情 報 保 護 學 會 誌
第 16 卷 第 6 號, 2006. 12

IP-USN 최신 기술 동향 및 보안요구사항 분석

김 학 범*

요 약

USN(Ubiquitous Sensor Network) 기술은 유비쿼터스 사회의 기반이 되는 중요한 기술 중의 하나로 USN 기술을 통해 산업 구조와 시장 구조에 전반적인 큰 변화를 가져올 것으로 예상된다. 본 고에서는 중요성 점증되고 있는 IP-USN 관련하여 표준화 현황으로서 IEEE 1451 워킹그룹, IEEE 802.15 워킹 그룹, ZigBee Alliance 및 IETF 6LoWPAN 워킹 그룹에서 추진 중인 내용에 대하여 고찰한다. 또한 관련 기술 및 IP-USN에서 요구되어지는 보안기술에 대해서 고찰한다.

Ⅰ. 서 론

USN(Ubiquitous Sensor Network) 기술은 유비쿼터스 사회의 기반이 되는 중요한 기술 중의 하나로 USN 기술을 통해 산업 구조와 시장 구조에 전반적인 큰 변화를 가져올 것으로 예상된다.

IP-USN은 인터넷 프로토콜-유비쿼터스 센서 네트워크(Internet Protocol-Ubiquitous Sensor Network)의 약어로 기존의 IP 인프라를 기반으로 광범위한 확장성을 제공하고 센서 노드, 게이트웨이 및 싱크 노드의 이동성을 보장하는 USN 서비스이다.

이와 관련해 국제 표준화 단체인 IETF 6LowPAN 워킹그룹이 관련 표준화 작업을 진행 중이며 경쟁 기술로 업체 연맹(얼라이언스)이 주축이 된 지그비(ZigBee)가 있다. 지그비가 소규모 센서 네트워크에 적합하다면 IP-USN은 U시티와 같은 대규모 네트워크에 유용하며 기존 인터넷 서비스와 바로 연계되는 장점이 있다.

IP-USN은 현재 인터넷과 IPv6 기반의 BCN, 3G, 4G, PLC 등과 같은 다양한 미디어를 통합해 주는 최적의 기술로 U시티 등 대규모 네트워크에 적합한 기술로 주목을 받고 있다. 특히 IP-USN 관련 표준화 단체인 IETF 6LowPAN 워킹그룹이 금년말부터 본격 작업할 표준화 작업(보안 등) 11개 안 가운데 우리나라가 제출한 안이 무려 6개에 달해 IP-USN의 활성화 여부에 이목이 쏠리고 있다. 이 표준안에는 삼성전자, 아주대학교, 한국전산원 등이 참여했다[1].

본 고에서는 중요성 점증되고 있는 IP-USN 관련하여 표준화 동향 및 기술 현황과 함께 관련 보안 기술에 대해서 고찰한다.

Ⅱ. USN 관련 표준화 동향

1. IEEE 1451 워킹 그룹

IEEE 1451 워킹 그룹은 '93년 9월 NIST와 IEEE의 기술 위원회를 중심으로 하여 스마트 센서 통신 인터페이스의 표준에 대한 논의를 시작으로 각 5개의 워킹 그룹을 통해 표준화가 진행되었으며, 현재 7개의 워킹 그룹이 활동하고 있다. 각 그룹의 목적은 표 1과 같다.

IEEE 1451 워킹 그룹은 '97년에 발표된 P1451.2 워킹 그룹의 'IEEE Std 1451.2-1997' 표준문서를 시작으로 각각의 그룹을 통해 표준문서가 작성되어, 1999년에는 'IEEE Std 1451.1-1999', 2003년에 'IEEE-Std 1451.3-2003', 2004년에 'IEEE Std 1451.4-2004'가 각각 공개되었다. 현재, P1451.5, P1451.6 워킹 그룹에서 표준화가 진행되고 있다[2].

2. IEEE 802.15 워킹 그룹

IEEE 802.15 워킹 그룹은 무선 개인 영역 네트워크(Wireless Personal Area Networks, WPAN) 또는 단거리 무선 네트워크를 위한 표준화를 목표로

* 순천향대학교 정보보호학과 (khb0305@sch.ac.kr)

〔표 1〕 IEEE 1451 워킹 그룹의 목적

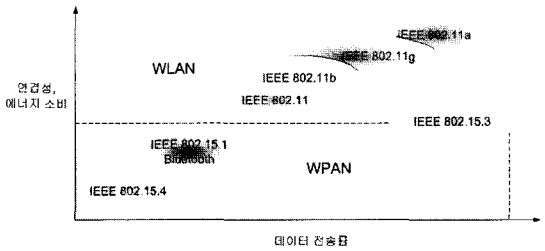
구 분	목 적
P1451.0	· 네트워크에 독립적인 지능형 변환기 객체 모델 정의
P1451.1	· 네트워크 화된 지능형 변환기 및 각 모델을 대표하는 클래스의 소프트웨어 인터페이스를 위한 공통의 오브젝트 모델 정의 · NCAP(Network Capable Application Processor) 정의
P1451.2	· 낮은 신호 대역폭을 요구하는 변환기의 인터페이스 정의 · STIM(Smart Transducer Interface Module), TEDS(Transducer Electronic Data Sheet) 정의
P1451.3	· 분산형 멀티드롭 시스템을 위한 디지털 통신 방식 정의
P1451.4	· 아날로그와 디지털 형태의 신호로 통신할 수 있는 혼합 방식의 변환기 인터페이스 표준 정의
P1451.5	· IEEE 802.11(WiFi), IEEE 802.15.1 (Bluetooth), IEEE 802.15.4(ZigBee) 프로토콜을 물리 계층으로 사용하는 무선 센서 인터페이스를 정의
P1451.6	· 멀티채널 모듈을 위한 CANopen에 기반을 둔 네트워크 형성

한다. WPAN은 PC, PDA, 셀룰러 폰 등의 무선 이동 기기간의 통신을 가능하게 하며, 다른 무선 통신 기술에 비해 에너지 소비가 낮고 저가이기 때문에 센서 네트워크에 도입되기에 적합한 통신 기술로 부각되고 있다. 특히, IEEE 802.15.4 표준은 센서네트워크에서 가장 적합한 통신 기술로 인정받고 있으며, 현재 ZigBee와 6LoWPAN의 MAC(Medium Access Control)/PHY (Physical layer) 표준으로 사용되고 있다[3].

