Journal of Digital Contents Society Vol. 13 No. 1 Mar. 2012(pp. 129-139)

무선센서 네트워크를 위한 효율적인 키 관리 연구

박성곤 *

요 약

최근 소형화, 저가격, 저전력 기술의 발달에 힘입어 무선 통신이 가능한 스마트 센서 기술이 발전하고 있다. 특히 스마트 센서의 소형화 기술인 MEMS (micro-electro-mechanical system) 및 NEMS (nano-electro mechanical system) 기반의 센서 기술을 바탕으로 무선 센서 네트워크에 대한 연구가 활발하게 진행되고 있다. 그러나 무선 센서 네트워크는 각종 물리적 자원에 대한 제약이 심하기 때문에 네트워크 보안을 유지하기 어렵다. 본 논문에서는 무선 센서 네트워크 환경에서 제한된 자원으로 안전한 키 확립하는 방법과 센싱된 정보의 암호화를 위해 사용할 수 있는 키 관리 메커니즘 및 키 관리 프로토콜, 보안 기술을 위한 제안한다.

An Efficient Key management for Wireless Sensor Network

Sungkon Park

Abstract

Recently, the smart sensor technologies are rapidly developing in accordance with the technology of implementation in small-size, low-cost, and low power consumption. With these sensor technologies, especially with MEMS and NEMS, the researches on the WSN are actively performing. For the WSN, a network security function is essential even it requires high physical resource level. But the WSN with the smart sensor technologies could not be provided with enough resources for the function because of limited size, computing-power, low-power, and etc. In this paper, we introduce security and key-management protocols of WSN.

Keywords : USN, WSN, Key management

1. 서론

무선 센서 네트워크는(WSN : Wireless Sensor Network)는 MEMS (micro-electro-mechanical system) 및 NEMS(nano-electro-mechanical system)의 발전은 센서, 전자 기술의 발달로 소형, 저가, 저 전력 RF 기술의 발달로 무선 네트워크 기술을 이용한 근거리 무선 통신이 가능한 스마트 센서 기술에 대한 연구가 활발하게 이루어지고 있다.[1-3]

무선화와 소형화가 가능한 센서 네트워크는 초소형의 무선 센서들을 필요한 모든 물리적 공간에 센서를 부착하고, 배치된 다수의 센서 노드들이 주위의 물리적 현상을 감지하고 감지된 정보를 네트워크와 연동하여 실시간으로 관리할 수 있는 기술이다. [1-4]

센서 네트워크 기반의 서비스에 대한 기술이 구체화 되면서 센서 네트워크를 통해 제공되는 정보들을 신뢰하고 동시에 개인의 프라이버시를 보장 받을 수 있도록 센서 네트워크상에서의 보안 연구와 개발이 반드시 병행되어야 한다.[5]

WSN에서의 보안을 위해서 가장 중요한 것은 센서 네트워크 보안 기술 특성과 표준화 현황에서 데이터 도청, 데이터 변조·위조, 프라이버스 침해 등 다양한 위협이다. 또한 센서 망의 특성상 센서 노드는 전력 공급과 메모리와 계산 능력이 매우 제한되어 있다. 따라서 이런 특성을 고려하고 다양한 위협에 대응하기 위하여 센서 망의 구성요소에 유효한 보안 기술을 정의하고

※ 제일저자(First Author) : 박성곤
접수일:2012년 03월 27일, 수정일:2012년 03월 28일
완료일:2012년 03월 31일
* 강원 원주대학교 멀티미디어공학과 교수
spark@gwnu.ac.kr

구현 가능한 보안 기술의 적용이 요구된다. [6]

