신뢰받는 u-Korea 구현을 위한 무선 정보보호 기술

한국전자통신연구원 정보보호연구단 나재훈, 정교일, 손승원

차 례

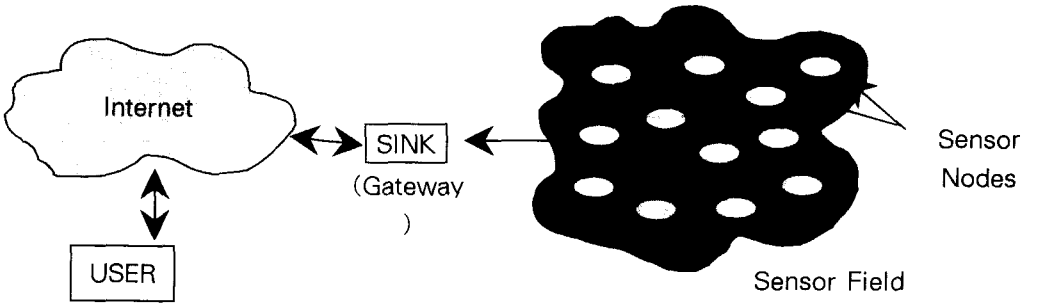
요 약

u-Korea 건설을 위한 요소 기술 가운데 무선을 기반으로 각 장치간의 정보를 주고 받으며 물리적 공간을 초월하여 사이버 공간을 구축하는 센서 네트워크가 으뜸이라고 하겠다. 이러한 센서 네트워크는 인프라가 없는 무형의 인프라를 구축하고 있으며 가변적이고 즉흥적인 면이 매우 강하다. 그러므로 이러한 네트워크의 구축, 서비스 제공 및 관리는 기존의 전통적인 방식과는 매우 다른 모습을 갖고 있으며, 그리고 센서의 크기가 비교될 만큼 작기 때문에 전통적인 방식의 보안 메커니즘을 그대로 적용하기가 어렵다. 본고에서는 센서 네트워크의 인프라, 보안 요구사항, 보안 메커니즘에 대하여 살펴보며 향후 센서 네트워크의 보안기술 개발 방향을 제시 하고자 한다.

1. 도 입

U-Korea 시대의 서비스를 제공하기 위한 인프라가 무엇인가 하고 생각을 하면, 사람에게 편리한 컴퓨팅 환경, 사람이 더 이상 학습을 하지 않고 사람의 지식을 이해하고, 사람이 처한 상황을 인지하여, 원하는 서비스를 예측하여 제공하는 인프라를 의미하는 것으로 정의를 할 수 있다.

U-Korea 구현을 위한 인프라로는 기존의 많은 인프라가 있지만 센서네트워크는 새로운 형태의 망을 구축하는 기술이 된다. 센서네트워크는 자율성을 갖고 있으며 전력을 절약하기 위하여



〔그림 2-1〕 센서 네트워크 인프라 구조

초소형 크기에 자연의 환경의 변화를 감지하도록 센서를 장착하고, 센서로부터 채득된 정보를 디지털화하여 이웃의 센서에게 전달하는 기본동작을 수행하는 3개의 콤포넌트로 구성된 전자 장치인 것이다. 그러나 이 장치 개발은 공교롭게도 미국 DARPA (Defense Advanced Research Projects Agency)의 MEMS (Micro Eletro Mechanical System) 프로젝트의 하나인 Smart Dust에서 출발을 하였다. 이 장치는 단순 정보 전달의 수단으로만 그치는 것이 아니라 로보트로의 발전을 염두에 두고 개발이 착수 되었으며 실제로 Smat Dust의 실체인 모트(Mote)에 팔을 달아서 움직이도록 한 장치가 개발 되어 있는 상태이다.

본 고에서는 센서네트워크의 인프라구조, 센서네트워크의 보안서비스 요구사항, 그러고 현재까지 이루어진 보안 메커니즘에 대한 특성을 살펴보며 앞으로 센서 네트워크의 기술개발의 방향에 대한 제언을 하고자 한다.

2. 본 론

2.1 센서 네트워크 인프라

센서 네트워크는 센서필드, 싱크, 그리고 전통적인 인터넷망 으로 크게 3개로 구분할 수 있다. 전통적인 인터넷 망은 현재까지의 전통적인 보안 메커니즘이 주요 개념으로 자리 잡고 있지만 유비쿼터스 컴퓨팅 서비스의 제공을 위해서는 진화를 해야만 하는 단계에 있다. 싱크는 일종의 베이스 스테이션과 같은 역할을 하여 센서 필드의 센서들이 얻은 정보를 전달 받아서 망의 사용자에게 전달하여 주고 또 역으로 사용자로부터의 정보나 프로그램을 다운하는 게이트웨이 위치에 있다.

센서 노드는 센서 네트워크를 구성하는 기본 요소로 온도, 습도, 물체이동, 밝기, 압력, 토양성분, 소리 등을 감지하는 센서들을 통해 관심 데이터를 수집하고 처리하여 상위 처리 시스템으로 전송해 주는 기술이다. 한정된 에너지원 내에서 동작하므로 전력 소모가 적어야 하고, 소형화로 어디든지 장착, 휴대가 가능하여야 하고, 밀도 높은 배치가 가능하기 위해서는 가격 또한 낮아야 한다. 센서 네트워크는 그 응용 범위가 다양하기에 여러 종류의 센서 노드들이 개발되었는데, 그 중에서도 버클리대의 MICA가 공개소프트웨어로 널리 참조되고 있다. MICA 센서 노드는 TinyOS라는 센서 노드용 운영체제와 NesC라는 응용 개발 환경과 함께 공개되었다. 또한, MICA는 RF 통신을 이용하여 센서 노드의 프로그램을 변경할 수 있도록 하여 센서 노드를 배치한 후 일일이 수거하여 프로그램을 변경할 필요가 없도

록 제작하였다. 그 외 Rockwell사의 WINS 노드, Sensoria사의 WINS NG2.0, UCLA의 iBadge, MIT의 u-AMPS 시리즈가 대표적인 센서 노드이다.

센서 노드들은 센서 네트워크를 통해 데이터들을 서로 주고 받는다. 이 센서 네트워킹 계층은 다음과 같다.

(1) 물리 계층(Physical Layer)

센서 노드들은 물리 계층을 공유하여 데이터 패킷을 다른 노드들과 주고 받는다. 주파수 선택, 캐리어 주파수 생성, 신호 감시, 데이터 암호화 및 변조 등의 기능을 수행한다. 전송하는 매체로는 ISM(Industrial Scientific Medical) band를 사용하는 Radio와 750~3000nm의 전자기파 적외선 및 광통신 매체 등이 있다. 앞으로 저전력 변조 기술 및 작은 크기, 저전력, 저가격의 하드웨어 설계 등의 연구가 필요하다.

