특집

USN 정보보호 기술

손승원 (한국전자통신연구원 정보보호연구단)

I. 서 론

일반적으로 USN(Ubiquitous Sensor Network)의 의미는 네트워크 인프라 개념에서 보면 다양한 네트워크 인프라의 상호 융합을 의미한다. 즉, 최근 업계와 학계에서 많이 회자되고 있는 RFID나 u-센서 네트워크, 그리고 BcN 및 IPv6 네트워크, 이동통신망, 방송망 등이 상호 유기적 연동 및 연계를 가지는 포괄적인 개념으로 USN을 볼 수 있다. 비록 원래의 USN 개념이 광범위한 의미를 가지지만, 본 고에서는 그 논의의 대상을 유비쿼터스 센서 네트워크, 즉, u-센서 네트워크로 한정지울 것이며, 본 고에서는 이를 USN이라고 부를 것이다.

본 고에서 다루는 USN에선 센서 노드가 무선 네트워크로 서로 연결되어 특정 서비스를 수행한다. 이때 센서 노드는 외부 환경 정보를 감지하는 센서와 이를 처리하는 컴퓨팅 요소, 외부와 통신을 위한 통신 요소, 그리고 전원을 공급하는 전원 요소로 구성된다. 센서는 인간의 오감(시각, 청각, 촉각, 후각, 미각)을 대신하여 물리계 또는 환경계의 현상을 정량적으로 측정하여 정보를 검출하는 소자 및 시스템이며, 컴퓨팅 요소는 감지한 외부 환경 정보를 처리하거나 자체 운영 체제를 수행하고 정보를 처리하는 역할을 하는 요소로서 대개 소비 전력 특성을 좋게 하기 위해 8 비트 프로세서를 현재 많이 사용하고 있다. 통신 요소는 IEEE 802.15.4의 Low rate WPAN 프로토콜이 현재 가장 유력한 MAC 프로토콜로서 IEEE 802.15.4a/b는 현재 계속 표준화 중에 있다. 전원 요소는 자체 배터리 혹은 태양열 전지처럼 외부로부터 전원을 공급 받는 요소다.

USN은 유비쿼터스 환경을 현실화하는 네트워크로서 전술한 것처럼 기존의 다양한 네트워크와 유기적인 연동이 필요하다. 현재 인터넷 강국이라는 한국의 위상을 유비쿼터스 환경에서도 유지하기 위해선 USN 네트워크 인프라를 BcN, IPv6, 이동망, 방송망 인프라와 연동하고, 이를 위해 효율적인 네트워킹 및 라우팅 환경을 바탕으로하여 적절한 보안 기술을 적용하여 안전하고 신뢰할 수 있어야 한다. 또한, 상황인지 기술이 연계된 네트워크 환경을 체계적으로 구축함으로써,

IT 강국의 위상을 지속적으로 유지할 필요가 있다. 여기서 특히 중요하게 다뤄할 요소는 보안 기술로서 USN에서의 보안 문제는 기존의 인터넷이 안고 있는 보안 문제보다 더욱 복잡하고 중요한 요소다.

한편, 이견이 있지만, USN의 초기 모델로써, RFID 기술을 볼 수도 있다. RFID 기술에 대해 자세히 살펴보면, RFID 기술은 향후 자체 센싱 기능을 가지거나 물품 정보 및 주변 환경 정보를 센싱하는 "Sensing USN" 기술로 진화될 것이며, 차후에 이 기술은 기존의 BcN 네트워크나 무선 센서네트워크, 홈 네트워크 등과 같은 네트워킹 기술과 완벽히 통합되는 "Networking USN" 기술로 진화될 것으로 보인다. USN 기술의 최종 목적지는 스마트 더스트(smart dust) 수준의 센서 노드 혹은 마치 "물체가 스스로 생각하는 것처럼 착각을 불러일으키는 진정한 유비쿼터스 환경"으로 진화할 것이다. 즉, 이는 RFID 기술을 SCM(Supply Chain Management)에 적용할 경우, 기존의 물류 체계를 보다 효율적으로 만들 수 있게 되는데, 현재까지 RFID 기술을 단순히 이러한 SCM 환경을 구현하는 수단으로 인식해 왔지만, RFID에 자체 연산 기능을 강화 되고 센싱 기능과 배터리를 장착할 경우, 센서 노드(sensor node)로 볼 수 있다. 이러한 센서 노드는 바로 USN을 구성하는 노드가 되는 것이다.