무선 랜과 무선 개인 영역 네트워크에서 사용되는 통신 기술에 대한 비교는 표 2 및 그림 1과 같다.

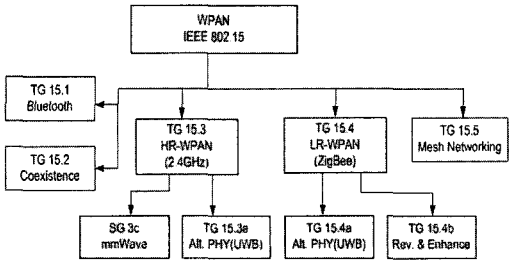
〔표 2〕 통신 기술 비교[4]

	802.11b WLAN	802.15.1 블루투스	802.15.4 LR-WPAN
통신 거리	100m 이내	10-100m	10m
데이터 전송률	2-11 Mbps	1 Mbps	250 kbps
에너지 소비	보통	낮음	아주 낮음
크기	큼	작음	가장 작음
비용 및 복잡성	높음	보통	낮음



〔그림 1〕 통신 기술에 따른 데이터 전송률, 연결성, 에너지 소비 비교[5]

그림 2는 IEEE 802.15 워킹 그룹의 구성을 나타내며, 표 3에는 각 그룹의 역할이 요약되어 있다.



〔그림 2〕 IEEE 802.15 워킹 그룹 구성

IEEE 802.15 TG1은 블루투스(Bluetooth) v1.1을 기반으로 WPAN을 구성한다. 표준은 블루투스의 하위 트랜스포트 계층인 L2CAP(Logical Link Control and Adaptation Protocol), LMP (Link Manager Protocol), 기저대역(baseband) 및 물리계층을 정의하며, 이동 기기들의 단거리 RF기반의 연결성을 제공한다. 또한, ISO 8802-2 LLC(Logical Link Control)를 위한 LLC/MAC 인터페이스를 포함하는 SAP(Service Access Point)를 정의한다.

IEEE 802.15 TG2는 WPAN과 WLAN(Wireless Local Area Networks)의 공존에 대한 연구를 수행한다. TG2에서는 WLAN과 WPAN의 상호 간섭을 정량화하기 위한 'Coexistence Model'과 WLAN과 WPAN의 공존을 용이하게 하는 'Coexistence Mechanism'을 개발하였다.

IEEE 802.15 TG3는 고속의 WPAN에 대한 연구를 진행한다. TG3에서는 MAC과 PHY를 정의하며, 데이터 전송 속도는 11~55Mbps 정도이고 이동 기기에서 이미지 및 멀티미디어 응용 서비스 제공에 초점을 맞추고 있다. TG3의 표준 제정 이후, TG3은 TG3a와 TG3b로 분리되어 운영되고 있다.

〔표 3〕 IEEE 802.15 워킹 그룹 산하의 Task Group

구분	Task Group	업무
IEEE 802.15	WPAN (TG1) 블루투스	• 10미터 정도 근거리에서의 무선 통신 기술에 대한 표준 제정 • MAC & PHY 블루투스 규격 채용
	Coexistence (TG2)	• WPAN과 WLAN과의 전파 간섭 축소 방법 연구
	High Rate(TG3)	• 20Mbps 이상의 전송률 지원을 위한 MAC 및 PHY 연구 • 2.4GHz ISM 대역. (11,22, 33,44,55Mbps까지 전송)
	High Rate (TG3a), Alt. PHY UWB	• TG3에서 PHY를 100Mbps 이상 고속화하기 위한 alternative PHY(UWB) 연구
	mmWave (SG3c)	• TG3a에서 밀리미터파(60GHz)를 활용한 초고속alternative PHY 연구
	Low Rate (TG4) ZigBee	• 최대 전송 속도 20~250Kbps의 MAC 및 PHY 연구 • 2.4GHz ISM 대역, 868/915MHz Dual PHY
	Low Rate(TG4a) alt. PHY UWB	• UWB PHY를 이용한 저속 위치인식 네트워킹 연구
	Mesh Networking (TG5)	• WPAN에서 메쉬 네트워킹을 위한 MAC 및 PHY 연구

IEEE 802.15 TG4는 데이터 전송률이 낮고 수개월 또는 수년간 지속되는 배터리를 이용하는 저가의 장비를 위한 데이터 표준을 제정한다. TG4에서 정의한 MAC과 PHY는 ISM(industrial, scientific and medical) 밴드에서 동작하며 센서, 장난감, 스마트 뱃지, 무선 컨트롤러 등에 사용가능할 것으로 예상된다[3]. 2003년에 발표된 'IEEE Std 802.15.4-2003'[6] 표준에 따르면 TG4의 MAC과 PHY는 250kbps 이하의 데이터 전송률을 지원하며, 2개의 주소 모드, 네트워크 설정 자동화, 낮은 에너지 소비 등의 특징을 갖는다. TG4의 표준 제정 이후, TG4는 TG4a와 TG4b로 분리되어 운영되고 있다.

IEEE 802.15 TG5는 WPAN의 메쉬 네트워킹(mesh networking)을 위해 PHY와 MAC 계층에서 필수적으로 제공되어야 하는 메커니즘들을 정의하기 위한 그룹이다. 다른 그룹에 비해 늦게 구성되었으며, 아직까지 특별한 성과는 보이지 않고 있다.

