u-센서 네트워크 보안 기술 동향

Technical Trend of Security in Ubiquitous Sensor Networks

김신효(S.H. Kim) 무선LAN보안연구팀 선임연구원
강유성(Y.S. Kang) 무선LAN보안연구팀 선임연구원
정병호(B.H. Chung) 무선LAN보안연구팀 선임연구원, 팀장
정교일(K.I. Chung) 정보보호기반그룹 책임연구원, 그룹장

최근 새롭게 등장한 유비쿼터스 컴퓨팅 환경은 기존의 컴퓨팅 환경과는 다르게 통신 인프라가 없는 환경에서도 동작이 가능한 저전력 소출력의 무선 센서간의 네트워크를 형성하고 이들간의 정보 유통이 이루어진다. 이러한 u-센서 네트워크는 Ad-hoc 성격뿐만 아니라 무선이 가지는 방송 특성으로 센서 정보의 도청, 비정상적 패킷의 유통, 메시지의 재사용 등의 데이터 위·변조 문제와 네트워크 전체를 마비시킬 수 있는 서비스 거부 등의 공격에 쉽게 노출된다. 본 고에서는 센서 네트워크에서의 정보보호 요구사항과 구조, 키 관리의 문제 및 라우팅과 수집된 데이터를 집계하는 데 있어서의 보안 이슈와 동향에 대해 소개한다.

I. 서 론

IT 산업의 발전과 국가적인 부의 창출을 위한 정보통신부의 야심찬 계획인 'IT 839 전략'의 추진 계획이 발표되었으며, 여기에는 언제, 어디서나, 임의의 장치를 사용하여 원하는 서비스를 누구라도 사용할 수 있는 u-센서 네트워크(Ubiquitous Sensor Network: USN)를 IPv6와 BcN과 더불어 3대 인프라로 정의하였다[1].

이러한 USN은 적은 메모리, 배터리 용량의 제한, 컴퓨팅 성능의 제약 등 제한적인 하드웨어 자원을 가진 수많은 센서 노드들이 무선 통신으로 거미줄처럼 연결된 거대한 네트워크로서, 사람 또는 주위의 사물들을 인식하고 이들간 네트워크를 구성하여 위치정보를 파악하여 디지털 홈 및 군사 목적으로 활용된다. 또한 센서는 인텔리전트 빌딩의 자동 환기, 무인 경비 시스템과 오염 물질이 산재된 공장 작업장 내 환기 및 개폐 장치, 차량 이동 장치 또는 가정용 자동 온도 조절기 등에 이용이 가능하고, 장난감, 게임기, 가전 제품 디바이스 및 PC 주변기기에서도 다양하게 이용될 수 있다. 하지만 이러한 USN의 활용성에도 불구하고 센서 정보의 도청, 비정상적 패킷의 유통, 메시지의 재사용 등의 데이터 위·변조 문제와 네트워크 전체를 마비시킬 수 있는 서비스 거부 등의 공격에 쉽게 노출된다. 디지털 홈에서의 센서 네트워크의 활용은 개인 프라이버시 보호가 선행되어야 하며, 지진, 화재 경보 센서 등의 공공의 목적이나 군사용으로 사용될 경우 보안 기능은 더더욱 필수적이다.

본 고에서는 이러한 센서 네트워크에서의 필요한 보안 요구사항과 센서 네트워크에서의 보안 구조와 키관리 및 보안 프로토콜과 시큐어 라우팅을 포함한 보안 기술 동향에 대하여 살펴보고, 결론을 맺기로 한다.

II. 센서 네트워크 보안 요구사항

차세대 무선통신 세계에 대한 비전과 연구 방향 및 기술개발 대상들에 대한 논의가 이루어지고 있는 Wireless World Research Forum(WWRF) 산하의 근거리 무선통신 시스템 표준 그룹 WG5에서 발표된

백서 중에 Wireless Body Area Network(WBAN)과 Wireless Sensor Network(WSN)이 포함되어 있을 만큼 USN은 차세대 네트워크의 주류임은 분명하다[2]. 그리고 WSN 정보 보안 기술 및 효율적인 전력 제어 기술, 스마트 센서 구현 기술에 대한 내용을 센서 노드 구현 관점에서의 향후 주요 핵심 기술로 정의하였으며, 정보보호 이슈는 매우 중요하다[3].