(2) 데이터링크 계층(Data Link Layer)

데이터 흐름의 다중화, 데이터 프레임 검출, 매체 접근, 오류 제어 등의 기능을 수행하며, 점대점 또는 점대다수의 네트워크 구성에서 신뢰성을 보장해야 한다. 센서 네트워크에서의 MAC 프로토콜은 스스로 네트워크를 구성할 수 있어야 하며, 공평성과 전력이나 전송 효율이 높은 매체 접근 방법을 보장할 수 있어야 한다. 센서 네트워크에서 MAC 프로토콜은 충돌(Collision), 오버히어링(Overhearing), 과도한 컨트롤 패킷(Control packet overhead) 및 비활성시 수신(Idle listening)이 문제가 된다. 이러한 문제점을 해결하기 위해 대표적인 센서 네트워크 MAC 프로토콜로써 SMAC(Sensor Medium Access Control)이 제안되었다. SMAC에서는 노드가 주기적으로 슬립 모드와 리스닝 모드 사이를 반복하여 실제로 데이터를 전송할 때만 깨어나서 전송을 하고 나머지는 슬립 상태에서 전력 소모를 최소화한다. 이 방법은 비활성시 수신과 충돌, 오버히어링 등에 대한 문제는 해결하나 노드들간의 동기화가 이루어져야 한다는 단점이 있다. 그 외에도 여러 가지 방식들이 연구되고 있으나, 향후 이동 센서 노드에 대한 고려나 간단한 에러 제어 코딩 스킴 및 기존의 저전력이나 자체 구성 능력을 개선하는 등 많은 연구 분야가 남아있다.

(3) 네트워크 계층(Network Layer)

상위 계층에 의해 제공되는 데이터의 라우팅 업무를 수행하는 것으로 Ad-hoc 라우팅 기능과 타 센서 네트워크나 외부 네트워크와의 통신 기능을 제공한다. 기존의 Ad-hoc 네트워크와 달리 센서 네트워크는 몇 가지 추가적인 요구 사항이 존재한다.

- 전력 소모 효율성(Power Efficiency)
  : 전체 네트워크의 전력 소모를 고려하여 저전력 라우팅을 수행해야 한다.
- 데이터 중심(Data Centric)
  : 싱크 노드가 요구할 경우에만 데이터를 전송하여 센서 노드들이 고유한 주소를 가지고 통신하기 보다는 속성기반 주소를 가진다.
- 데이터 통합 수집(Data Aggregation)
  : 한 노드가 다른 여러 노드의 데이터를 모아서 의미있는 하나의 데이터로 만들어서 싱크 노드로 전송한다.
- 속성기반 주소화(Attribute-based Addressing)
  : 센서 노드가 고유 주소를 가지는 것이 아니라 싱크가 관심있는 데이터(속성)를 가진 특정 센서 노드들만 주소를 가진다.
- 위치 인식(Location Awareness)
  : 센서 노드들은 이웃 노드들의 위치를 인지함으로써 전력 소모와 작업 등을 조절하여

수행한다.

네트워크 토폴로지의 급격한 변화, 고도의 확장성, 인터넷과 같은 외부 네트워크와의 연동등에 대한 연구 분야가 남아있다.

(4) 전송 계층(Transport Layer)

센서 노드의 데이터를 전송하거나 흐름을 관리하는 기능을 수행하며, 시스템이 인터넷이나 다른 외부 네트워크에 접속할 때 필요하다. 싱크와 사용자간의 통신은 인터넷이나 인공 위성을 통한 UDP 또는 TCP 통신을 하며, 싱크와 센서 노드들간의 통신은 UDP 형태의 프로토콜이 요구된다. 현재 제한된 전력과 메모리와 같은 하드웨어 제약을 위한 새로운 프로토콜 개발이 필요하다.

(5) 응용 계층(Application Layer)

실제 응용 분야에 따라 센싱을 하는 업무를 수행한다. 속성기반 명명화와 위치기반 주소화를 이용하여 센서 노드에 접속하는 SMP(Sensor Management Protocol)이 있으며, 더 나은 서비스 제공을 위한 프로토콜 연구가 필요하다.

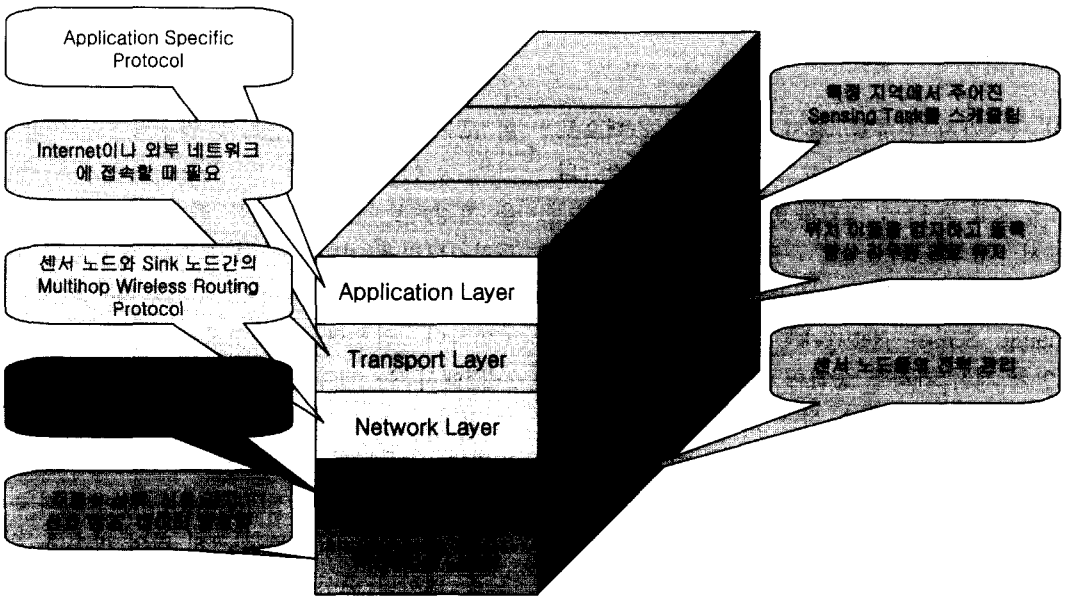
이와 더불어 센서 네트워크를 관리 측면에서 살펴보면 다음과 같이 분류할 수 있다.

(1) 전력 관리 측면(Power Management Plane)

센서 노드와 전체 센서 네트워크에 의한 전력 사용에 대해 관리하는 측면으로, 트래픽 처리의 분산 및 네트워크의 효율적인 구성을 통해 전력 소모를 감소한다. 센서 노드는 데이터 송수신이 없을 때 비활성(Idle) 상태가 아닌 휴지(Sleep) 상태로 전환하여 전력 소모를 최소화한다.

(2) 이동 관리 측면(Mobility Management Plane)

센서 노드의 이동을 인지해서 사용자에게로의 경로를 중앙집중적 방식/분산적인 방식 또는 절대적 위치/상대적 위치 측정으로 유지한다. 센서



〔그림 2-2〕 센서 네트워크 프로토콜 스택

〈표 2-1〉 센서 네트워크 프로토콜 스택별 기능

Plane / Layer	Power Management	Mobility Management	Task Management
Application	에너지 효율성을 고려한 응용 프로토콜	센서 노드들의 이동관련 Task 관리	응용 분야에 따른 Sensing Task 동작 관리
Transport	센서 노드와 싱크 사이의 제한적인 전력과 메모리를 고려한 UDP 통신	이동 특성을 고려한 데이터 흐름 유지	응용 분야에 따른 데이터 흐름 유지
Network	에너지 효율성을 고려한 라우팅	위치 정보에 의한 네트워크 토폴로지 정보 유지	Task 요구 사항을 고려한 라우팅
Data Link	On/Off Mode로 동작프레임 오버헤드 최소화	Peer Discovery Auto-synchronize	Task에 따른 스케쥴 테이블 형성
Physical	에너지 효율적인 매체 선택	전송 매체에 따른 제한적 이동	Task 요구 사항을 고려한 매체 선택

노드들은 이웃 센서 노드들의 위치를 인지함으로써 전력 소모와 작업을 조절하여 수행한다.

