보를 변조/누락시키는 경우 교통대란 및 교통사고 초래
환경 관리	강수량, 댐 수위 관리, 대기 오염 모니터링 등 서비스 제공	센서의 오작동으로 댐 수위 조절을 못하는 경우 홍수, 범람의 자연재해 초래
물류/유통	고객의 취향을 파악하여 최적의 물건 제공	개인정보 및 구매물건의 잘못된 가격정보 제공

3. RFID/USN 정보보안 위협

RFID/USN 기반의 서비스는 현재 편리한 세상을 살아가는데 있어 필요한 것은 사실이다. 하지만 RFID의 특성상 칩에 수록된 개인정보는 사용하는 당사자도 모르는 상태에서 쉽게 판독이 될 수 있으며 UNS 보안은 핵심적인 요소로서 제한된 자원에 비해서 보안 솔루션들은 자원 필요하며 네트워크 토폴로지, 라우팅의 빈번한 환경과 제한된 컴퓨팅 자원을 소모시키는 공격에 취약하고 최소한의 자원을 사용하는 보안기술로서 기존의 정보보호 기술을 그대로 사용불가능 함이 사실이다[7]. 이러한 문제점과 RFID/USN의 발전에 따라 USN 서비스의 유형도 다양해질 것으로 예상되어, RFID의 활용에 USN 서비스에 따른 정보보호 위협과 RFID 시스템 특성으로 인한 개인정보 침해 위협 요인을 제시해보고자 한다.

3.1 RFID 시스템 특성으로 인한 정보보호 위협

RFID 태그는 소형화, 지능화되는데 비하여 가격은 저가화가 실현되면서 물류, 유통뿐만 아니라 동물관리, 환경, 재해예방, 의료관리, 식품관리 등 실생활에서 활용이 확대되고 있다[8]. RFID 태그를 눈에 띄지 않도록 제작하여 부착하여 소비자에게 편리성을 가져다주는 반면, 이로 인해 소비자가 RFID 태그 부착 사실을 알 수 없도록 함으로써 개인정보 침해 의혹을 가져다 줄 수도 있다. 게다가 RFID 태그를 이용하여 사물의 식별이 가능해야 하므로 용도에 따라 단위 지역 또는 전 세계적으로 고유번호를 부여하기 위한 체계를 정립하고 있어 고유번호를 모든 사물에 부여하여 통제 관리의 편리성을 갖고 있지만 고유번호에 대한 정보만을 알아내면 이 제품에 연결된 상품이력정보, 고객정보 등 모든 정보를 알아낼 수 있게 된다[9].

개인정보 및 상품정보 등 대량의 데이터 수집에 따른 RFID 태그를 통해 한곳으로 집중될 우려가 있다. 또한 한번 수집된 정보는 파기되지 않고 수차의 분석을 통해 다양한 용도로 재활용될 수 있어, 고객선호도 분석을 통한 고객 맞춤형 광고성 스팸메일 발송 및 고객정보 불법 거래 등의 역기능 발생이 예상된다.

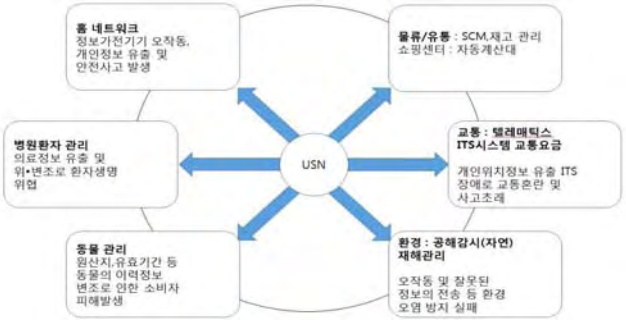
3.2 USN 서비스에 따른 정보보호 위협

RFID/USN 발전단계에 따라 USN 서비스의 유형도 다양해질 것으로 예상된다. 다음은 RFID 활용 USN 서비스 유형별로 정보보호 위협에 대한 가상 시나리오이다[2].

- 홈 네트워크와 연계된 환경정보 센싱 서비스 : 가전제품들과 스마트폰으로 홈 네트워크로 연결되어 이상 발생시 서비스센터에 자동으로 연락을 취하도록 설계되어 있으나 가전제품의 이상 발생을 탐지하지 못하거나 오작동으로 인한 오류정보 전송으로 적절히 대응하지 못하여 안전사고 발생을 초래할 수 있다.

- 자동차 교통 분야의 RFID 태그 간 통신 서비스 : 차량 결함 및 열악한 도로 조건 등에 대한 정보전송 오류가 발생하거나 고의로 정보를 변조/누락 시키는 경우 교통대란 및 교통사고 초래의 가능성이 있다.