센서 네트워크는 센서 노드들이 좁은 영역에 조밀하게 분포되고, 대량의 노드들이 산재하며 이 노드들의 동작이 항상 성공적이지는 못하다는 특징으로 네트워크의 토폴로지는 매우 빈번하게 변경되어야 함은 물론 방송(broadcast) 방식의 통신 방식을 사용하는 등의 특징을 가진다. 또한 주위의 노드들이 믿을 수 있는 상태인지에 대한 판단조차 어려운 열악한 배터리와 컴퓨팅 파워 제약성을 가진 무선 Ad-hoc 형태로써, 센서 정보를 통해 목적지까지 전달하기 위한 경로를 설정하거나 유지하는 라우팅 시에도 네트워크 형성에 비협조적인 노드를 경로에서 제외하여 라우팅의 신뢰도를 높이거나, 노드의 오버헤드를 최소로 하는 인증 기능도 필요하다. 즉, 하나의 센서 노드가 통신하는 노드의 수가 하나가 아닌 다대다 통신인 그물망 통신(mesh)으로 이루어지는 센서 네트워크에서는 노드들의 상호 인증과, 제한된 센서 자원을 이용하여 인증과 암호화에 사용될 암호키 관리의 문제가 주 이슈 중의 하나이다. 또한 센서 네트워크가 가지는 Ad-hoc 환경은 노드들이 네트워크 진입과 탈퇴가 빈번하므로 비합법적인 노드가 라우팅 정보를 혼란시키거나 잘못된 정보를 계속적으로 전파함으로써 생길 수 있는 서비스 거부(denial of service) 공격에도 대응할 수 있어야 한다.

센서 네트워크에서의 보안 요구사항을 정리하면 아래와 같다.

- 암호키를 관리할 수 있는 기능을 제공하여야 한다.
- 센서 환경에 적합한 경량화된 암호 및 인증 기능을 제공하여야 한다.
- 라우팅 시에 보안 기능을 제공하여야 한다.
- 서비스 거부 공격에 강한 구조이어야 한다.
- 사용자에 대한 위치 정보와 센서 노드의 집합정보에 대한 암호 기능을 제공하여야 한다.

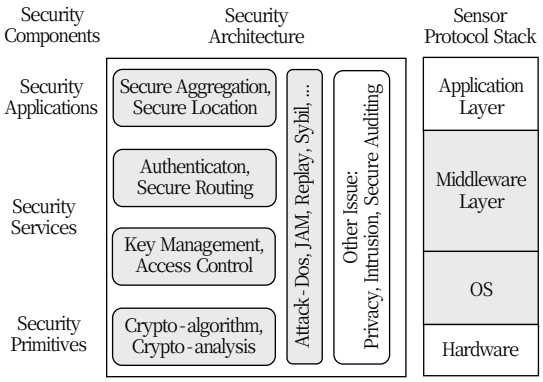
Ⅲ. 센서 네트워크 보안 기술 동향

1. 센서 보안 기능

센서 네트워크에서 필요한 보안 요구사항은 앞절에서 전술한 바와 같으며, 이를 기준으로 센서 네트워크에서 필요로 하는 보안 기능으로는 암호 알고리듬, 키관리 및 보안 프로토콜, 인증 및 시큐어 라우팅, 시큐어데이터 집합 등으로 압축할 수 있을 것이다. 일부 연구기관에서는 (그림 1)과 같은 보안 구조를 제시하였으며 여기에서 위의 보안 기능 이외에 프라이버시와 침입 그리고 시큐어 감시 등도 추가 이슈로 정의하고 있다[4].

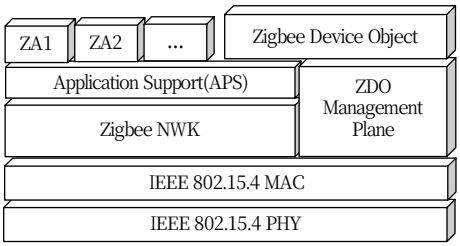
이중에서 키관리 및 접근 제어 등의 암호 서비스를 제공하기 위한 동향으로는 센서 노드용 운영체제로 개발된 TinyOS에서 구동 가능하도록 하는 TinySec이 있다[5]. 이 프로젝트에서는 링크 보안 기술을 적용한 간단한 접근제어와 메시지 위·변조를 막을 수 있는 무결성 기능과 비합법적인 노드에 의한 센서 정보의 해석을 방지하는 기밀성 기능을 제공한다.