(3) **업무 관리 측면**(Task Management Plane)

특정한 지역에 주어진 감지 작업을 조절 및 관리하는 측면이다. 모든 센서 노드가 특정 지역에서 동시에 감지 작업을 수행하는 것이 아니라 노드의 전력 수위에 따라 노드들끼리 작업의 양을 조절한다.

이 두 가지 분류를 센서 네트워크 스택으로 [그림 2-2]와 같이 도식화할 수 있으며, 각각의 기능을 <표 2-1>에 정리하였다.

센서 네트워크의 토폴로지는 크게 Dynamic/Distributed/Reactive로 구분할 수 있다. Dynamic Sensor Network는 GPS 동기화와 전력 인식 센서 관리를 통하여 효율적인 전력 인식 라우팅 및 통신 기술을 이용함으로써 센서 네트워크의 수명을 개선한 구조이며, Distributed Sensor Network는 많은 센서 노드들을 가진 네트워크 설계 시 정보의 수집, 처리 및 저장과 같은 데이터 처리 문제를 효율적으로 개선하기 위해 분산 네트워크 구조를 적용한 것이다. 마지막으로 Reactive Sensor Network는 협력적인 신호처리 기법과 이동 기술을 위한 Data aggregation 및 flexible tasking을 지원하는 구조이다.

센서 네트워크는 그 구조적인 특징으로 인하여 일반적으로 적용되는 Ad-hoc 라우팅과는 다른 라우팅 기법이 요구된다. 라우팅 기법은 크게 평면 라우팅(flat routing)과 계층적 라우팅(hierarchical routing)으로 나누어 진다. 평면 라우팅은 네트워크 전체를 하나의 영역으로 간주하여 모든 노드들이 동등하게 라우팅에 참여할 수 있는 방식으로 멀티홉 라우팅(multi-hop routing)을 특징으로 한다. 계층적 라우팅은 네트워크를 클러스터링을 기반으로 한 다수의 영역으로 분할하여 각각의 영역 내 특정 노드에 헤드의 역할을 부여하여 라우팅을 수행하는 방식이다. <표 2-2>에서 두 라우팅 기법을 비교한 내용을 볼 수 있다.

평면 라우팅의 대표적인 라우팅 프로토콜은 Directed Diffusion과 SPIN, MCF 등이 있다.

Directed Diffusion은 싱크의 질의 방송에 기반을 둔 데이터 중심적 라우팅 기법으로 질의 유포 및 처리 응용에 적합하다. 싱크 노드가 원하는

〈표 2-2〉 센서 네트워크의 라우터 기법 비교

구 분	평면 라우팅	계층적 라우팅
스케줄링	경쟁 기반 스케줄링	예약 기반 스케줄링
충돌	충돌 오버헤드 존재	충돌 회피
Duty Cycle	노드의 sleeping 시간을 제어한 duty cycle이 가변적	주기적인 sleeping에 의해 duty cycle 감소
Data Aggregation	멀티홉 경로상의 노드가 이웃 노드로부터 데이터를 수집	클러스터 헤드가 데이터를 수집
라우팅 복잡도	복잡하나 최적은 라우팅	단순하나 최적은 아닌 라우팅
동기	동기 없음	전역적, 지역적 동기가 필요
경로 설정 방법	전송할 데이터를 가지는 지역에서 경로가 설정	네트워크 전체에 클러스터 형성 오버헤드 존재
지연	중간 노드를 깨워 멀티홉 경로를 설정하는데 지연 존재	클러스터 헤드들이 형성하는 멀티홉 네트워크가 항상 존재하므로 지연이 적음
에너지 소비	트래픽 패턴마다 에너지 소비가 다름	에너지 소비가 일정
채널 할당 공정성	고정성 보장 안됨	공정성이 보장

데이터 정보(Interests)를 각 센서 노드로 전송하면 일치하는 데이터가 있을 때만 센서 노드들이 싱크 노드로 데이터를 전송한다. SPIN(Sensor Protocols for Informative via Negotiation)은 협상과 자원 적응에 의해 Flooding(모든 이웃 노드에게 데이터를 broadcasting)의 결함을 처리하기 위해 설계된 것으로, 센서 노드가 데이터에 대해 광고하고, 싱크로부터 요청을 기다리는 형태의 데이터 중심적 라우팅 기법이다. 센서 노드가 데이터를 방송하는 대신 센서 데이터를 기술하는 메타 데이터를 전송하여 보다 효율적으로 동작하고 전력 소모를 줄이도록 한다. 센서 노드가 메타 데이터를 가지는 ADV 메시지를 방송하면, ADV의 메시지를 수신한 이웃 노드가 데이터에 대한 관심을 가지고 RFQ 메시지를 전송하면 해당 이웃 노드를 위한 DATA 메시지를 전송한다.

MCF(Minimum Cost Forwarding Algorithm for Large Sensor Networks)는 센서 네트워크에서 데이터 흐름이 항상 싱크를 향한 방향으로 이루어지는 특성을 이용하여 센서 노드는 유일한 ID나 메시지를 전송할 라우팅 테이블을 가질 필요 없이 싱크까지의 최소 비용 측정치만을 관리하여 최소 비용 경로를 이용하여 데이터를 전송한다.

계층적 라우팅의 대표적인 라우팅 프로토콜은 LEACH 등이 있다.

LEACH(Low-Energy Adaptive Clustering Hierarchy)는 클러스터링 기반 라우팅 기법으로, 클러스터 헤드가 클러스터의 멤버 노드들로부터 데이터를 수집하여 "데이터 퓨전"을 통해 데이터를 모아서 직접 싱크로 전달한다. 네트워크에 있는 모든 센서 노드들에 에너지 소비를 공정하게 분산시키기 위해 각 노드가 주어진 확률에 따라 스스로 클러스터 헤드가 될 지를 결정하고 이러한 결정이 골고루 발생하도록 한다. 전체적인 통신 비용을 줄이기 위해 클러스터 헤드에서 클러스터 내의 모든 노드로부터 데이터를 받아 싱크 노드로 전송한다.

〈표 2-3〉 IEEE 802.15.4의 특성

구 분	특 성
데이터 전송률	868MHz : 20kbps ,915MHz : 40kbps, 2.4GHz : 250kbps
적용 거리	10~75m
잠복 시간	Down to 15ms
채널 수	868MHz : 1ch, 915MHz : 10ch, 2.4GHz : 16ch
주파수 대역	2 물리층 : 868/915MHz 및 2.4GHz
어드레싱	8-bit short 또는 64-bit IEEE
채널 접속	CSMA-CA 및 slotted CSMA-CA
활용 온도 범위	-40 to +85℃

2.2 표준 동향

센서 네트워크에서 표준을 사용하지 않고, 업체 고유의 기술에 의존하게 되면 사용자들은 센서, 컨트롤러, 인터페이스 등 모든 것을 해당 업체에 구속받게 되어 네트워크 구성 시 혼선을 빚게 된다. 이에 센서 네트워크의 네트워킹 기술을 표준화함으로써 복잡한 제어 루프의 구현을 상당히 단순화시켜 센서 네트워크의 확장을 용이하게 하고 있다.

다음은 센서 네트워크 관련 표준이다.