〔표 4〕 IEEE 802.15 워킹 그룹에서 제정한 표준 현황

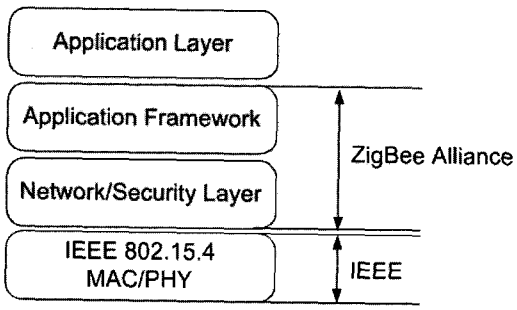
그룹	문서 제목	최종 버전
IEEE 802.15.1	Part 15.1: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Wireless Personal Area Networks (WPANs)	2005 (개정)
IEEE 802.15.2	part 15.2: coexistence of wireless personal area networks with other wireless devices operating in unlicensed frequency bands	2003
IEEE 802.15.3	part 15.3: wireless medium access control (MAC) and physical layer (PHY) specifications for high rate wireless personal area networks (WPANs)	2003
IEEE 802.15.4	part 15.4: wireless medium access control (MAC) and physical layer (PHY) specifications for low-rate wireless personal area networks (LR-WPANs)	2003

3. ZigBee Alliance

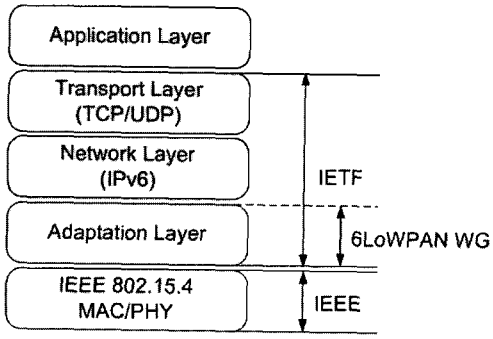
ZigBee Alliance의 프로모터는 Chipcon, 필립스(Philips), 미쓰비시(Mitsubishi), 모토로라(Motorola), Honeywell, Freescale, Ember, 삼성으로 구성되어 있으며, 100개 이상의 참여 기업이 존재한다. 국내에서도 LG, TTA, 한국무선네트워크(korwin), 한국전자통신연구원(ETRI) 등 다수의 기업 및 연구단체가 참여 기업으로 활동하고 있다[7].

ZigBee Alliance는 2003년 완성된 IEEE 802.15.4 표준을 기반으로 저전력 무선 네트워킹이 가능한 모니터링 및 제어(control) 제품을 위해 상위 프로토콜 표준을 정의하는 것을 목표로 한다.

ZigBee Alliance는 ZigBee 네트워크를 구성하기 위해 그림 3과 같이 네트워크 계층, 응용프로그램을 지원하기 위한 응용 지원 부계층(Application support sublayer), 응용 프레임워크(Application Framework), 보안 계층, ZDO(ZigBee Device Object)등에 대한 표준화를 진행하여, 2005년 6월에 ZigBee 표준 1.0 버전을 완성하여 공개하였다[8]. ZigBee는 IEEE 802.15.4 표준을 기반으로 하며 네트워크 계층에서 응용 계층까지 모든 계층을 정의하고 있다.



〔그림 3〕 ZigBee Alliance 표준화 작업 범위



〔그림 4〕 6LoWPAN 워킹 그룹 작업 범위

4. IETF 6LoWPAN 워킹 그룹

2004년까지 소형 장치의 통신을 위한 표준은 Bluetooth나 ZigBee와 같이 업계의 제휴에 의해 다뤄지고 있었다. 그러나 2004년 하반기에 이르러 소형 장치에서 IP(Internet Protocol)를 사용하는 방안에 관한 새로운 워킹 그룹에 많은 관심이 몰리기 시작했다. 이에 힘입어 2004년 11월 10일 미국 워싱턴에서 열린 61번째 IETF 정기 회의에서 6LoWPAN (IPv6 over Low power WPAN)의 첫 번째 BOF(Bird Of a Feather)가 시작되었다. 그리고 2005년 3월 62번째 IETF 정기 회의에서 인벤시스(Invensys)의 Geoff Mulligan을 의장으로 하여 워킹 그룹이 시작되었다[9].

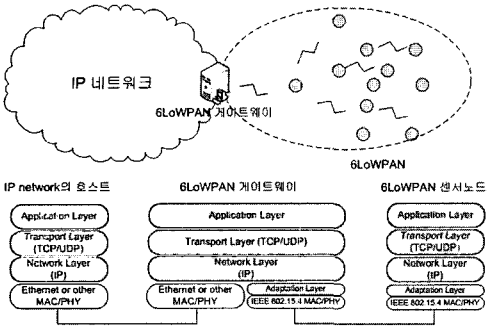
6LoWPAN 워킹 그룹의 목적은 IEEE 802.15.4 MAC/PHY 상위 계층으로 IP 및 TCP/UDP 등의 기존 인터넷에서 사용하는 통신 프로토콜을 이용하는 환경에서의 IPv6 패킷 전송 방안을 결정하는 것이다. 6LoWPAN은 IPv6를 사용하기 때문에 기존에 구축된 인프라를 그대로 이용할 수 있다. 따라서 추가 비용이 절감될 뿐만 아니라 잘 알려지고 검증된 IP 기술들을 많은 수정 없이 사용할 수 있다. 또한, IPv6의 큰 주소 공간과 자동 주소 설정과 같은 기능을 LoWPAN에 적용하는 데에 유리하다. 마찬가지로 IEEE 802.15.4를 기반으로 동작하는 ZigBee의 경우에도 IPv6를 적용하는 방안이 연구되고 있지만, 무겁고(64k) 비용이 많이 들며 복잡하여 6LoWPAN의 대안이 되지는 못할 것으로 내다보고 있다. 인텔(Intel)의 경우에도 처음에는 ZigBee Alliance에 참여하였지만 여러 가지 문제점들로 인해 ZigBee Alliance에서 나오게 되었다. 위와 같은 이유로 인해 최근 6LoWPAN에서 활동하고 있는 기업의 수가 증가하고 있다. 현재 국외의 마이크로소프트, 인텔, 선 마이크로 시스템즈 등과 국내의 삼성, 아주대학교, 한국전산원 등의 기업 및 대학, 연구단체에서 적극적으로 참여하고 있다. 6LoWPAN 워킹 그룹이 표준화 작업을 수행하는 범위는 그림 4와 같다.