또한 업체를 중심으로 하는 Zigbee Alliance는 저전력 무선 센서에 다양한 응용의 활용이 가능하도록 하는 기능과 보안 기능에 대한 정의를 진행중이다[6]. 송/수신이 필요한 경우에만 수면모드에 있는



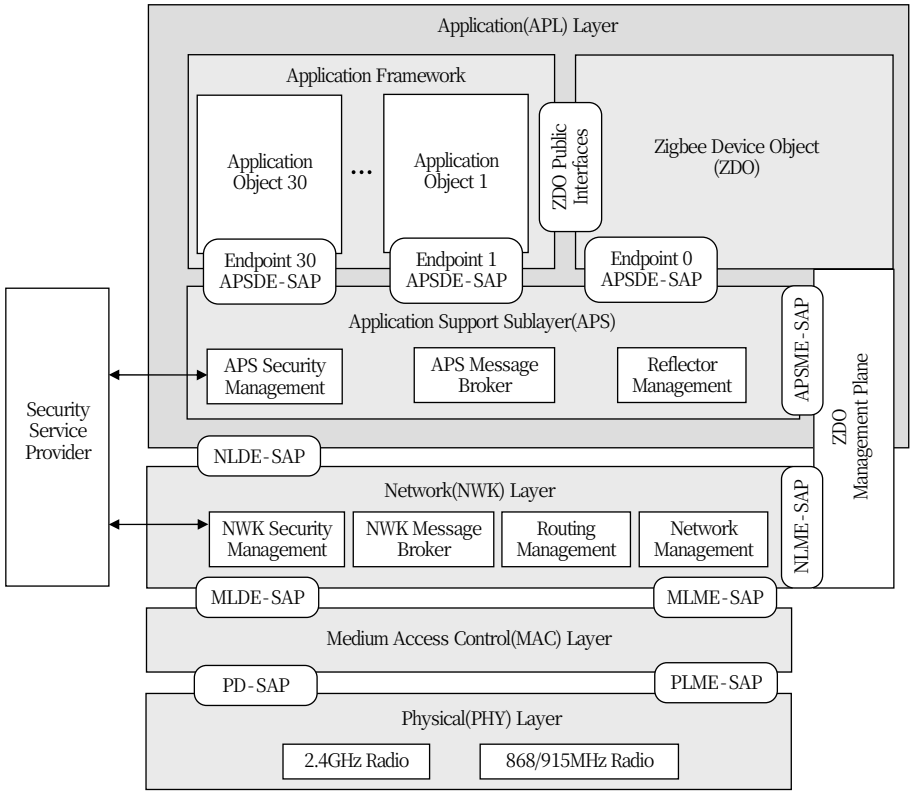
(그림 1) 센서 네트워크의 보안 구조

노드들을 활동 상태로 변경함으로써 전력 소모를 최대한 줄인 IEEE 802.15.4 WPAN 물리 계층과 MAC 계층 규격을 준수하는 Zigbee 네트워크는 독자적인 네트워크 참조모델을 구성할 수 있으며, 그 구성 예시는 (그림 2)에 도시하였다. 즉, Zigbee Alliance에서는 IEEE 802.15.4의 물리계층과 MAC 계층을 사용하고 네트워크 상위 계층에 다양한 응용과 보안 서비스 지원이 가능하도록 하는 프레임워크를 제공한다.



(그림 2) Zigbee 네트워크 프로토콜 예시

(그림 3)에서는 Zigbee 프로토콜 스택 구조로서, 네트워크 계층(network kayer)과 응용 지원 하부 계층(application support sublayer)에서는 보안 서비스 제공자(security service provider)의 도움으로 보안 서비스를 제공하게 된다. Zigbee 보안 서비스는 대칭키 암호 방식을 이용하여 두 노드 간의 비밀키 설정과 상호 인증 과정을 수행하고, 이 키를 이용하여 MAC 계층, 네트워크 계층, 응용 계층에서의 데이터 프레임에 대한 보안기능을 제공한다. 비밀키의 전달, 상호 인증 등의 프로토콜에 대한 정의는 Zigbee Alliance 규격에 포함되어 있으나, 마스터 비밀키를 안전하게 각 노드에 전달하기 위한 방법을 제공하지는 않는다. 즉, 트러스트 센터(trust center)라고 불리우는 장치를 활용하여 노드 사이의 마스터 비밀키는 중간 노드들의 중계에 의하여 키 전달은 가능하지만 이 통신 채널의 안전성을 항상 보장하지는 않는다.