(1) Bluetooth

휴대용 장치간의 양방향 근거리 통신을 저가격으로 구현하기 위한 근거리 무선 통신 기술로서 기본적으로 개인이 사용할 수 있는 무선 통신을 제공하는 것을 목표로 하는 대표적인 WPAN(Wireless Personal Area Network) 무선 네트워크 기술이다. Bluetooth는 크기가 작고, 저렴한 가격과 적은 전력 소모로 네트워크 단말들을 10m~100m 내의 무선 연결을 가능하게 하는데, 2001년 2월에 v1.1에 이어 2003년 11월에 v1.2를 표준화하였다. 새로이 표준화된 v1.2는 기존의 v1.1에 비해 많은 문제점을 개선하였으나, 많은 노드들이 넓은 범위를 구성하는 네트워크에 적용하기에는 부적절하다. Bluetooth는 원래 유선의 대체로 인식되었으나 점점 구조가 복잡해지는 경향과 저전력 소모 응용에 적절치 못하여 초기의 설계 목표를 이루지 못하고 있다. 또한, 배터리의 수명에도 한계가 있어 연간 여러 차례의 배터리 교환이 요구되어 저속의 저가, 저전력 응용에는 적합하지 못하다.

(2) IEEE 802.15.4

저속 무선 PAN에서 간단한 구조로 저가 저전력으로 고정장치나 휴대/이동장치를 무선으로 연결할 수 있는 방안을 표준화하는 것으로, 물리계층과 데이터링크 계층에 대해 정의하고 있다. IEEE 802.15.4의 상위 계층 특성은 <표 2-3>과 같다.

IEEE 802.15.4은 WPAN의 물리 계층과 데이터링크 계층을 기반으로 하여 상위의 네트워크 계층에서 응용 계층까지는 응용 분야의 환경에 따라 비영리 조직인 Zigbee 연맹에서 개발되고 있으며, 이 조직에서는 다양한 응용 분야에서 활용될 수 있도록 응용 프로파일의 정의 및 개발에 초점을 맞추고 있다. IEEE 802.15.4 표준안은 Draft18까지 나와 있는 상태로 네트워크 계층에서의 소모 에너지 관리를 중요시 하였고, 스타형과 peer-to-peer 네트워크 토폴로지를 모두 지원한다. 어드레싱 타입도 8-bit short와 16-bit

IEEE를 지원한다.

(3) Zigbee

Zigbee는 IEEE 802.15.4로부터 발생한 표준 활동 그룹으로서 수개월부터 수년까지의 배터리 수명을 갖는 낮은 데이터 전송률의 솔루션 개발을 목표로 하고 있다. Philips, Motorola, Honeywell, Mistbishi, Invensys, 삼성 등이 promoter로 참여하고, 약 50여개 업체가 member로서 참여하고 있다. IEEE 802.15.4에서 물리 계층과 데이터링크 계층에 대한 표준화를 담당하고 있고, Zigbee의 경우 보안, 네트워크 계층, 응용 하위 계층, 마케팅 및 세부 프로파일에 대한 표준화 작업을 한다. 현재 Draft 0.7이 완료된 상태이고, 기능적인 측면을 추가한 ver1.0을 위한 작업이 진행되고 있다.

Zigbee의 가장 큰 특징은 저렴한 가격으로 무선 송수신 회로의 구성을 단순화하여 칩셋 가격을 미화 1.5달러 정도로 하는 것을 지향하고 있다. Bluetooth가 1Mbps, 1mW 이상의 송신전력을 갖는데 반해 Zigbee는 250kbps, 1mW 미만의 송신전력을 사용하고, 2.4GHz 주파수 대역에서 16 채널을 지원하여 같은 대역 내에서 더 많은 사용자를 수용할 수 있다. 또한, Zigbee의 RF 링크 프로토콜과 사용자 어플리케이션은 실행 코드 사이즈가 작고, 통신 모드가 송/수신 활동이 필요한 경우에만 sleep 모드에 있는 노드들을 활동 상태로 변경하는 방식을 채택하여 전력 소모를 극소화하였다. 특정 노드가 네트워크 상의 다른 모든 노드들을 인식하지 못할 때는 네트워크를 스스로 구성할 수도 있어, 센서 네트워크의 표준 방식이 될 가능성이 매우 높다.

(4) P1451.5(Wireless Sensor Network Interface)

센서 네트워크의 표준 활동 중 하나인 P1451.5는 무선 인터페이스 표준화를 위하여 다양한 현존의 무선 기술을 통합 적용시킬 수 있는 무선 통신 표준을 확립하고자 한다. P1451.5는 IEEE-1451 표준의 확장으로서 센서들을 네트워크 버스에 결합시키는 개방형 방법으로 표준 인터페이스를 통해 Transducer(Sensor와 Actuator)들 간의 통신을 단순화 시키는 것이다. 현재 Axonn LLC, Boeing, NSWC-Dahlgren, Motorola, 3eTI 등이 참여하고 있으며, Sensor Expo에서 디지털 자동차 창문 센서, 무선 타이어 압력 센서, 스마트 고속도로 센서, 환자용 무선 의료 센서 등 다양한 어플리케이션에 적용한 예시를 발표하였다. P1451.5는 크게 TEDS(Transducer Electronic Data Sheet) 포맷과 이 TEDS와 Transducer 데이터에 접근하는 무선 통신프로토콜을 정의하고 있다. 그리고 이 스펙을 적용하면 센서들은 자신을 증명하고, 이더넷, Profilebus, DeviceNet 또는 기타 업체 고유의 시스템을 포함한 여러 종류의 산업용 버스와도 동작할 수 있는 충분한 지능을 가질 수 있게 된다.

2.3 센서 네트워크와 Ad-hoc

센서 네트워크에서는 센서 노드들이 서비스 영역에 배치된 후 자동적으로 Ad-hoc 네트워크를 구성한다. 기존의 무선 Ad-hoc 네트워크는 많은 프로토콜과 알고리즘이 연구되고 있지만, 이를 센서 네트워크에 그대로 적용하기에는 일부 어려움이 있다. 두 네트워크가 다음과 같은 차이점이 존재하기 때문이다.

- 센서 네트워크를 구성하는 센서 노드의 수는 Ad-hoc 네트워크에 비해 월등하게 많다.
- 센서 노드들은 Ad-hoc 노드에 비해 밀집하여 배치된다.
- 센서 노드는 상대적으로 고장 날 확률이 높다.
- 센서 노드는 Ad-hoc 노드에 비해 배터리,

CPU, 메모리 기능에 제약이 심하다.

- 센서 노드는 제한된 메모리로 인해 작은 양의 데이터 전송만이 가능하며, 주기적인 데이터를 전송한다.
- 센서의 이동 또는 고장으로 인해 센서 네트워크의 망 구성은 자주 변경될 수 있다.
- 센서 네트워크는 broadcast 통신을 주로 이용하는 반면 Ad-hoc 네트워크는 point-to-point 통신에 기반한다.
- 센서 네트워크에서는 많은 센서 노드들의 수와 메시지 교환 시의 오버헤드로 인하여 GID(Global Identification)을 갖지 않을 수도 있다.
- 센서 네트워크에서는 데이터가 특정 노드로 요청되지 않고, 특성을 기반을 두고 데이터가 요청되는 데이터 중심적인 특정을 가진다.(예: 어떤 지역의 기온이 몇 도인가?)
- 인접한 센서 노드들이 유사한 데이터를 가지므로, 각 센서 노드들이 데이터를 각각 전송하는 것은 비효율적이다.
- 응용에 따라 네트워크 요구 사항이 변하는 응용 특정적 특성을 가진다.

센서 네트워크는 위의 차이점과 더불어 다음과 같은 부가적인 특성을 수용하여야 한다.