현재 6LoWPAN 워킹 그룹에서는 6LoWPAN의 문제점 및 목표, IPv6 패킷 전송 방법에 대해 2건의 워킹 그룹 드래프트(draft)가 작성되었다. 금년 말에 개최되는 IETF 회의에서는 보안을 비롯한 11개의 문서가 제출되어 있다.

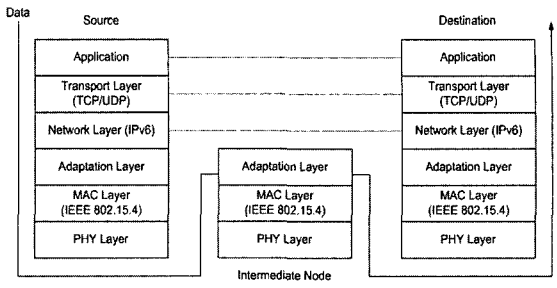
Ⅲ. IP-USN 관련 기술(6LoWPAN)

6LoWPAN은 IEEE 802.15.4 MAC/PHY 상위 계층으로 IP 및 TCP/UDP 등의 기존 인터넷에서 사용하는 통신 프로토콜을 이용하는 환경을 말한다. 6LoWPAN은 IEEE 802.15.4 MAC/PHY를 사용하기 때문에 패킷 전송에 있어서 여러가지 제약을 갖게 된다. LoWPAN의 특징은 다음과 같다[10].

① 작은 패킷 크기: 물리 계층 패킷 크기가 최고 127바이트로 주어진다. 따라서 MAC 계층에서 사용 가능한 프레임 크기는 102바이트이다.
② MAC 계층에서 16비트 주소 및 64비트 확장 주소를 지원한다.
③ 250kbps 이하의 적은 대역폭(bandwidth)
④ Star형 토폴로지와 메쉬(mesh) 토폴로지를 지원한다.
⑤ 일반적으로 저전력 배터리로 동작한다.
⑥ 비교적 저가형 센서와 스위치 등의 장비와 관련이 있다.



〔그림 5〕 6LoWPAN의 구조



〔그림 6〕 6LoWPAN에서의 데이터 전송

⑦ 기기들의 위치는 일반적으로 정해지지 않는다. 또한, 때때로 기기들에대한 접근성이 떨어질 수 있다.

⑧ LoWPAN 내의 기기들은 다양한 이유로 신뢰성을 보장받기 힘들다.

6LoWPAN에서 각 센서 노드는 IPv6 주소를 부여받기 때문에, 외부에 있는 IP 네트워크 내의 호스트가 6LoWPAN 내의 센서 노드를 제어할 수 있다. 그리고 6LoWPAN 내의 센서 노드 또한 외부의 IP 네트워크에 있는 서버와 통신을 수행할 수 있다. 즉, 센서 노드가 능동적으로(active) 외부와 통신을 수행하는 것이 가능하다. 궁극적으로 추구하는 6LoWPAN의 구조는 그림 5와 같다[3].

1. 네트워크 내에서의 데이터 전송

네트워크 내에서의 데이터 전송 시간에 가장 큰 영향을 미치는 것은 라우팅(Routing)을 어떤 계층에서 하는가이다. 소스에서 목적지까지 데이터가 전송될 때 거치게 되는 중간 노드들에서는 목적지를 찾기 위해서 경로를 탐색한다. 그러나 라우팅을 보다 상위 계층에서 하게 될수록 중간 노드를 거칠 때마다 거쳐야 하는 계층의 수가 많아지고 그에 따라 프로세싱 처리 시간이 커지게 된다. 프로세싱 처리 시간의 증가는 데이터 전송 시 지연(delay) 시간이 길어짐을 의미하기 때문에 라우팅과 같이 네트워크 연결에 관련된 기능은 최대한 하위 계층에 있는 편이 좋다.

6LoWPAN에서는 MAC계층에서 바로 위 계층인 adaptation 계층이 경로 탐색을 위한 기능을 가지고 있다. IPv6에서도 자체적인 라우팅 기능이 있지만 6LoWPAN 네트워크 내에서는 이 라우팅을 사용하지 않는다. 기존의 IP네트워크와는 다르게 네트워크 계층(IPv6)을 포함한 그 위 계층의 정보는 adaptation 계층의 페이로드가 되어 6LoWPAN 네트워크를 통과한다. 그로 인해 네트워크 계층, 트랜스포트 계층, 응용계층은 단대단 연결이 된다. 그림 6은 6LoWPAN 네트워크 내에서의 데이터 흐름에 대한 것이다.

2. 네트워크 주소 및 주소 할당

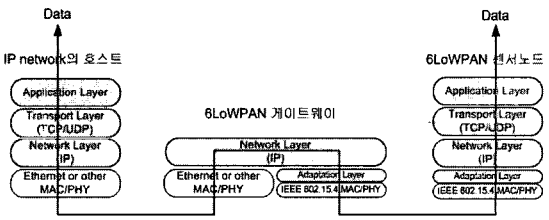
6LoWPAN의 각 노드들은 IPv6주소를 가지고 있다. 이 주소는 EUI-64 식별자를 이용해 자신이 IPv6 주소를 만들 수 있다. 이 주소는 6LoWPAN 네트워크 내에서만 아니라 전 세계적으로 유일한 주소가 된다. 즉, 6LoWPAN에서는 IPv6 주소를 사용하기 때문에 외부 네트워크와 연결 시 하나의 장치에 대한 식별에 대한 추가적인 기능이 필요하지 않다.