(그림 3) Zigbee 프로토콜 스택 구조

대칭키 방식의 암호 메커니즘에서는 비밀키의 안전성을 보장하는게 가장 중요함에도 불구하고, Zigbee 네트워크는 트러스트 센터와 노드 사이의 마스터 비밀키를 공유하고 있다는 가정 하에 암호 통신 서비스를 진행함은 물론, 트러스트 센터에서 통신하고자 하는 모든 노드의 비밀키를 관리하도록 되어 있는 구조적인 약점을 가지고 있다.

새로운 노드의 보안 접속을 위한 비밀키를 분배하고 노드의 연결 해지를 담당하는 트러스트 센터를 어디에 두어야 하는냐에 대한 결정은 Zigbee 표준에서도 이슈로 남아 있는 상태이다.

2. 센서 네트워크용 표준 인터페이스

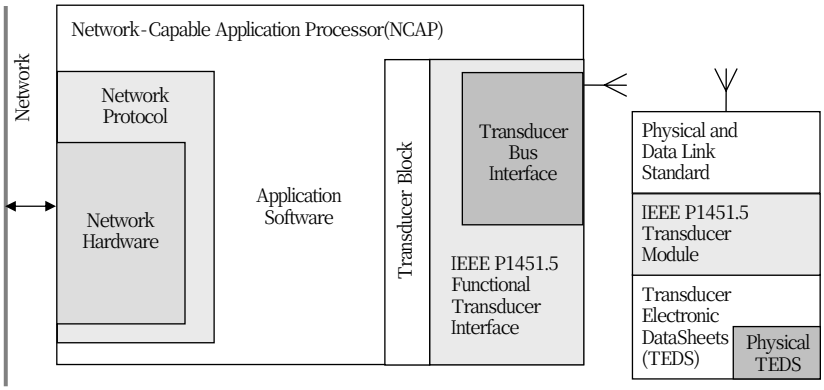
현재 운용되고 있는 센서 네트워킹은 대부분 업체 고유의 기술을 사용함으로 인해 센서, 컨트롤러, 인터페이스 관련 표준이 없었으나, IEEE P1451 하에 이에 대한 표준을 주도해오고 있다. 이 표준은 트랜스듀서 버스와 서로 다른 네트워크 버스 사이의 인터페이스 역할을 하는 NCAP(Network-Capable Application Processor)을 사용하여 모든 센서가 표준의 인터페이스를 갖도록 정의하고 있다.

IEEE P1451 산하의 IEEE P1451.5에서는 무선 인터페이스의 표준에 대한 필요성을 인식하고, 다양한 무선 기술을 통합 적용시킬 수 있는 무선 통신 표준으로 (그림 4)에 도시한 바와 같이 규격을 발표하였다[7]. 하지만 이 표준에서는 무선 통신 물리 계층 규격으로는 IEEE 802.11, IEEE 802.15.1의 Bluetooth, IEEE 802.15.4의 Zigbee 규격 등이 제시되었으나, IEEE 802.15.4가 유력한 상태이며 이와 맞물린 보안 규격이 고려될 것이다. 즉, 아직까지는 개별 망 형태의 센서 네트워크들이 혼재되어 있는 상태이지만 표준화된 센서 인터페이스를 가지면서 보안 서비스가 가능하도록 진화할 것이다.

3. 키 관리 메커니즘과 보안 프로토콜

일반적으로 두 노드 사이의 안전한 통신을 위해서는 별도의 복잡한 키 관리를 필요로 하지 않는 공개키 방식을 많이 사용하고 있으나, 센서 네트워크 환경에서는 제약사항이 많은 Ad-hoc 네트워크로 이를 그대로 활용하기가 매우 어렵다. 이런 이유로 센서 네트워크 키 관리와 보안 프로토콜에서는 대칭키 방식의 암호 방법을 이용하는 방법이 대부분 제안되고 있다.