- 센서 네트워크에서는 감지될 물리적 파라미터를 지시하는 속성 기반 어드레싱이 사용된다.
- 대부분의 데이터가 위치에 기반을 두고 수집하므로, 필요할 때마다 노드들의 위치를 기반으로 라우팅이 가능해야 한다.

위와 같은 센서 네트워크의 특징으로 인해 이를 만족시키는 센서 네트워크 구조를 개발할 필요성이 있으며, 이미 많은 연구가 진행 중에 있다.

2.4 무선 센서 네트워크 정보보호 기술

(1) 센서 네트워크 보안 고려 사항

무선 및 분산화의 특성을 갖는 센서 네트워크는 센서의 경량화로 인하여 에너지 저장 용량, 컴퓨팅 파워 및 통신 능력면에서 제한성을 갖는다. 이러한 점 때문에, 기존의 네트워크 환경에서 제공되었던 보안 기술들을 그대로 센서 네트워크에 적용하기에는 많은 문제점이 예상된다.

본 장에서는 센서 네트워크를 구축하는데 필수적으로 해결해야 할 보안 고려 사항에 대하여 기술하며 키 설정, 통신 기밀성, 중요 정보에 대한 프라이버시, DoS 에 대한 견고성, 보안 라우팅, 물리적인 공격에 대한 대응, 보안 그룹 관리 및 침입탐지 측면에서 살펴본다.

• 키 설정

기존의 보안 기술에서 분산화된 여러 노드들에게 키를 분배하는 방식으로 주로 공개키 방식을 사용하였다. 그러나, 센서 네트워크의 노드는 제한된 컴퓨팅 파워로 이러한 공개키 방식을 적용하는데 무리가 따른다. 또한, 센서 노드는 특정 지역에 수백, 수천개씩 설치되므로 이러한 수의 노드를 지원할 수 있는 확장성을 고려한 키 설정 프로토콜이 필요하다. 센서 네트워크에서의 공개키 방식 사용에 대한 대안으로 공유키 사용, bootstrapping 키 사용 및 랜덤 키 배포방식 등이 제안되었으나 확실한 해결책은 제시되고 있지 못한 상황이다.

• 통신 기밀성

센서 노드들간의 통신에 대한 기밀성을 제공하는 방안으로, 종단 노드들간에 암호화를 사용하거나 네트워크상의 공유키를 활용한 링크 계층상에서의 암호화를 제공하는 방안을 고려할 수

있다. 종단간 암호화 방안은 보안성 측면에서는 뛰어나지만, 모든 통신주체들간의 키 분배가 필요하다는 점에서 확장성면에서 문제점을 갖는다. 반면에, 공유키를 활용한 링크 계층에서의 암호화 방안은 특정 공유키를 기반으로 암호화가 진행되므로 확장성면에서는 뛰어나지만, 중간 노드에서 도청 및 메시지 변조가 일어날 수 있다는 점에서 보안 강도측면에서 단점을 갖는다.

• 중요 정보에 대한 프라이버시

센서 네트워크에서 발생할 수 있는 프라이버시 침해는 악의를 갖는 개인이 다른 사용자의 중요 정보를 획득하기 위하여 악의의 센서를 설치하는 경우와, 정상적으로 설치된 센서가 악의의 사용자로 인하여 오용되는 두가지 경우가 있다. 이러한 방식에 의한 프라이버시 침해가 센서 네트워크에서 특히 주목 받는 이유는, 센서 네트워크에서의 중요 데이터가 네트워크상의 특정 지점에서 수집되는 특성을 갖기 때문이다. 이러한 대규모로 분산화되는 특성을 갖는 센서 네트워크에서의 중요 정보에 대한 프라이버시 문제는 기술적인 측면 이외에도 법률 및 사회 규범 측면과 연관하여 대처할 때 효과적인 대응이 가능할 것으로 보인다.

• DoS(Denial of Service) 에 대한 견고성

센서 네트워크에서는 악의의 특정 노드를 통하여 높은 에너지를 갖는 시그널을 전체 네트워크측으로 broadcasting 하거나 MAC 프로토콜을 위반함으로써 통신을 방해하여, 전체 네트워크의 서비스를 마비시키는 DoS 공격이 발생될 소지가 매우 높다. 이러한 DoS 공격중에서 Jamming 을 주로 이용하여 발생시키는 공격은 spread-spectrum 방식을 이용하여 사전에 방지할 수 있지만, 아직까지 암호화된 안전한 spread-spectrum 방식에 대한 상용 수준의 해결책은 없는 상황이다.

• 보안 라우팅

현재 네트워크에서 사용되는 라우팅 프로토콜에서는 보안이 제대로 보장되지 못한다. 라우팅 프로토콜의 보안성은 특정 노드의 침해발생이 전체 네트워크에 영향을 미친다는 점에서 반드시 해결되어야 한다. 특히, 센서 네트워크에서는 노드간의 라우팅으로 전체 네트워크의 연결성을 제공하는 Ad-hoc 라우팅의 형식을 띄므로, 라우팅 프로토콜의 보안성 제공은 안전한 센서 네트워크를 구축하는데 필수적인 요구사항이다.

• 물리적인 공격에 대한 대응

센서 노드들은 특성상 공격자가 물리적으로 쉽게 접근할 수 있는 위치에 놓이게 되어, 공격자의 물리적인 공격 위협에 자주 노출된다. 이러한 문제점을 해결하기 위한 가장 기본적인 방안으로 물리적으로 센서 자체를 보호하는 방안이 있을 수 있으나 이러한 방식은 비용측면에서 효과적이지 못하다. 최근의 연구에서는 센서 네트워크의 중요 정보에 대한 상태를 복제하여 특정 노드에 문제가 발생했을 경우, 여러 다른 노드에서의 voting 결과에 의해서 특정 노드의 정보에 대한 진위를 판단하는 방식등이 제안되고 있다.

• 보안 그룹 관리

센서 네트워크에서의 데이터 수집과 분석은 여러 노드로 구성된 노드 집합군에 의해서 수행된다. 이러한 노드 집합군을 이루는 센서들은 시간의 연속성을 갖고 빠르게 변화하게 된다. 이렇게 빠르게 변화하는 센서 노드 집합군을 구성하는 데 필요한 안전한 그룹 멤버의 허가 방안과 안전한 그룹 노드들간의 통신방법이 필요하다.

• 침입 탐지

기존의 네트워크상에서의 침입탐지는 네트워크상의 특정 지점에서 집중적으로 정밀한 탐지가 수행되었다. 센서 네트워크에서는 여러 센서에서 데이터가 수집되며, 동적으로 변화하는 여러 특정 지점에서 데이터 수집이 이루어 지므로, 분산적이며 비용측면에서 효과적인 침입 탐지 방안이 고안 되어야 한다.

(2) SPINS(Security Protocols for Sensor Networks)

SPINS(Security Protocols for Sensor Networks)는 센서 네트워크의 특성에 맞도록 설계한 보안 프로토콜들로서 UC Berkeley에서 설계하여 제안한 프로토콜이다. SPINS 프로토콜은 다음과 같은 센서 네트워크의 특성을 고려하여 설계하였다.

- 센서 네트워크의 통신 방식인 무선 통신은 많은 전력을 소모 시키는 방식이므로 통신 오버헤드를 최소화 하는 것이 필요하다.
- 제한된 파워를 갖는 센서의 특성상 기존의 보안 알고리즘을 그대로 적용하기는 불가능하다.
- 제한된 메모리를 갖는 센서의 특성상 비대칭형 암호 알고리즘을 적용하기 위한 변수를 저장하기 위한 공간의 마련에 어려움이 있다.
- 전원공급에 제한이 많다.
- 인증된 데이터가 전체 센서 네트워크에 브로드캐스트 되는 센서 네트워크의 특성상 비대칭형 디지털 서명 방식의 적용은 적합하지 않다.