USN은 anytime, anywhere, anynetwork, anydevice, anyservice라는 유비쿼터스 특성을 가지고 있기 때문에, 본질적으로 그 안전성에 문제가 있다. 하지만, 인터넷 환경에서 안전성을 높이기 위해 개발된 여러 가지 정보보호 기술은 USN의 자원 제약성과 특별한 네트워킹 특성(무선 및 ad-hoc 네트워크 특성)에 의해 바로 적용하기 힘들다. 따라서 여러 가지 편리성에도 불구하고 USN 환경이 오히려, 보안의 취약성 및 관리의 어려움으로 그 장점을 충분히 살리지 못하게 될 가능성이 크다.

따라서 본 고에서는 USN 환경에서의 보안 취약성을 먼저 살펴본 후, 이에 대한 정보보호 기술 개발 동향 및 핵심 정보보호 기술을 다루기로 한다.

II. USN 보안 취약성

USN 환경의 고유한 특성(anytime, anywhere, anynetwork, anydevice, anyservice 특성)과 구성 요소의 자원 제약성에 의해 다음과 같은 보안을 위한 당면 문제들을 생각할 수 있다.

- 보안 설계자들은 기존의 인터넷 환경에서 사용하던 다양한 정보보호 기술(암호 기술, 보안 프로토콜 기술, 운영체제 보안 기술, 네트워크 정보보호 기술 등)을 USN 환경의 특성 및 연산 능력 및 메모리 용량, 통신 대역폭과 같은 제한된 자원을 가지는 USN 환경에는 적용할 수 없게 된다.
- 보안 설계자들은 이러한 USN의 자원 제약성을 극복하기 위해 경량 암호 기술 및 정보보호 기술을 개발하여 이를 사용하고자 할 것인데, 이는 다양한 기술적 문제를 유발할 수 있다.
- USN 환경은 수 천대의 컴퓨터가 서로 연결된 인터넷 환경의 단순한 무선 네트

워킹 버전이 아니므로 기존의 분산 시스템을 위한 전통적인 정보보호 기술을 적용할 수 없다. 특히, 인증 및 권한부여, 심지어 소유(ownership)에 관한 기본적인 개념까지 재고할 필요가 있으며, USN 환경에서는 보안 문제 및 프라이버시(privacy) 문제 뿐만 아니라 신뢰(trust)와 제어(control)에 관한 새로운 문제가 발생할 수 있다.

이러한 상황에서 USN 환경에 적합한 정보보호 기술을 개발하기 위해선 기존의 인터넷 환경에서 사용하던 정보보호 기술의 특성을 살펴본 후, USN 환경에 적합한 정보보호 기술을 논할 필요성이 있다. 보안 위협에 대한 전통적인 분류법은 위협 대상 시스템의 특성에 의존하지만, 크게 기밀성(confidentiality), 무결성(Integrity), 가용성(availability)과 같은 세 가지 범주로 분류할 수 있다. 이 중, 기밀성은 인가되지 않은 개체가 보호하고자 하는 정보를 알게 될 때 침해 되며, 무결성은 인가되지 않은 개체가 정보를 임의로 변조할 때 침해 된다. 가용성은 예로서 누군가가 웹 사이트를 다운시키는 것처럼 시스템의 기능을 수행하는 것을 방해할 때 침해 된다고 볼 수 있다.[2] 이 경우 모두 인가된 개체와 인가되지 않은 개체는 구별이 필요한데, 두 개체를 구별하기 위해선 다음과 같은 식별과 인증, 권한 부여라는 세 단계의 처리 과정이 필요하다.[3]

- 식별(identification): 사용자가 자신이 누구인지를 말함
- 인증(authentication): 시스템이 그 주장의 당위성을 검증
- 권한부여(authorization): 사용자가 특정 접근 권한을 부여 받음

인증의 실패는 쉽게 기밀성과 무결성, 가용성 침해를 유발한다. 예를 들어, 수신자의 진짜 신원이 송신자가 기대한 개체가 아니라면, 암호화를 통해 비밀을 보호하는 것이 무의미한 일이 될 것이다.