센서 네트워크 보안 프로토콜로 초기에 발표된 SPINS 프로토콜은 SNEP(Secure Network Encryption Protocol)과 μTESLA(Timed Efficient Stream Loss-tolerant Authentication)를 이용한 구조이다. SNEP를 이용하여 데이터의 기밀성과 노드 간 데이터 인증 과정, 그리고 과거에 사용된 데이터의 재사용 공격이 불가능하도록 하기 위한 키 재설정(freshness) 기능을 제공한다. TESLA 프로토콜의 변형된 형태인 μTESLA 프로토콜은 키를 알고



(그림 4) IEEE P1451.5 무선 규격

있는 노드에 의해 해석이 가능하도록 하는 대칭키 기반의 인증 방식을 제공한다[8],[9]. 이 μTESLA는 두 노드 사이에 공유하여야 하는 비밀키의 노출을 최대한 늦춤으로써 비대칭 암호키 방식을 사용하는 듯한 효과를 누릴 수 있다. 하지만 이 방식은 인증하여야 하는 노드 수가 많아질 경우에는 지연 시간이 길어져서 활용이 어렵고 각 노드간 시간의 싱크 과정도 필요하다는 단점이 있다.

하나의 키를 사용하는 메커니즘으로는 대량의 센서가 흩어져 있는 센서 네트워크에서는 안전한 키 메커니즘의 설계가 어렵다는 판단으로, 4개의 암호키와 키 설정 프로토콜을 가진 LEAP(Localized Encryption and Authentication Protocol) 프로토콜에 제시되었다[10]. 각각의 암호키는 아래와 같다.

- 개인키: 베이스 스테이션과 공유하는 키
- 그룹키: 네트워크에 있는 모든 노드와 공유하는 브로드캐스팅 키
- Pairwise 키: 다른 센서 노드와 공유하는 키
- 클러스터 키: 몇 개의 이웃노드와 공유하는 키

이 방법은 공격 노드는 개인키를 알 수 없으며, pairwise 키와 클러스터 키는 주위의 이웃 노드를 인증하기 위해서만 사용되고 그룹키는 방송되는 메시지를 복호화하기 위해서만 사용되므로, 위협 노드를 가진 센서 네트워크의 생존성을 극대화 할 수 있는 방법이다.

4. 시큐어 라우팅

Ad-hoc 환경의 센서 네트워크에서 저전력 센서 노드를 구현하기 위해서는 네크워크 경로를 찾기 위한 라우팅 오버헤드를 최소화하여야 하며, 현재 모바일 Ad-hoc과 관련된 연구와 표준화는 이 분야에 집중되어 있다. 모바일 Ad-hoc 라우팅 기법은 DSDV처럼 노드들의 라우팅 정보를 테이블 형태로 관리하는 선행적(proactive) 프로토콜과 AODV처럼 필요에 따라 라우트 요구 패킷을 네트워크 전체에 보낸 후 이를 토대로 목적지 경로를 찾는 방식인 반응적(reactive) 라우팅으로 나뉜다.

하지만 센서 네트워크는 이러한 Ad-hoc 특성 이외에 센서 노드들의 자가 구성적 능력, 제한된 자원과 데이터 흐름이 주로 이루어지는 특성을 가지므로 Ad-hoc 라우팅 프로토콜들은 무선 센서 네트워크에 적합하면서 보안성이 강화된 라우팅 프로토콜로 변형되어야 한다. 이러한 라우팅 프로토콜에는 센서 노드가 원하는 데이터 정보를 모든 센서에게 flooding한 후 이들로부터 라우팅 정보를 전송받는 directed diffusion 방식과 네트워크를 클러스터링 기반으로 다수의 영역으로 분할하여 각각의 영역내 특정 센서 노드에 헤드의 역할을 부여하여 라우팅을 수행하는 LEACH(Low-Energy Adaptive Clustering Hierarchy) 등이 있다[11],[12].