SPINS 프로토콜의 프로토타입은 UC berkeley에서 개발한 SmartDust 노드에 적용하여 개발되었으며, SPINS 프로토콜의 설계 자체도 SmartDust 노드를 염두에 두고 개발한 것이다. SmartDust 노드의 하드웨어 사양은 <표 2-4>와 같다.

<표 2-4> SmartDust node의 특성

CPU	8-bit, 4Mhz
Storage	8KB instruction flash 512 bytes RAM 512bytes EEPROM
Operating Systems	TynyOS
OS code space	3500bytes
Available code space	4500bytes
Communication	912 MHz radio
bandwidth	10Mbps

SPINS에서 대상으로 하는 센서 네트워크는 Node와 BS(Base Station)으로 구성된 네트워크로서, 기본적인 통신 방식은 Node에서 BS로의 통신 (e.g., sensor readings), BS에서 Node로의 통신 (e.g., specific request) 그리고 BS에서 모든 Node로의 통신 (e.q., routing beacon, queries or reprogramming of the entire network), 이렇게 세 가지로 가정하고 있다. 센서 노드가 생성되는 시점에서 각 노드는 BS와 공유하는 master key를 받는 다는 가정과 BS는 기본적으로 신뢰할 수 있다는 가정을 두고 있다.

SPINS는 SNEP 프로토콜과 μTESLA 프로토콜로 구성되는데, SNEP(Secure Network Encryption Protocol)은 통신 데이터의 암호화, 인증 등의 서비스를 제공하기 위한 프로토콜이며, μTESLA는 브로드캐스트 메시지에 대한 인증 서비스를 제공하기 위한 프로토콜이다.

SNEP프로토콜

SNEP(Secure Network Encryption Protocol) 프로토콜은 기본적으로 Data confidentiality, two-party data authentication, integrity, replay protection, weak message freshness를 제공하며, 단지 메시지 당 8byte만의 정보를 추가하여 보안 서비스를 제공하는 경량화 된 방식의 프로토콜이다. SNEP은 데이터를 암호화 하여 도청을 방지

한다. 통신 양단은 counter mode의 block cipher를 위한 두 개의 counter를 공유하며, 이 counter의 상태를 양단이 각각 유지하도록 하여 counter를 메시지에 실어 전송하는 오버헤드를 줄이도록 하였다. Counter 값의 동기화는 통신 양단이 counter exchange protocol을 이용하여 유지한다. 통신 양단은 master secret key X를 공유하며 pseudorandom 함수를 이용하여 독립된 key들을 유도한다.

A가 B로 전송하는 SNEP 프로토콜이 적용된 메시지의 구성방법은 수식 (1)과 같다.

$$A \rightarrow B: \quad \{D\}_{(K_{AB},C_A)}, \mathrm{MAC}(K'_{AB}C_A \| \{D\}_{(K_{AB},C_A)}) \qquad (1)$$

수식 (1)의 D는 메시지, K는 encryption key, K' 은 MAC key, C는 counter를 표현한다. KAB는 A와 B가 공유하는 encryption key, CA는 A가 보유하고 있는 counter를 의미한다. {D}<KAB,CA>는 K를 encryption key로 하고, CA를 counter로 하여 D 메시지를 encrypt 한 메시지를 의미한다.

Encryption key KAB와 MAC key K' AB는 A와 B가 공유하는 master secret를 가지고 Pseudo-Random Function(PRF)을 돌려 생성한 key가 된다.

이러한 SNEP 프로토콜의 경우, counter 값은 메시지가 전송될 때마다 증가되고, encryption 할 때 counter 값이 사용되므로, 동일한 메시지라도 전송되는 시점에 다라 다르게 암호화 되어 semantic security가 보장된다고 볼 수 있다. 또한 MAC 검증을 통해 수신자는 송신자를 검증할 수 있게 되며, MAC에 포함된 counter 값을 통해 replay protection 서비스를 제공할 수 있게 된다. 또한 메시지의 검증이 정확히 이루어졌다면, 수신자는 지금 수신한 메시지가 자신이 수신한 이전 메시지 이후에 보내진 메시지라는 점을 확인할 수 있으므로 weak freshness도 제공된다고 볼 수 있다. 또한 counter 값은 양단에서 각기 관리하고 메시지에 실어 전송하지 않음으로 통신 오버헤드를 줄일 수 있게 된다.

수식 (2)는 counter exchange protocol의 동작을 보여준다.

$$\begin{aligned} A &\rightarrow B: \quad C_A, \\ B &\rightarrow A: \quad C_B, \mathrm{MAC}(K'_{BA}C_A \| C_B), \\ A &\rightarrow B: \quad \mathrm{MAC}(K'_{AB}, C_A \| C_B). \end{aligned} \qquad (2)$$

Counter exchange protocol은 어떠한 이유로든 공유되고 있는 counter의 상태가 일치하지 않게 되는 경우가 발생하면 구동 된다.

μTESLA 프로토콜

μTESLA 프로토콜은 TESLA 프로토콜의 micro version으로 이해할 수 있다. TESLA 프로토콜을 센서 노드에 적용하기 위해 변형한 프로토콜이 μTESLA 프로토콜 이다.

TESLA 프로토콜과 μTESLA 프로토콜의 주요 차이점을 기술하면 다음과 같다.

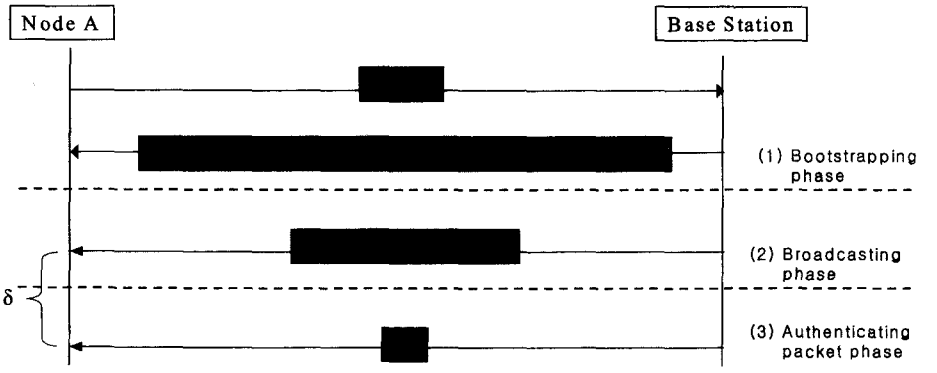
TESLA 프로토콜의 경우 digital signature를 이용하여 initial packet을 인증하는 구조를 갖는데, 이를 센서 노드에 적용하기에는 너무 무겁다는 문제가 있다. 반면 μTESLA 는 단지 symmetric 메커니즘 만을 사용 하도록 하여 인증 구조를 단순화 하였다. TESLA는 각각의 패킷에 대해 key를 노출하는 방식을 사용하고 있는데, 이는 너무 많은 에너지가 소모되는 방식으로 센서 노드에 적용하기에 어려움이 있다. μTESLA의 경우에는 메시지를 보낼 때 마다 key를 노출시키는 것이 아니라, 일정한 time interval을 두고 key를 노출시키는 방법을 통해 키 노출 횟수를 줄임으로 경량화 하였다.