3. 라우팅 및 토폴로지의 확장성

6LoWPAN에서는 자신이 IPv6 주소를 할당하기 때문에 토폴로지의 제약이 없다. Mesh 구조의 네트워크를 자유롭게 형성할 수 있고 확장하기도 편리하다. 현재 6LoWPAN에서는 라우팅 기법에 대해서는 인터넷 드래프트로 LOAD(6LoWPAN Ad Hoc On-Demand Distance Vector Routing)가 제시되었지만 아직 이에 대해 자세한 표준화는 진행 되지 않고 있다. 그러나 ad hoc 네트워크와 유사점이 많은 6LoWPAN 네트워크의 특징 상 AODV(Ad hoc On-demand Distance Vector) 라우팅과 유사한 LOAD 혹은 이와 유사한 형태의 라우팅 알고리즘을 사용할 가능성이 높다.

4. 외부 네트워크와의 호환성 및 게이트웨이 구조

6LoWPAN의 게이트웨이는 그림 7과 같이 네트워크 수준에서 설계 할 수 있다. 이는 6LoWPAN이 IP 계층부터 응용 계층까지는 기존의 IP네트워크에서 사용하는 프로토콜을 그대로 이용하기 때문이다. ZigBee와 비교해 프로세싱 딜레이가 크게 줄어 들 수 있고, 설계의 간단함도 장점으로 꼽을 수 있다.



〔그림 7〕 6LoWPAN 게이트웨이의 구조

Ⅳ. IP-USN 관련 보안요구사항 분석

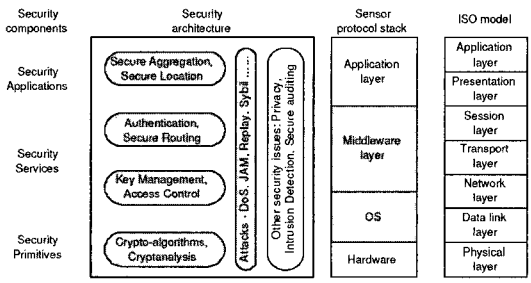
1. USN에서의 보안 요구사항

센서 네트워크는 무선 Ad-hoc 형태로써, 센서 정보를 통해 목적지까지 전달하기 위한 경로를 설정하거나 유지하는 라우팅시에도 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(mesh) 통신으로 이루어지는 센서 네트워크에서는 노드들의 상호 인증과 제한된 센서 자원을 이용하여 인증과 암호화에 사용될 암호키 관리 문제가 주 이슈중의 하나이다[11].

센서 노드에서의 보안 요구사항을 정리하면 다음과 같다[11].

① 암호키를 관리할 수 있는 기능을 제공하여야 한다.
② 센서 환경에 적합한 경량화된 암호 및 인증 기능을 제공하여야 한다.
③ 라우팅 시에 보안 기능을 제공하여야 한다.
④ 서비스 거부 공격에 강한 구조이어야 한다.
⑤ 사용자에 대한 위치 정보와 센서 노드의 집합 정보에 대한 암호 기능을 제공하여야 한다.

일부 기관에서는 그림 8과 같은 보안 구조를 제시하였으며, 위의 보안 기능 이외에 프라이버시와 침입 및 시큐어 감시 등도 추가 이슈로 정의하고 있다[12].



〔그림 8〕 센서 네트워크의 보안 구조

앞에서 언급한 요구사항을 만족시킬 수 있는 보안기술은 다음과 같이 나열할 수 있다[13].

① 키 관리 기술 : 자원의 제약성 등으로 인하여 PKI 등의 기존의 키관리 기술을 적용하기 어려우며, 다양한 키 관리 기법이 존재한다. 현재 SNEP (Secure Network Encryption Protocol)와 μTESLA(Timed Efficient Stream Loss-tolerant Authentication)를 이용한 구조인 SPINS(Security Protocols for Sensor Networks)[14] 프로토콜 등 센서 네트워크에 적합한 키 관리 기술에 대한 연구가 진행중이다.

② 경량 암호 및 인증 기술 : 센서 네트워크의 자원 제약성에 적합한 경량 암호 및 인증 기술이 필요한데, AES 대칭 암호 알고리즘인 경우, 경량으로 구현하는 경우, 128비트 암/복호화에 20μW 정도의 전력을 소비하면서, 수 msec 이내에 구현이 가능하다. 공개키 암호의 경우에는 RSA는 적용하기 어렵지만, ECC인 경우 저전력 버전으로 만들면 센서 노드에서 사용할 수 있을 가능성도 있다.

③ 라우팅 보안 기술 : 기존의 라우팅 프로토콜은 DOS 공격 및 packet injection, replay attack이 용이하여 사용이 부적합하며, 캡쳐된 노드에 의한 routing protocol tampering을 방지하는 경량 대칭키 암호 사용이나 Disjoint path를 통한 라우팅 공격 탐지 등의 보안 기술이 필요하다.

④ 물리적 공격 및 부채널 공격 방지 기술 : 센서 노드 개발시에 tamper-resistance 기술을 적용하며, 공격 받아 위조된 노드에 대한 사후 탐지 기술이 필요하다. 또한 부채널 장비를 위한 랜덤 마스킹 기법이나 부채널 공격 기술 감래형 암호 알고리즘과 코딩 기술이 필요하다.

⑤ DoS 공격 방지 기술 : 다양한 네트워크 공격(Sybil Attack, Sink Hole Attack, Flooding 등)과 H/W failure, S/W 버그 등의 공격이 발생할 수 있고 물리 계층에서 전송 계층까지 다양한 공격에 의해 결과적으로 일어날 수 있기 때문에 센서 네트워크의 현실적 측면을 고려한 DoS 공격 방지 기술이 필요하다.