- 환경 관리 분야의 RFID 태그 간 통신 서비스 : 강수량을 측정하는 센서의 오동작으로 댐 수위 조절을 못하는 경우 홍수, 범람의 자연재해로 이어질 수 있고, 물의 오염도를 잘못 감지하거나 오염 정보에 대한 정보를 잘못 전송하는 경우 대기오염으로 인한 적절한 대응조치를 취할 수 없다.



(그림 1) USN서비스에 따른 정보보안 위협

4. RFID/USN 정보보안 동향

위에서 살펴본 RFID/USN의 보안 문제들을 해결하기 위하여 태그는 태그 소유자의 개인정보를 위협 또는 손상시키지 말아야 하며, 정보는 인증이 되지 않은 리더로 유출이 되어서는 안된다. 또한 추적을 막기 위하여 태그를 감지하거나 사용불가로 만들 수 있어야만 한다.

- 키(key) 관리 기술 : 모든 센서 노드가 동일한 그룹 키를 공유하게 하는 방식으로서 하나의 센서 노드라도 공격자에게 포획되면 전체 그룹 키가 노출됨. 또한 모든 센서 노드 쌍마다 유일한 키들을 할당하는 방식으로서 각각의 센서 노드는 전체 센서 노드의 수만큼 키들을 저장해야 하며 센서노드의 메모리 제약조건을 만족시키지 한다[10].

- 암호화 인증 기술 : USN의 경우 암호화 인증 기술을 사용할 경우에도 센서 노드의 에너지, 계산, 통신, 메모리 한계를 고려하여야 하므로 일반적으로 사용되는 공개키 알고리즘이나 인증기술들이 그대로 사용될 수는 없다. 따라서 대칭형 시스템이나 속도가 빠른 해쉬함수를 사용하여 암호화 인증 기술을 구성하는 것이 바람직하다.

- DoS공격에 대한 대응 : 공격자는 DoS 공격으로 USN 통신을 제한할 수 있어, 이러한 DoS 공격에 대응하기 위한 필수적인 요구사항은 에너지를 적게 사용하는 프로토콜을 구성하는 것이다.

5. 결론 및 발전방향

RFID/USN 기술이 많은 분야에서 사용 되는 것에 비해 보안위협은 취약한 것으로 알려져 있다. RFID에 대한 암호학적으로 엄밀한 안전성 모델 수립 및 분석이 필요하며 안전성과 실제 환경을 고려한 현실적인 프로토콜들이 제안되어야 한다. 또한 RFID 정보보호 필요성에 대한 인식 제고 및 홍보가 필요하며 현실적인 적용 가능성과 이론적 엄밀함을 고려하여 지속적인 연구 개발이 필요할 것으로 예측된다.

USN기술은 현재 서비스 관점에서의 보안과 연계된 체계적인 연구가 부족한 상태로서 센서 네트워크 정보보호 기술 개발의 각 발전 단계에 따라 달라질 수 있는 센서 노드 전송 메커니즘, 센서OS, 응용서비스의 제원들을 파악하여 개발초기단계부터 보안 기능에 대한 고려가 충분하여야 한다. 즉, USN의 초기 단계인 RFID 기반 센서 네트워크 기술 개발 단계에 적절한 보안 서비스를 제공하느냐에 따라 센서 네트워크가 우리나라의 초고속 인터넷을 능가하는 IT분야의 새로운 인프라로 자리 잡을 수 있을지 여부가 판가름 날 것으로 생각된다.

감사의 글

이 논문은 2013년도 정부(미래창조과학부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임 (2013R1A1A1A05012348). 또한 '산학협동재단'지원으로 수행된 연구임.

참고문헌

[1] S. E. Le et al, "A trend of RFID technology", Electronics and Telecommunications Trends, Vol.25, No.4, Aug. 2010.

[2] 노승민, "RFID 표준특허 데이터 분석을 통한 RFID 기술 동향", 2014년 4월 한국항행학회논문지 제18권 제2호

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

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

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

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

[7] 김원영 외3명, "USN환경에서 2단계 사용자 인증을 이용한 침입 방지 방안", 2014년 1월 한국정보통신학회논문지 Vol. 18, No.1

[8] 정보통신부, "RFID/USN 정보보호대책 로드맵", 전략협의회 2차 회의, June. 2004

[9] 정보통신부, "u-센서 네트워크 구축 기본계획(안)", Feb. 2004.

[10] 송복섭, 김정호, "RFID/USN 기반에서 안전한 출입통제 서비스모듈 구현", 2010년 8월 보안공학연구논문지 제7권 4호