이러한 센서 네트워크에서의 네트워크 계층 이상에서 이루어질 수 있는 공격은 크게 Bogus routing information, Sinkhole, Sybil, Wormhole, Selective forwarding, HELLO flood 등으로 나뉠 수 있으며, 프로토콜에 따른 공격 유형을 분류하면 <표 1>과 같다[13].

- Bogus routing information: 라우팅 메시지를

<표 1> 센서 네트워크 라우팅 프로토콜의 공격 유형

프로토콜	관련 공격
TinyOS Beaconing	Bogus routing information, selective forwarding, sinkholes, Sybil, Wormholes, HELLO floods
Directed diffusion and its multipath variant	Bogus routing information, selective forwarding, sinkholes, Sybil, Wormholes, HELLO floods
Geographic routing (GPSR, GEAR)	Bogus routing information, selective forwarding, Sybil
Minimum cost forwarding	Bogus routing information, selective forwarding, sinkholes, Wormholes, HELLO floods
Clustering based protocols(LEACH, TEEN, PEGASIS)	Bogus routing information, selective forwarding, sinkholes, Sybil, Wormholes
Rumor routing	Bogus routing information, selective forwarding, sinkholes, Sybil, Wormholes, HELLO floods
Energy conserving topology maintenance(SPAN, GAF, CEC, AFECA)	Bogus routing information, Sybil, HELLO floods

스푸핑, 변경 또는 재전송하여 라우팅을 교란시켜서 에러를 고의로 발생시키거나 라우팅 루푸를 형성하거나 라우팅 정보의 전송을 지연시킴으로써 통신을 방해함

- Selective forwarding: 특정 메시지(또는 노드)에 대한 전달을 거부하거나 삭제하는 공격
- Sinkholes: selective forwarding과 같이 사용하여 라우팅 정보를 변경하여 공격자의 노드(sinkhole)로 모든 데이터들이 지나가도록 조작하여 엿듣기가 가능함
- Sybil: 하나의 노드가 다른 노드에게 여러 식별자로 인식하도록 하는 공격으로 geographic routing에 치명적인 공격
- Wormholes: 실제로는 존재하지 않는 노드 연결이 있는 것처럼 인식하게 하는 공격으로 엿듣기 공격이나 selective forwarding과 같이 활용됨
- HELLO floods: 멀리 있는 공격자가 강한 강도의 신호로 HELLO 패킷을 보냄으로써 가까운 곳에 위치하지 않는 공격자에게 패킷을 보내도록 하는 방법

5. 시큐어 정보 집합

일반적인 센서 네트워크에서는 노드들이 생산해낸 센서 정보들을 가공없이 모두 전송함으로써 통신 부하를 준다. 하지만 이러한 정보를 모두 전송하는 것보다는 한 곳에 모아서 의미있는 데이터로 수집하여 전송하는 것이 통신 부하를 줄일 수 있는 방법이다. 센서 노드에서 센싱된 측정치를 중간값 또는 평균값, 최고/최저값, 결과값의 합 등을 구해서 네트워크에 부하를 주지 않은 수준의 집합 정보로 만들어 전송하는 것이 센서 네트워크에서의 정보 집합이다. 하지만 이 경우도 센서 노드의 불순한 의도에 의해 대량의 데이터를 발생하여 네트워크를 무력화하거나 불순한 의도의 집합자 또는 센서에 의한 오차범위 내의 데이터를 임의로 주입하여 센싱 정보에 대한 위·변조 역시 가능하므로 정보보호는 매우 중요하다. 센서들과 하나의 집합자, 그리고 하나의 서버가 있다는 가정 하에, 각각의 센서는 서버와 공유하는 키, 집합자와 공유하는 암호키를 가지고 있으며, 센서 노드는 자신의 센싱 정보를 집합자에 보내도록 하고 집합자는 이러한 정보의 집합된 정보를 계산하여 이 데이터가 정확함을 검증할 수 있는 정보와 함께 서버에 전하는 시큐어 정보 집합(secure information aggregation) 모델이 제시되었다[14].