⑥ 프라이버시 보호 기술 : 프라이버시 보호를 위해 법/제도, 정책뿐만아니라 PET(Privacy Enhancing Technology) 개발을 통한 기술적인 차원의 대응책이 필요하다.

2. 6LoWPAN에서의 보안요구사항

IPv6 over LowPAN(6LoWPAN) 응용에서는 비밀성 및 무결성 보호를 요구하는 경우가 있다. 이는 응용 계층, 전송 계층, 네트워크 및 링크계층(즉, 6LoWPAN의 규격집합 내)에서 제공될 수 있는데, 이 모든 경우에 우위를 점하는 제한사항이 특정 프로토콜 선택에 영향을 줄 수 있다. 몇가지 밀접하게 관련된 제한사항으로는 작은 코드 크기, 저전력 동작, 낮은 복잡도, 저대역폭 등의 요구사항이 있다.

주어진 제약환경 중에서 첫 번째로 6LoWPAN 장치를 위한 위협 모델이 의미 있는 가정과 단순화가 비용을 줄이기 위하여 필요하다. 위협에 관련된 예로는 man-in-the-middle-attack과 서비스 거부 공격 등을 들 수 있다.

필요한 보안요구사항들은 6LoWPAN 장치의 부팅 시에 적용할 수 있도록 네트워크에 적용된다. 이는 일반적으로 초기 키 설정을 위해서 응용-레벨의 교환이나 out-of-band 기법을 포함하며, 응용에 적합한 신뢰 모델에 의존할 수도 있기 때문에 6LoWPAN의 예외로서 고려될 수도 있다.

프로토콜의 다음번 집합을 설계 또는 선택하기 위해서 초기 키 설정에서 생성된 키 material의 공통 모델이 있어야 할 필요가 있다[10].

초기 키 설정을 제외하면 sebsequent 키관리 및 안전한 데이터 트래픽을 위한 프로토콜이 6LoWPAN의 범위에 포함된다. 또한 TLS, IKE/IPSec 등과 같은 방법들은 6LoWPAN 제약사항을 고려하여 평가되어야 한다.

링크 계층 보안을 사용하는데 있어서의 설득력 있는 주장은 대부분의 IEEE 802.15.4 장치들이 이미 AES 링크 계층 보안을 지원하고 있다는 것인데, AES는 고정된 길이의 블록에서 운용되는 블록 암호로서, 긴 메시지를 암호화 하기 위해서 몇가지 운용모드가 사용되어 질 수 있다. ECB, CBC, OFB 및 CFB와 같은 초기 모드들은 비밀성만을 제공할뿐 메시지 무결성을 보증하지는 않지만 CCM* 모드와 같은 것들은 비밀성과 메시지 무결성 둘다를 보장하기 위해 설계되었다.

6LoWPAN 네트워크는 이전의 어떤 모드에서도 운용될 수 있지만 가장 안전하고 효율적으로 수행하기 위해서는 적절한 모드(예를 들면 CCM*)를 탑재해야 한다.

네트워크 계층 보안을 우해서는 두가지의 모델이 적용가능한데 그 하나는 IPSec 전송 모드를 사용하는 end-to-end 보안이고, 나머지는 네트워크의 무선 부분에만 한정되는 보안으로 보안 게이트웨이를 사용하거나 IPSec 터널 모드를 사용하는 것이다. 후자의 경우에 있어서의 단점은 큰 헤더로 인하여 6LoWPAN 프레임 MTU가 무겁게 되는 문제가 있는데 6LoWPAN 구현을 단순하게 하기 위하여 관련 보안 모델을 파악하는 것이 유리하며 주어진 제약사항에 적절한 암호 suite 집합을 우선적으로 식별해야 한다.

IEEE 802.15.4 네트워크를 통한 IPv6 패킷의 전송상에서 고려하여야 할 보안사항은 다음과 같다[15].

EUI-64 MAC 주소로부터 인터페이스 식별자를 유도하는 방법은 가능한 글로벌한 유일성을 보호해야 하지만 고의에 의하든 위조한 것이든지 간에 복제로부터의 보호는 불가능하다.

IEEE 802.15.4 링크 내의 NDC(Neighbor Discovery)는 RFC 3756[16]에서 정의된 위협들을 허용할 수 있다. 메쉬 라우팅이 IEEE 802.15.4 네트워크에서 일반적인 것으로 예측되는데, [17]에 대해서 ad hoc 라우팅에 따른 추가적인 위협이 포함된다. IEEE 802.15.4는 몇가지의 링크 레벨의 보안을 제공하는데 사용자는 그러한 규정들이 가능하고 실제적이라면 사용하여야 한다. 그렇게 함으로써 위에서 언급한 위협들을 완화시킬 수 있다.

IEEE 802.15.4 장치의 많은 부분은 자신들의 PAN 내부에서 항상 통신을 해야 한다는 것이다. 비용과 전력 소모 관련된 고려사항에 대해서 IEEE 802.15.4 "Reduced Function Devices(RFDs)" 모델을 유지해야 하는데 이 장치들은 필요한 최소한의 특징만을 구현한다. 따라서 그러한 장치에 대한 보안은 IEEE 802.15.4의 링크 계층에서 정의된 메커니즘에 강하게 의존하게 된다.

그러나 IEEE 802.15.4 프레임의 인증 또는 암호화를 위하여 AES 모드만을 정의하면 특히 키관리와 같은 것은 정의되지 않는다.

다른 이슈들은 안전한 구성이나 관리에 관련된 실제 배치에 대한 내용들로 이들 내용들도 강제적으로 수용해야 하는 것들이다. 물론 FED(Full Function Devices) 장비들도 연합하거나 통합되어 구현될 수 있는데 이는 오프링크 IPv6 peer와 정기적으로 통신할 수 있다. 이러한 IPv6 장치들은 상용 메커니즘(IPSec, TLS 등)과 end-to-end 통신을 안전하게 할 수 있을 것이다.