III. USN 정보보호 기술

USN 정보보호 기술을 논하기 전에 먼저 국내외 USN 기술 동향을 먼저 살펴 보기로 한다. 센서 노드에 있어서의 국외 기술과 USN 네트워킹에 있어서의 국외 기술 동향을 살펴보고 이어서 국내 기술 동향을 살펴 보기로 한다.

1. USN 기술 동향

USN 기술과 관련한 국외 기술 동향을 살펴보면, USN이라는 것은 그 핵심 기반 기술로서 센서 기술과 센서 노드용 OS 기술, 프로세서 기술, 보안 기술 등을 볼 수 있는데, 선진 외국의 학계 및 연구소는 전통적으로 이 분야에 대하여 매우 앞선 기술을 가지고 있다. 예를 들어, 센서 노드용 OS인 TinyOS와 프로토콜 기술, 기반 프로세서 기술은 매우 앞서있다. 하지만, USN용 정보보호 기반 기술이나 보안관리 및 보안미들웨어 등은 아직 선진 외국도 초기 단계에 머물러 있다.

센서 노드 요소 기술과 관련하여 버클리 대학에서는 저가의 극소형 지능형 디지털 스

마트센서/통신 시스템을 개발하는 Smart Dust 프로젝트를 추진했으며, 또한, OS 차원에서는 모트(mote)라고 명명한 센서 노드에 효율적인 TinyOS를 개발했고 이를 이용해서 센서 노드들 간의 다양한 통신을 수행하였다. 또한, 보안 기술로는 SPINS(Security Protocols for Sensor Networks)이라는 프로토콜 개발을 시작으로 다양한 센서 통신용 경량 프로토콜에 대한 연구를 활발히 수행하고 있다.

일본은 수 년 전부터 진행해 온 TRON 프로젝트를 통해 다양한 사양의 T-Engine 및 이를 위한 운영체제인 T-Engine 마이크로커널을 개발하였으며, 높은 사양의 T-Engine에서는 암호 프로토콜의 수행도 가능할 것으로 추정됨. 또한, 외부 발표에 의하면 T-Engine에 경량 비대칭키 암호 매커니즘도 구현할 것이라고 한다.

한편, 네트워킹 및 라우팅 기술 측면에서는 네트워크 요소 기술 개발과 센서 노드의 배포, 유지 및 관리, 감지 기반 응용의 수행을 원활하게 하도록 응용 및 연구개발의 목적에 따라 네트워킹 기술에 대한 다양한 연구를 진행하고 있다.

센서 네트워크의 응용 서비스에서 요구하는 센서 정보의 유효성은 센서 노드들 간의 시간적 동기화에 기반하며 대표적인 기술로는 RBS[1], TPSN[2] 등 여러 대학에서 프로토콜을 연구하고 있다. 데이터 링크 프로토콜로는 IEEE 802.15.4의 Low-rate WPAN[3] 프로토콜이 현재 가장 유력한 MAC 프로토콜로서 IEEE 802.15.4a/b는 현재 계속 표준화 중에 있으며 그 외 UCLA의 S-MAC(Sensor MAC), T-MAC(Time-out MAC)등 대학에서 개발된 프로토콜도 있다. ZigBee는 무선 송수신 회로의 구성을 단순화하고 칩셋의 가격을 $1.5 목표로 하고 있으며, 이러한 사양을 조기에 실현할 수 있다면 USN의 표준 방식이 될 가능성이 매우 크다. 네트워크 프로토콜로는 ZigBee Alliance에서 네트워크 계층을 표준화하고 있고, Flooding/Gossip, SPIN[4], LEACH[5], TEEN[6], MECN[7], GAF[8] 등과 같이 전용 네트워크 프로토콜이 많이 연구되고 있으나 현재 주도적인 프로토콜은 없는 상황이다.