센서 네트워크에서는 보안 위협으로 안전한 환경을 구축하기 위해서 센서 네트워크에서 전송하는 데이터의 기밀성, 무결성, 인증 등을 만족하기 위해서는 기본적으로 암호화키를 사용한다. 센서 노드의 경우, 일반적인 무선 통신 모바일 장치에 비해서 연산 능력, 저장 공간 등 제약 요소를 가지므로 기존의 방법으로 암호화키를 공유, 생성, 분배 하기는 어렵다. 센서 네트워크 환경을 위한 다양한 기법이 존재하더라고 그에 적절한 키 관리 기술을 선택하는데 적절한 지침이 존재하지 않아 키 관리 기술 선택에 어려움이 있다. 따라서 센서 네트워크 환경에서 제한된 자원으로 안전한 키 확립하는 방법으로 싱글 네트워크 키(single network-wide key), 양방향 키 확립(pair-wise key establishment), 신뢰기반 키 설정(trusted base station) 등 다양한 기술이 개발되었다. 센서 네트워크에서의 보안 요구사항은 암호 키를 관리할 수 있는 기능을 제공하여야 하며, 센서 환경에 적합한 경량화 된 암호 및 인증 기능을 제공하여야 하고, 라우팅 시에 보안 기능을 제공해야 한다.[7-8] 메모리, 전력, 계산 능력 등 자원이 제한 되어있는 노드에 보안 프로토콜 기능을 부여하기가 어렵다.

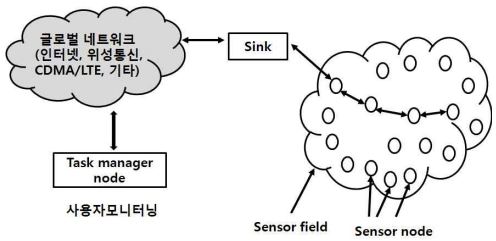
본 논문에서는 무선 센서 네트워크의 보안 프로토콜을 소개하고, 키 관리 프로토콜의 장단점을 기술하고, 외부에 노출된 센서 노드가 외부 공격으로 부터 안정성 뿐 만이 아니라, 기밀성, 무결성 및 인증을 제공하는 기법과 센서 네트워크에서의 노드의 인증이나 센싱된 정보의 암호화를 위해 사용할 수 있는 키 관리 메커니즘 및 키 관리 프로토콜, 보안을 위한 요구사항들을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 무선 센서 네트워크에 대하여 알아보고 3장에서는 센서 네트워크 보안의 요구사항들에 대하여 알아본다. 4장에서는 WSN에서의 라우팅 프로토콜과 키 관리 기술을 하고, 5장에서는 센서 네트워크에서의 공격 유형에 따른 키 관리 적용 고려사항, 6장에서는 결론 및 향후 연구 과제를 제시하였다.

2. 관련 연구

센서 네트워크에서는 센서 노드의 제한된 자원으로 동작하기 때문에 LEACH, LEACH-C, HEED와 같은 클러스터 기반의 라우팅 방법을 통해 네트워크의 수명을 향상시키고 있다. 그러나, 무선 전송 매체를 통한 상호간의 통신으로 유선 네트워크에 비해 보안이 매우 취약하다. 따라서, 매우 많은 수의 센서 노드가 오류 및 장애를 허용해야 하고 자율적인 네트워크 구성을 통한 효과적인 관리 및 보안 기능 강화가 중요하다. WSN는 대규모의 초소형 센서로 구성되고, 각 센서 노드는 배터리 기반의 제한된 전원으로 동작하며 특정 지역의 환경변화를 감지하고, 각종 센서에서 수집된 정보를 무선으로 수집할 수 있도록 구성한 네트워크이다.[1-3]

센서 네트워크에서 안전한 통신을 위한 보안 서비스 기법으로 키 관리 방법에 대한 다양한 연구가 진행되어 왔다. SINK Node와 베이스 스테이션이 안전하다고 가정하고 중앙 키 관리 기법과 랜덤 키 선 분배 방식을 통해 임의 간에 pairwise 키를 계산 할 수 있는 방법과 노드 노출시에 어느 정도 탄력을 제공하는 방법이 제안되었으나, 노드를 추가로 확장하는 경우에는 키 정보를 확장하기 어려운 단점도 있다. [5-7].