RFC 3756에 정의된 신뢰 모델과 보안 위협 요소는 다음과 같다.

IPv6 ND(Neighbor Discovery) 프로토콜에 적절한 보안 방안을 제시하려면 먼저 실제 네트워크에 적용 가능한 신뢰 모델을 정의하고 그 신뢰 모델 환경하에서 발생할 수 있는 보안 위협 요소를 분석하여야 한다. 이에 2004년 5월 IPv6 ND 프로토콜에 대한 신뢰 모델(Trust Model)과 그에 따른 보안 위협 요소(Threat)를 정리하여 "IPv6 ND Trust Models and Threats(RFC 3756)"로 표준화 하였다[18].

신뢰 모델은 ND와 RD(Router Discovery) 프로토콜의 라우터 개입 여부에 따라 크게 3가지 모델로 정의한다.

① Corporate Intranet Model: 모든 노드들이 하나의 관리 도메인 하에 존재하며, 비공개 그룹을 형성하는 모델로서 모든 노드들이 IP 계층에서 서로 신뢰하여 잘못된 ND나 RD 메시지를 전송하지 않는다. 이 모델 하에서는 네트워크가 물리적으로 안전하거나 링크 계층에서 암호학적으로 보안이 제공된다면 굳이 IPv6 ND를 위한 보안이 필요하지 않다. 그러나, 물리적으로 안전하지 않거나 링크 계층의 보안이 만족할만한 수준이 되지 못한다면, IPv6 ND에 대한 보안이 필요하다.

② Public Wireless Network with an Operator: 호텔, 공항, 카페에서의 무선 LAN과 같이 공중 무선 네트워크를 관리하는 운영자가 있는 모델이다. 네트워크 내의 모든 노드들이 신뢰하는 라우터가 하나 이상 존재하며, 이 신뢰 라우터는 외부 네트워크와의 접속점 역할을 수행한다. 그러나, 클라이언트들 간에는 서로 신뢰하지 않으며, 잘못된 ND나 RD 메시지를 전송할 가능성이 있다. 클라이언트나 액세스 라우터 간에 강력한 보안 서비스를 제공함으로써 잘못된 메시지를 필터링할 수 있다.

③ Ad-hoc Network: 신뢰할 수 있는 운영자도 존재하지 않고, 모든 노드들이 서로 신뢰하지 않는 모델로서 상대방의 ND나 RD 메시지를 신뢰하지 않는다. 일반적으로, 노드들이 상대 노드들과 어떠한 신뢰 관계도 형성하고 있지 않아 기존의 전통적인 인증 메커니즘을 이용할 수 없다. 따라서, CGA(Cryptographically Generated Address)와 같은 스스로가 자신임을 확인해 줄 수 있는 메커니즘을 이용하여야 한다.

정의된 신뢰 모델 환경에서 발생할 수 있는 위협 요소들은 크게 다음 3가지 형태로 일반화할 수 있다.

① Redirect Attack: 공격자가 최종 목적지 노드나 라우터의 패킷을 링크상의 다른 임의의 노드로 리다이렉트시키는 공격

② Denial-of-Service(DoS) Attack: 공격자가 특정 노드가 다른 모든 노드나 특정 목적지 노드와 통신하지 못하도록 하는 공격

③ Flooding DoS Attack: 공격자가 다른 노드들의 패킷을 특정 노드로 리다이렉트시켜서 그 특정 노드에 Bogus 트래픽을 생성하는 공격

일반화된 위협 요소들을 좀 더 자세히 분석하여 도출하면 표 5와 같다.

〔표 5〕 ND 프로토콜에 대한 위협 요소

Threats	Attack	ND/RD	R/D	Msgs	1	2	3
Non Router/Routing Related Threats	NS/NA Spoofing	ND	Redirect	NA/NS	+	+	+
	NUD Failure	ND	DoS	NA/NS	-	+	+
	DAD DoS	ND	DoS	NA/NS	-	+	+
Router/Routing Involving Threats	Malicious Router	RD	Redirect	RA/RS	+	+	R
	Default Router Killed	RD	Redirect	RA	+/R	+/R	R
	Good Router goes BAD	RD	Redirect	RA/RS	R	R	R
	Spoofed Redirect	RD	Redirect	Redirect	+	+	R
	Bogus On-link Prefix	RD	DoS	RA	-	+	R
	Bogus Address Config Prefix	RD	DoS	RA	-	+	R
	Parameter Spoofing	RD	DoS	RA	-	+	R
Replay Attacks & Remotely Exploitable Attacks	Replay Attacks	All	Redirect	All	+	+	+
	Remote ND DoS	ND	DoS	NS	+	+	+

ND/RD : Neighbor Discovery/Router Discovery
R/D : Redirect/Dos
1 : Trust Model 1(corporate Intranet)
2 : Trust Model 2(Public operator run network)
3 : Trust Model 3(ad hoc network)
+ : 위협이 존재하고 적어도 하나의 해결책이 알려짐
- : 위협이 없거나 관련이 없음
R : 위협이 있지만 해결책은 연구 문제임

① Non router/routing related threats: ND, NUD(Neighbor Unreachability Detection)나 DAD(Duplicate Address Detection)와 같은 ND 고유의 기능을 수행할 때 발생할 수 있는 위협 요소로서 크게 다음과 같이 분류할

수 있다.

- Neighbor Solicitation/Neighbor Advertisement spoofing
- Neighbor Unreachability Detection failure
- Duplicate Address Detection DoS attack

② Router/Routing Involving Threats: RD나 다른 라우터와 관련된 메커니즘과 관련된 위협 요소로서 크게 다음과 같이 분류할 수 있다.