USN 정보보호 기술 체계 구축 동향을 보면, 미국 NIST의 CSRC(Computer Security Resource Center)의 보안연구반에서는 새로운 위협에 대응하는 차세대 보안기술 개발 중이다. "E-Authentication 프로젝트" 추진을 통해 사용자 인증 신뢰등급에 적합한 시스템의 안전기준을 마련하고 이에 따라 사용자 인증시스템의 구현기술 지침을 마련하고자 한다. 이는 USN에 적합한 인증 기술 개발을 목표로하고 있다고 볼 수 있다.

미국 DARPA는 유비쿼터스 첨단기술을 8개 분야로 나누어 개발하고, 첨단 보안기술관련 프로젝트는 ATO(Advanced Technology Office) 등에서 나누어 진행 중이며, 일본 노무라종합연구소에서 발표한 '유비쿼터스 네트워크를 선도하는 정보통신기술 로드맵'에

1) RBS: Reference Broadcast Synchronization
2) TPSN: Time-sync Protocol for Sensor Networks
3) WPAN: Wireless Personal Area Network

4)SPIN:SensorProtocolsforInformation via Negotiation
5) LEACH:LowEnergyAdaptiveClustering Hierarchy
6) TEEN:Threshold sensitive Energy Efficient sensor Network protocol
7) MECN:MinimumEnergyCommunication Network
8) GAF: Geographic Adaptive Fidelity

서는 Identity 통합관리 기술을 유비쿼터스 환경의 차세대 보안기술의 하나로 선정하였으며, 일본 uID 센터에서는 물품정보 검색서비스를 위한 보안기술 연구를 주된 활동으로 하고 있으며, RFID 네트워크 보안을 위한 기반 인증기관인 eTRON CA를 운영 추진이다.

선진 외국 상황을 보면, 차세대 보안기술 개발을 위해 대학, 업체 및 민간 연구기관의 다양한 프로젝트가 진행 중이다. 미국 캘리포니아 대학은 유비쿼터스 환경에서 모바일 기기 이용자의 프라이버시 보호를 위한 보안기술 프레임워크 개발 중이고 미국 펜실베니아 대학에서는 유비쿼터스 네트워크 환경에서의 이동통신 보안환경 구축 프로젝트 추진이다. 여기에 SUN사와 HP사 등을 중심으로 서로 다른 서비스에 등록한 별도의 Identity를 체인으로 연결함으로써, 다른 Identity를 가지고 있더라도 통합인증을 수행할 수 있는 Federated Identity 솔루션을 개발중이다. BBN 연구소는 2002년 9월부터 2004년 9월까지 DARPA IXO NEST 프로그램으로부터 예산을 지원받아 "TinyPK" 프로젝트를 추진중이다.

국내의 상황을 보면, USN 정보보호 기술은 현재 주로 학계에서 연구하고 있으며, 기술개발 초기단계에 머물러 있다. 국내의 몇몇 소형 업체에서 주로 교육용 및 기기 감지/제어 목적으로 센서 노드를 개발하고 있음. 하지만, 통신 기술과 센서 기술, 계산 기술 등은 거의 모두 외산 제품에 의존하고 있음. 또한, 관련 보안 기술 개발은 거의 전무한 실정이다.

USN과 유사한 형태를 가지는 Smart Card의 경우 ETRI 정보보호단에서 관련 정보보호칩 및 보안체계 등이 연구되어 있으나 플랫폼 및 네트워크 인프라 차원에서의 보안 부문은 많은 연구가 필요하다. 최근 한국전자통신연구원(ETRI)에서는 ICU와 함께 센서 노드용 나노 OS 플랫폼인 Nano Qplus를 개발했으며, 또한, 삼성에서 역시 센서 노드를 위한 초소형 운영체제를 개발하고 있으며, KETI에서도 운영체제를 개발 중임. USN 보안 기술은 센서 노드용 초소형 운영체제의 지원을 많이 받아야 하므로, 센서 노드용 초소형 보안 운영체제를 개발할 필요가 있다. 그리고, 2004년에 TTA의 RFID/USN 표준화 프로젝트 그룹이 결성되어 본격적인 표준화– 보안워킹그룹 신설 예정이며, 2004년에 USN 표준화포럼이 결성되고 보안워킹그룹이 결성되었으나 아직까지 표준 진척이 미비한 상황이다.