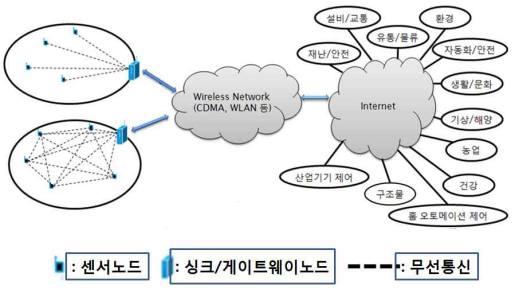
(그림 1) 센서 네트워크의 구성

(그림 1)에 나타난 것처럼 초소형 센서 노드들은 센서를 통한 정보 감지, 감지된 데이터 처리 및 무선 통신이 가능하다.

2.1 무선 센서 네트워크의 구성

센서 네트워크는 아주 작은 초소형의 센서 노드들이 무선통신을 통해 네트워크에 연결되어 있다. 센서 노드가 가져야 할 기능은 컴퓨팅(Computing), 센싱(sensing), 무선통신(wireless communication)이다. 또한, 센서 노드의 조건은 센서들을 통한 정보취득, 무선 네트워크를 통한

통신, 초전력 소모 등이다. 센서 노드들의 연결 장치는 적외선이나 무선방송(radio) 신호를 이용하고 있다. 센서 네트워크의 구성 요소에는 센서 노드, 게이트웨이, 시스템 서버가 있다.



(그림 2) WSN 구성 및 USN 서비스 구조

WSN 구성과 일반적인 USN 서비스 구조는 (그림 2)와 같다.

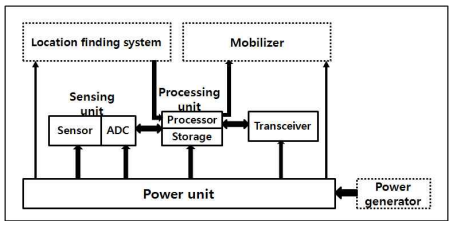
2.2 무선 센서 네트워크 설계 영향 요인

무선 센서 네트워크 설계를 할 때에는 고장 방지 능력(fault tolerance), 확장성, 생산비용, 작동 환경, 센서 네트워크 토폴로지, 하드웨어의 제약, 전송 매체, 그리고 전력 소모와 같은 여러 가지 요소들이 센서 네트워크를 구성하는데 영향을 미친다. [5]

장애 허용 (fault tolerance)은 일부의 센서 노드가 물리적인 손상이나 환경적인 간섭에 의해 동작이 멈추는 경우가 발생한다. 장애 허용은 센서 노드의 고장 원인으로 인한 중단 없이 센서 네트워크 기능을 유지하는 능력이다.[3-5]

확장성 (scalability)은 어떤 현상을 관찰하기 위해 배치된 센서 노드의 수는 응용에 따라 수백에서 수 만개에 까지 있다. 센서 노드의 수는 응용 범위에 따라 네트워크 구조에 관계없이 동작을 잘 할 수 있는 능력을 의미한다. 생산가격(production cost)이란 네트워크는 매우 적은 수의 센서 노드로 구성 되므로 노드의 가격이 매우 저렴해야 한다. 네트워크 설계 시에 전체 가격을 결정하는데 중요한 요인이다.

하드웨어 제약 (Hard constraints)에서 센서 노드는 (그림 3)처럼 초소형 저 전력장치로 센싱을 위한 센서, 센싱 정보를 디지털 신호로 변환하기 위한 ADC (Analog to Digital Converter), 데이터 가공 처리를 위한 프로세서와 메모리, 전원 공급을 위한 배터리, 그리고 데이터 송수신을 위한 무선 트랜시버 4가지 요소로 구성된다. [3-5]