TESLA 의 동작을 위해서는 one-way key chain을 저장해야 하는데 이러한 방식 역시 소형의 센서노드에 적합하지 않다. 이러한 문제를 해결하기 위해 μTESLA는 인증된 센서의 수에 제약을 가하는 방법을 사용한다.

μTESLA의 노드는 앞서 언급한 SNEP 프로토콜을 이용하여 브로드캐스트할 메시지를 BS로 보낸다. BS는 이 메시지를 송신 노드를 대신하여 안전한 방법으로 브로드캐스트를 수행한다. BS가 메시지를 브로드캐스트 하는 동작 과정을 [그림 2-3]에서 볼 수 있다. [그림 2-3]에서 처럼 크게 (1) 수신 노드의 bootstrapping 단계 (2) 메시지를 브로드캐스트하는 단계 (3) 수신한 브로드캐스트 패킷을 검증하는 단계로 구분할 수 있다. [그림 2-3]의 Bootstrapping 단계에서서 수식에 사용된 심볼의 의미는 다음과 같다. T_{now}는 BS의 시간, K_i는 바로 이전 interval i에서 노출한 one-way key chain의 key, T_i는 interval i의 시작 시간, T_{int}는 interval의 지속시간(duration), δ는 키를 노출하기 위한 지연시간을 의미한다. 노드 A가 Bootstrapping이 종료되고 난 이후 BS로부터 브로드캐스트 메시지를 받게 되면 (broadcasting phase), 노드는 K_j(interval j에서 BS가 전송한 메시지인 경우)가 현재까지 노출되지 않았는지를 검증하고 나서 메시지를 저장한다. 다음으로 Authenticating packet phase에서, 즉 K_j를 브로드캐스트하고 δ 만큼의 시간이 지난 후에 BS는 K_j 값을 브로드캐스트한다. 노드 A가 이 메시지를 받으면 $F(K_j)=K_j-1$ 또는 $F(F(K_j))=K_j-2$ 인지를 계산하는 방법으로 검증을 수행한다. 다음으로 메시지의 MAC 값을 검증하는 것이 마지막 단계이다.

(3) Jeffery Undercoffer등의 센서 네트워크 보안 기술

이 장에서는 Jeffery Undercoffer 등이 제안한 분산 센서 네트워크에서의 보안기술에 대해 다룬다. 그들은 SPINS가 소스 라우팅을 사용하는 것과 트래픽 분석에 취약점을 가진다는 데에 착안하여 암호화를 이용한 end-to-end 브로드캐스팅 제공하는 새로운 프로토콜을 제안하였다.그들이 제안한 프로토콜의 특징은 다음과 같다.



〔그림 2-3〕 μTESLA의 동작 과정

* base station 모델에서 동작한다.
* end-to-end로 암호화된 패킷의 브로드캐스팅을 이용하여 공격자의 트래픽 분석을 방지할 수 있다.
* base station의 인접노드를 이용하여 브로드캐스팅 범위를 벗어나는 노드들에게도 패킷을 안전하게 중계할 수 있도록 한다.
* 비정상 노드들을 발견할 수 있다.

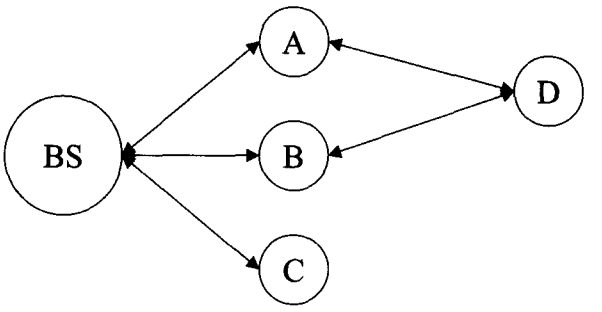
Base station은 뛰어난 컴퓨팅 성능을 가진 신뢰할 수 있는 노드이어야 하며, 통신은 기본적으로 base station과 센서간에 이루어 진다. 다만, 무선 통신 범위를 벗어날 경우, 중계 노드에 의해 데이터의 중계가 일어난다. 다음 [그림 2-4]은 프로토콜이 동작하기 위한 센서 네트워크의 구조를 간단히 나타내고 있다. 각 노드는 base station과 미리 설정된 키를 공유한다.

[그림 2-4]에서 센서 노드 A,B,C는 base station으로부터 한 홉 거리에 있으며 D는 센서 노드 A와 B의 중계를 통하여 base station과 통신할 수 있다. Base station은 통신을 위한 라우팅 테이블과 관련 상태 파악을 위해 액티비티 테이블 및 보안을 위한 키 테이블을 가진다. DTG는 Data Time Group을 의미하며 데이터 생성 시간을 나타낸다.

통신을 위한 메시지는 다음 그림과 같은 형태로 정의된다.

Addr_1은 base station에서 각 센서 노드로 메시지를 보낼 때, 공란으로 남긴다. 하지만, 각 노드로부터 base station으로 메시지를 보낼 때는 base station이 키의 로딩을 빨리할 수 있도록 하기 위해 전송노드의 주소가 담긴다. Addr_2는 base station이 메시지를 보내고자 하는 노드의 주소나, 각 노드가 base station으로 메시지를 보낼 때 자신의 주소를 담기 위해 사용한다.

이제, 위의 메시지를 이용하면 네트워크 셀업



Route Table
A : ( )
B : ( )
C : ( )
D : (A)*
D : (B)

Activity
A : (D)(X)(Y)+
B : (D)(X)(Y)
C : (D)(X)(Y)
D : (D)(X)(Y)

Key Table
Key_A
Key_B
Key_C
Key_D

* denotes primary route

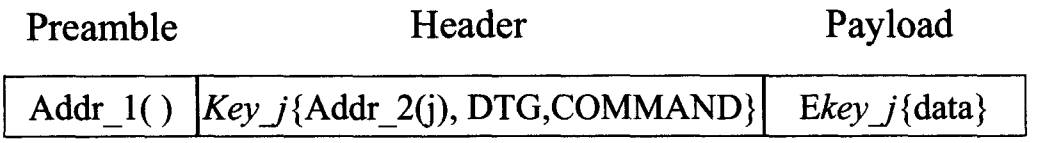
\+ D denotes most recent DTG

X denotes count of corrupted message

Y denotes count of route failures

64bit key (Between BS and sensor)

〔그림 2-4〕 네트워크 토폴리지



〔그림 2-5〕 메시지 형식

과 비정상 노드들을 제거하기 위한 네트워크 수정이 가능하다.

먼저, 네트워크 셀업 과정을 살펴보면 다음과 같다. 이 때 생성된 각 메시지들은 공유된 키로써 암호화되고 브로드캐스팅된다.

* Base station은 HELLO메시지를 인접 노드에게 브로드캐스팅한다.
* 메시지를 받은 노드들은 HELLO-REPLY 메시지로 base station에게 응답한다.
* base station은 응답받은 노드들에 대해 라우팅 테이블에 등록한다.
* base station은 인접하지 않은 노드로의 HELLO메시지와 인접노드로의 HELLO-RELAY메시지를 인접노드에게 브로드캐스팅 한다.
* 인접노드는 HELLO-RELAY를 확인하고, base station이 보낸 HELLO 메시지를 HELLO-RELAY와 함께 인접치 않은 노드들에게 브로드캐스팅한다.
* 인접노드가 중계한 메시지를 받은 인접치 않은 노드는 HELLO-REPLY를 작성하고 이것을 다시 인접노드에게서 받은 HELLO-RELAY와 함께 브로드캐스팅한다.
* 인접노드는 인접하지 않은 노드의 HELLO-RELAY를 확인하고 최종적으로 인접치 않은 노드의 HELLO-REPLY메시지를 base station으로 중계하게 된다.