USN 네트워크 측면에서 국내의 기술 개발 동향을 보면, DHCP[9] 또는 IPv6 자동 주소 설정 등으로 노드 자동 네트워킹 기술이 개발되고 있으나 단일 홉 내에서의 동작으로 그치고 있으며, USN이 구성하는 멀티 홉 환경에 대한 지원 필요성이 제기되고 있는 상황이다.

삼성에서는 ICU와 함께 센서 네트워크 계층 프로토콜을 개발 중이며,국내 여러 대학에서 네트워크 계층 프로토콜 관련 논문을 발표하고 있지만, 아직 연구 수준에 머물러 있다. ETRI를 중심으로 IPv6 핵심 기술 표준화와 IPv4/IPv6 전환 기술 개발이 시작되어 IPv6를 기반으로 하는 단일 서브넷 또는 Ad-hoc 네트워크에서 활용될 수 있는 자동

9) DHCP: Dynamic Host Configuration Protocol

네트워킹 기초 기술이 개발되고 있음. 또한 메쉬 형태로 구성된 라우터 간에 계층적 IPv6 프리픽스 할당 기법도 개발되고 있다. KAIST의 MICROS 프로젝트에서 무선 통신 소자의 센서 네트워크 활용을 위해 MICROS MAC 프로토콜을 개발 중이며, ETRI가 이동망과 WLAN망 사이의 핸드오버 기능을 개발하여 향후 USN 네트워크에서 활용할 무선 네트워킹 기술의 일부가 확보 된 상황이다.

2. USN 정보보호 기술

다음은 안전한 USN 환경 개발을 위해 필요한 정보보호 기술 요소를 나타내었다. 먼저 크게 암호 알고리즘과 프로토콜과 같은 USN의 경량 특성에 맞는 보안 프리미티브 기술 개발이 필수적이며, 복잡하고 동적인 USN 환경에 적합한 인증 기술의 개발, USN 네트워크 보안 관리 기술의 개발, 키 관리 기술 개발, 보안 통신 및 라우팅 기술의 개발, 센서 노드 공격 탐지 기술의 개발이 필요하다. 이에 대하여 각각 살펴보면 다음과 같다.

USN 환경은 저전력 및 적은 메모리, 낮은 컴퓨팅 파워와 같이 자원 제약성이 매우 높다. 이러한 응용에 적합한 기밀성, 무결성, 인증, 프라이버시 보호, 위치 추적 방지를 위한 암호 프리미티브 기술 개발이 필요하다. 이는 경량 대칭키 암호나 비대칭키 암호, 해쉬 함수 등에 의해 현실화 된다. 그리고 분실 혹은 도난으로 인한 정보유출을 막고 위장, 도청 등을 막기 위한 경량 인증 기술 및 위변조 방지 기술 개발 필요이 필요하다. USN의 Ad-hoc 네트워크 특성과 복잡한 라우팅 기능을 효율적이고 안전하게 관리할 수 있는 보안 소프트웨어 기술 개발도 필요한데, USN상에 새로운 센서 노드의 join시의 관리, 센서 노드의 fail, 위장 노드 탐지 등과 같은 관리 기술이 필요하며, USN 네트워크상에서의 데이터 수집에 대한 권한 부여, 수집 제한 등과 같은 데이터 관리 기술 개발도 필요하다.

자원 제약성이 높은 센서 노드에서 효율적인 보안 프로토콜 처리와 보안 라우팅 지원, 암호 수행, USN 보안 메커니즘 제공, 메모리 보호, 등, 센서 노드에 적합한 경량 보안 OS 기술 개발도 필요하다. USN 보안 프로토콜에 적합한 대칭키 암호 기반 혹은 일방향 함수 기반의 경량 그룹 키 및 클러스터 키, 공유 키 분배 및 관리 기술 개발도 필요하게 된다.