- Malicious last hop router
- Default router is "KILLED"
- Good router goes BAD
- Spoofed redirect message
- Bogus on-link prefix
- Bogus address configuration prefix
- Parameter spoofing

③ Replay Attacks & Remotely Exploitable Attacks: 위의 ND의 고유 기능이나 라우터와 관련된 위협 요소를 제외하더라고 ND나 RD 메시지 자체는 항상 Replay 공격이나 원격 ND DoS 공격에 노출되어 있다.

V. 결 론

USN 기술은 다가올 유비쿼터스 사회에서 사회적 기반 환경이 될 중요한 기술 중의 하나이며, USN 기술을 통해 전반적인 산업구조 및 시장 구조는 크게 변화할 것으로 예상된다. 정부는, 이처럼 산업으로의 파급 효과가 큰 USN 기술의 중요성을 인식하고, IT839 전략의 3대 인프라에 USN을 포함시켰으며, 관련 기술의 연구 개발을 적극적으로 지원하고 있다.

본 고에서는 중요성 점증되고 있는 IP-USN 관련하여 표준화 동향 및 기술 현황과 함께 관련 보안 기술에 대해서 살펴보았다.

표준화 현황으로서 IEEE 1451 워킹그룹, IEEE 802.15 워킹 그룹, ZigBee Alliance 및 IETF 6LoWPAN 워킹 그룹에서 추진 중인 내용에 대하여 고찰하였다.

해외에서 USN의 기반 기술이 되는 센서네트워크에 대한 연구가 활발히 일어나고 있는 것과 달리, 현재 국내에서의 USN 환경을 조성하기 위한 기반 기술에 대한 연구는 미미한 실정이다. 하지만, 센서네트워크를 기존의 인터넷과 연동하여 USN 환경을 구축하기 위한 연구는 세계적으로 시작단계에 놓여 있다. 또한 보안기술에 대한 중요성도 나날이 커지고 있기 때문에 현재 연구된 센서네트워크 기술을 분석하고, 이를 바탕으로 USN 기술 및 USN 응용 서비스 모델을 창출한다면, 유비쿼터스 사회에서도 정보 통신 강국으로서의 위치를 확고히 할 수 있을 것이다.

참 고 문 헌

[1] 김무종, "미래 U환경 구현 IP-USN 이목 집중", 디지털타임스 기사, 2006.9.22.

[2] NCA II-RER-05075, *RFID 및 USN에 IPv6 적용방안 및 활용 분야에 관한 연구*, 한국전산원, 2005.11.

[3] NCA V-RER-05022, *USN 기술 동향 분석 연구*, 한국전산원, 2005.11.

[4] 채동현, 한규호, 임경수, 안순신, "센서 네트워크의 개요 및 기술동향", 정보과학회지 제 22권 제12호, 12. 2004.

[5] 윤명현, "IEEE 802.15.4 무선 PAN 기술", 전자부품연구원(KETI), 7. 2005

[6] IEEE, "802.15.4 Wireless Medium Access Control(MAC) and Physical Layer(PHY) Specifications for Low-Rate Wireless Personal Area Networks(LR-WPANs)", IEEE Computer Society, 2003. 10.

[7] ZigBee Alliance 홈페이지, http://www.zigbee.org

[8] ZigBee Alliance, "ZigBee Specification v1.0", 2005. 6.

[9] www.ietf.org/ Pv6 over Low power WPAN (6LoWPAN) Working Group

[10] N. Kushalnagar, G. Montenegro, "6LoWPAN: Overview, Assumptions, Problem Statement and Goals", 2006. 8. (download available at http://tools.ietf.org/id/draft-ietf-6lowpan-problem-05.txt)

[11] 김신효, 강유성, 정병호, 정교일, "u-센서 네트워크 보안 기술 동향", 전자통신동향분석 제20권 제1호, 2005. 2.

[12] Tyeyan Li, "Security Map of Sensor Network", http://www.ir2.a-star-edu-sg/icsd/SecureSensor/papers/security-

map.pdf, 2004. 8
[13] 김호원, "USN 정보보호 요구사항 및 표준화 전략", 2006.5.
[14] Adrian Perrig et al., "SPINS : Security Protocols for Sensor Networks", Proceedings of Seventh Annual International Conference on Mobile Computing and hetworks, 2001. 7.
[15] N. Kushalnagar, G. Montenegro, "Transmission of IPv6 over IEEE 802.15.4 Networks ", 2006. 8. (download available at http://tools.ietf.org/id/draft-ietf-6lowpan-format-04.txt)
[16] RFC 3756, "IPv6 Neighbor Discovery (ND) Trust Models and Threats", 2004. 5
[17] Karlof, Chris and Wagner, David, "Secure Routing in Sensor Networks: Attacks and Countermeasures", Elsevier's AdHoc Networks Journal, Special Issue on Sensor Network Applications and Protocols vol 1, issues 2-3, 2003. 9.
[18] 박소희, 나재훈, 정교일, "IPv6의 SEND 표준화 동향", ETRI 주간기술동향, 통권 1165, 2004.9

〈著者紹介〉

사 진

김 학 범 (Hak-Beom Kim)
종신회원
1990년 8월 : 중앙대학교 대학원 컴퓨터공학과 졸업(석사)
2001년 2월 : 아주대학교 대학원 컴퓨터공학과 졸업(박사)
1991년 10월~1996년 6월 : 한국전산원 주임연구원
1996년 7월~2001년 8월 : 한국정보보호진흥원 기술표준팀장
2001년 9월~2003년 1월 (주)드림시큐리티 상무이사
2003년 2월~2005년 3월 (주)장미디어인터렉티브 상무이사
2005년 4월~현재 정보보호연구소 부소장
2001년 3월~현재 순천향대학교 공과대학 정보보호학과 겸임교수
관심분야 : 컴퓨터보안, 공개키 기반구조(PKI), 정보보호 표준화/평가, 스마트카드 보안, 유비쿼터스 보안