[그림 2-6]는 비정상 노드의 제거를 위한 네트워크 수정 알고리즘을 나타내며, 이것은 다음과 같이 수행된다.

* Base station은 어떤 메시지 송수신 과정에서 현재 시간과 DTG의 차이가 일정값 이상이거나, 액티비티 테이블(Activity Table)의 X값이 임계치 보다 크게 될 때 네트워크 수정 알고리즘을 시작한다.
* 먼저, 어떤 노드에 대해 주경로를 이용해 POLL메시지를 보낸다.
* 응답이 없으면 대체 경로를 통해 POLL메시지를 보낸다.
* 대체 경로를 통해 응답이 오면 액티비티 테이블에서, 주경로에 대해 실패변수 Y 값을 증가시킨다.
* 만약, 대체경로를 통해서도 응답이 오지 않으면 base station은 주경로를 이루는 중계노드로 다시 POLL메시지를 보낸다.
* 주경로의 중계노드로부터 POLL-REPLY가 오면 주경로상의 노드는 이상이 없으므로 이전 노드를 비정상 노드로 인식하고 라우팅 테이블에서 제거한다.
* 한편 변수 Y값이 임계치를 초과 할 때도 해당 노드를 라우팅 테이블에서 제거한다.

3. 결 론

본 고에서는 센서 네트워크의 정의, 표준, 특징에 대하여 설명을 하였으며 센서 네트워크에서

```
"j"{(Current Time T-DTG)>} OR Activity_x > Threshold do
    Base Station → K_primary → j : POLL
    if j (not →) Base Station : POLL-REPLY then
            Base Station →K_alternate →j : POLL
            if j → Base Station : POLL-REPLY then
                    Base Station →K_alternate →j : UPDATE-PSI + k_alternate
                    K_primary Activity_Y ++
            else
                    Base Station →K_primary : POLL
                    if K_primary → Base Station : POLL-REPLY then
                            Route Table = Route Table - j
"j"Route Table do
    if Activity_Y > Threshold then
```

〔그림 2-6〕 네트워크 수정 알고리즘

필요로 하는 보안 요구사항을 기술하였다. 보안 기술적인 측면에서는 센서 필드에 있는 센서들의 인증 및 그룹관리에 관련한 기술에 대하여 살펴보았다.

센서 네트워크 보안에서의 가장 급선무는 보안 프로토콜의 경량화다. 즉 작은 크기의 센서에서 동작할 수 있는 보안 프로토콜을 위해서는 기존에 사용하고 있는 보안 메커니즘은 너무 크고 전력을 다량으로 소모시키는 다연산 구조로 되어 있다. 센서는 소량의 연산과 정보를 갖는 전자장치 이며 공개키 인프라와 같은 기존의 인프라가 없는 분산형 구조를 갖는 인프라 이다. 이러한 환경에서 동작 할 수 있는 안전하고 신뢰할 수 있는 경량의 보안 프로토콜 개발이 센서 네트워크 보안 산업의 사활이 달려 있다고 해도 과언이 아니라고 생각한다. 그리고 공개된 자연 환경에서 서로 섞여 있는 센서들간의 정보를 정당한 사용자만이 취득할 수 있도록 하는 것은 정보의 프라이버시 관점에서 매우 중요한 관리적 요소이다. 그러므로 유비쿼터스 컴퓨팅 환경에서는 보안 서비스가 선택이 아니라 사람과 밀접한 정보를 저장 관리하여야 하는 관점에서 필수적 서비스로 대두가 되는 것이다.

센서 네트워크은 앞으로 유비쿼터스 네트워크를 구축하는데 매우 주요한 부분을 차지 할 것이라는 것을 의심치 않으면서 센서 정보를 상황인지 정보로 변환, 전달, 이용하는 과정에서 필요로 하게 되는 보안 요소는 Context-aware security, Location-aware security 서비스와 이러한 서비스가 제공되기 위한 미들웨어 기반의 보안 인프라가 조속하게 연구가 진행이 되어야 하고 정보의 프라이버시를 보장하기 위한 데이터베이스의 보안 연구가 병행하여 진행되어야 테마라고 생각된다.

참 고 문 헌

[1] J. Deng, R. Han, S. Mishra, "Security Support In-Network Processing in Wireless Sensor Networks" , In Proc. of 1st ACM Workshop on Security of Ad Hoc and Sensor Networks, 2003.

[2] Y.C. Hu, A. Perrig, D.B. Johnson, " Rushing Attacks and Defense in Wireless

Ad Hoc Network Routing Protocols", In Proc. of 2nd ACM Workshop on Wireless Security(WiSe' 03), 2003.

[3] A. Perrig, J. Stankovic, and D. Wagner, "Security in Wireless Sensor Networks," CACM, Vol. 47, No. 6, June 2004

[4] ADRIAN PERRIG, ROBERT SZEWCZYK, J.D. TYGAR, VICTOR WEN and DAVID E. CULLER, "SPINS: Security Protocols for Sensor Networks," Wireless Networks 8, 521-534, 2002

[5] O. Goldreich, S. Goldwasser and S. Micali, "How to construct random functions," Journal of the ACM 33(4), 792-07, 1986

[6] A. Perrig, R. Canetti, D.Song and J.F.Tygar, "Efficient and secure source authentication for multicast," Network and Distributed System Security Symposium, NDSS' 01, 2001

[7] A. Perrig, R. Canetti, J.F.Tygar and D.Song, "Efficient Authentication and Signing of multicast streams over lossy channels," IEEE Symposium on Security and Privacy, 2000

나 재 훈

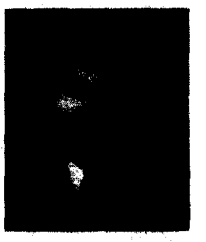
1985년 : 중앙대학교 컴퓨터공학과 공학사

1987년 : 중앙대학교 컴퓨터공학과 공학석사

1987년 ~ 2000년 : 한국전자통신연구원 TDX 교환기 개발 연구원

2001년 ~ 현재 : 한국전자통신연구원 IPv6보안연구팀장

<관심분야> IPv6 보안, Mobile IPv6 보안, Mobike, 센서 네트워크 보안 등



정 교 일

1981년 : 한양대학교 전자공학과 공학사

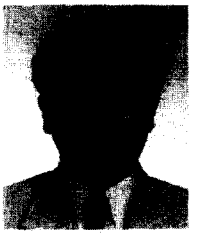
1983년 : 한양대학교 전자계산학과 공학석사

1997년 : 한양대학교 전자공학과 공학박사

1980년 ~ 1981년 : 엠-시스템즈 사원

1982년 ~ 현재 : 한국전자통신연구원 정보보호기반그룹 그룹장

<관심분야> IC카드, 국가기반보호, 신호처리, 생체인식 등



손 승 원

1984년 : 경북대학교 전자공학과 공학사

1994년 : 연세대학교 전자공학과 공학석사

1999년 : 충북대학교 컴퓨터공학과 공학박사

1983년 ~ 1986년 : 삼성전자 연구원

1986년 ~ 1991년 : LG 전자(주) 중앙연구소 HI8mm 캠코더 팀장

1991년 ~ 현재 : 한국전자통신연구원 정보보호연구단 단장

<관심분야> 네트워크보안, 차세대인터넷, Active Network, 생체인식 등