Ⅳ. 결 론

u-센서 네트워크 기술은 온도, 습도, 압력, 성분, 소리 등을 감지하는 센서 관련 기술과 센싱 정보를 센서 노드간 전달하고 공유하기 위한 라우팅을 비롯한 통신 프로토콜 기술과 센서 응용에 따른 이동성 제공 기술 등이 융합된 복합 기술이지만 서비스 관점에서의 보안과 연계된 체계적인 연구는 부족한 상태이다. 따라서 센서 네트워크 정보보호 기술 개발은 각 발전 단계에 따라 달라질 수 있는 센서 노드, 전송 메커니즘, 센서 OS, 응용 서비스의 제원들을 파악하여 개발 초기단계부터 보안 기능에 대한 고려가 충분하여야 한다. 즉, USN의 초기 단계인 RFID 기반 센서 네트워크 기술개발 단계에 적절한 보안 서비스를 제공하느냐에 따라 센서 네트워크가 우리나라의 초고속 인터넷을 능가하는 IT 분야의 새로운 인프라로 자리잡을 수 있는지 여부가 판가름 날 것이다.

지금까지 살펴본 바와 같이 센서 네트워크의 정보보호 기술은 크게 센서 노드에 대한 보안, 시큐어 라우팅과 정보집합, 키 관리 및 인증 그리고 보안 프로토콜 기술로 분류될 수 있으며, 키관리와 인증은 센서 노드의 제한적인 컴퓨팅 능력을 고려한 대칭키 기반의 연구에 집중되어 있다. 하지만 공개키의 비밀 정보를 각 노드에 분산하여 저장하고 관리하는 threshold cryptography 기법과 같이 노드들이 협력하여 키 관리가 가능한 방식을 포함하여 소출력/저성능의 센서에서도 충분히 수행 가능한 공개키 방식에 대한 연구는 매우 중요하다.

2004년 라스베가스에서 열린 블랙햇 회의에서 시연된 RFID dump에서 보듯이 센서 정보의 접근이

비교적 손쉬운 개방된 센서 네트워크는 공격 위협을 조기에 찾아내고 방지할 수 있는 보안 관리와 서비스 거부 공격에 충분히 감내할 수 있는 구조는 필수적이며, 이러한 보안 개념이 설계 시부터 적절하게 반영되어야 한다. 아울러 유비쿼터스 보안 환경에 걸맞는 법과 제도 정비가 선행된 상태에서 USN 정보보호 기술 개발이 이루어져야 함은 물론이다.

참 고 문 헌

[1] 정보통신부, "국민소득 2만불로 가는 길 IT839 전략," 2004.

[2] WWRF home page, http://www.wireless-world-research.org

[3] 김정곤, "WWRF에서의 근거리 무선통신 표준화 기술," *IT Standard Weekly*, 2004-36호, 2004. 7.

[4] Tieyan Li, "Security Map of Sensor Network," http://www.i2r.a-star.edu.sg/icsd/SecureSensor/papers/security-map.pdf, Aug. 2004.

[5] TinySec home page, http://www.cs.berkeley.edu/~nks/tinysec/

[6] ZigBee Document 03322r6ZB, Security Services Specification Release0.80, April 2, 2004.

[7] IEEE 1451.5 home page, http://grouper.ieee.org/groups/1451/5

[8] Adrian Perrig et al., "SPINS: Security Protocols for Sensor Networks," *Proceedings of Seventh Annual International Conference on Mobile Computing and Networks*, July 2001.

[9] Adrian Perrig et al., "Efficient Authentication and Signing of Multicast Streams over Lossy Channels," *IEEE Symposium on Security and Privacy*, May 2000.

[10] Sencun Zhu, Sanjeev Setia, and Sushil Jajodia. "LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks," *In Proc. of the 10th ACM CCS'03*, Oct. 2003.

[11] C. Intanagonwiwat et al., "Directed Diffusion for Wireless Sensor Networking," *IEEE/ACM Transactions on Networking*, Vol.11, No.1, Feb. 2003, pp.2-16.

[12] Wendi B. Heinzelman et al., "An Application-Specific Protocol Architecture for Wireless Microsensor Networks," *IEEE Trans. on Wireless Communications*, Vol.1, No.4, Oct. 2002, pp.660-670.

[13] Chris Karlof and David Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," *First IEEE International Workshop on Sensor Network Protocols and Applications*, May 2003.

[14] B. Przydatek, D. Song, and A. Perrig, "SIA: Secure Information Aggregation in Sensor Networks," SenSys 2003.

[15] RFDUMP home page, http://www.rf-dump.org/