센서 노드 위변조 및 악성 센서 노드에 대한 감지 및 제어, 부채널 공격(SPA, DPA, EM 공격 등)을 탐지 및 방지(tamper evidence/resistance) 하는 기술도 개발해야 한다. 하지만, 센서 노드는 일반적으로 저가이며 자원 제약성이 높기 때문에 이러한 물리적인 공격을 방지하는 기술을 구현하기가 매우 어렵다. 이 때문에 센서 노드는 본질적으로 물리적인 보안 취약성이 있다는 전제하에 프로토콜 및 관리 차원에서 보안 기술을 개발하는 경우가 많다.

지금까지 USN 정보보호 기술에 대한 국내외 동향과 기술 개발이 필요한 USN 정보보호 기술에 대하여 간략히 살펴봤다. 본 고에서 언급한 다양한 USN 정보보호 기술을 개발하기 위해선 경량 암호 기술과 프로토콜 기술, 센서 노드용 소형 OS 기술 및 경량 보안 기술, 라우팅 보안 기술, 물리적인 보안 기술 개발이 필수적이다.

Ⅳ. 결론

본고에서는 USN 환경이 당면한 보안 위협을 알아보았으며 이에 대한 적절한 정보보호 기술을 국내외 상황을 예로 들면서 간략히 언급했다. USN 환경이 기존의 인터넷 망과 홈 네트워크, RFID 시스템, USN 시스템, WPAN 등을 모두 포함하고 있는 광범위한 개념이기 때문에 USN 환경에 적합한 정보보호 기술을 개발하는 것은 안전한 유비쿼터스 환경을 위한 필수 요소가 된다. USN은 높은 자원 제약성과 ad-hoc 무선 네트워크 특성을 가지므로 기존의 인터넷 환경에서의 정보보호 기술을 그대로 적용할 수 없으며, USN 환경에 적합한 정보보호 기술을 개발하는 것도 쉽지 않은 일이다. 하지만, 향후 유비쿼터스 환경은 USN 기술을 시작으로 사물의 지능화 및 네트워크화가 진행될 것이므로, 안전고 편리한 유비쿼터스 세상을 만들어가기 위해선 본 고에서 언급한 여러 가지 핵심 정보보호 기술을 개발해야 할 것이다.

참고 문헌

[1] 김호원, Light weight crypto module for RFID and USN applications, 유비쿼터스 정보보호 workshop 2005, 2005년 6월1일

[2] Frank Stajano, "Security for Ubiquitous Computing", John Wiley & Sons, 2002

[3] Bruce Schneier, Applied Cryptography, John Wiley & Sons, 1996

[4] Frank Stajano, "The Resurrecting Duckling - What Next?", Security Protocols Workshop 2000

[5] EPC Global, "EPC Radio-Frequency Identity Protocols Class 1 Generation 2 UHF RFID Protocol for Communications at 860MHz-960MHz, version 1.0.9", Sep. 2004

[6] Klaus Finkenzeller, RFID Handbook 2nd Edition, John Wiley & Sons, 2003

[7] Steven Shepard, RFID : Radio Frequency Identification, McGraw-Hill, 2005

저자소개

손 승 원

1984년 2월 : 경북대학교 전자공학과(공학사)
1994년 2월 : 연세대학교 대학원 전자공학과 석사(공학석사)
1999년 2월 : 충북대학교 대학원 컴퓨터공학과 박사(공학박사)
1983년 – 1986년 삼성전자(주) 연구원
1986년 – 1991년 LG전자(주) 중앙연구소 HI8mm 캠코더팀장
1991년 – 현재 한국전자통신연구원 정보보호연구단 단장/책임연구원
주관심 분야 네트워크 정보보호, RFID/USN 정보보호, 유비쿼터스 정보보호, Biometry, 정보보호 정책 등