(그림 3) Sensor node의 구성요소

센서 네트워크 토폴로지는 사람의 접근이 불가 능하고 방치되는 수백에서 수천 개의 노드는 일정한 지역에 서로 10피트 미만의 간격으로 배치되는 센서는 빈번하게 고장이 발생하기 때문에 토폴로지 유지는 중요한 일이다. 센서 토폴로지 유지와 변경을 위하여 사전 배치단계, 배치 후 단계, 재배치단계로 구분한다. 초기 배치 계획은 설치비용을 낮아야 하며 먼저 조직을 하거나 계획을 짜는 필요성을 제거하고 배치의 유연성을 증가시키고 자체 조직화와 고장방지능력을 증가시켜야 한다. 배치 후 단계에서 센서 노드는 위치, 도달 가능성, 전원 가용성, 오작동, 업무 수행 때문에 토폴로지를 변경한다. 세 번째 단계는 추가적인 노드는 임무변화나 노드의 오작동을 대체하기 위해 언제든지 유동성 있게 재배치 될 수 있다. 센서 네트워크의 동작 환경에서 센서 노드는 센서 노드들이 접근하기 어려운 지역이나 멀리 떨어진 곳에 설치되어 동작할 수 있다. 어떤 현상을 관측하기 위해 그 현상의 아주 가까운 곳이나 안에 밀집하여 배치된다. 이러한 여러 가지 환경들은 자연에 그대로 노출된 상태로 동작되기 때문에 센서 네트워크 설계는 열악한 환경을 고려하여 설계되어야 한다.[11] 멀티 hop 센서 네트워크에서 통신 노드는 무선 전송 매체 radio, 적외선, 광통신 매체가 있다. 센서 네트워크의 경우 크기가 작고 저렴하며 아주 낮은 전력의 transceiver를 필요로 한다. 그러므로 하드웨어 제약과 안테나 효율과 전력소비 사이의 균형은 맞추기 위해서는 아주 높은 주파수 범위를 가지는 transceiver를 위한 캐리어 주파수를 선택하는데 있어 제약이 있다. 이런 제약

때문 에 유럽에서는 433MHz를 그리고 북아메리카에서는 915MHz 제안되었다. 센서 네트워크 내부 통신이 가능한 다른 방법은 적외선이다. 적외선은 라이센서 무료이고 다른 전기적 장치로부터 간섭에 강하다. 그러나 송신기와 수신기 간의 바라보는 시야를 확보해야 된다는 결점을 가지고 있다. 그 밖에 특별한 응용분야는 특별한 통신 매체를 필요로 한다. [9-10]

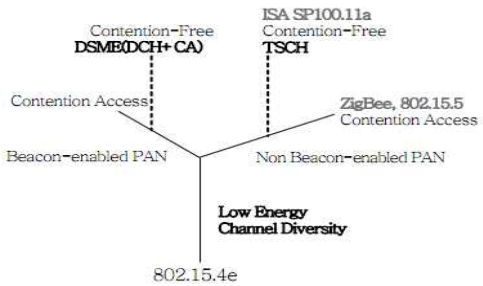
전력 소모는 응용분야의 특성에 따라 다양하다. 산발적인 감지의 경우 지속적인 감지에 비해 전력 소모가 작다. 감지해야 하는 일의 복잡성에 따라서도 전력소모가 다르다. 데이터 통신은 3가지 전력소모 중에 가장 많은 전력을 소모한다. 데이터 통신의 전력 소모를 계산할 때, 활성화 전력뿐만 아니라 전송회로가 켜질 때 소비되는 전력소모도 계산해야한다. 데이터 처리의 에너지 소비는 데이터 통신보다 작다. 1KB를 100미터 전송하는 에너지 소비와 초당 100만 명령어를 처리하는 프로세서에서 3만 명령어를 처리하는 에너지 소비는 똑같다. 이런 이유로 지역 데이터 프로세싱은 멀티 홉 센서 네트워크에서 전력소비를 최소화 하는데 중요하다. 그러므로 센서 노드는 반드시 계산 능력과 그 노드의 주위환경과 상호작용을 할 수 있도록 설계 되어야 한다.

2.3 무선 센서 네트워크 전송기술

무선 센서 네트워크 표준기술은 무선 근거리 개인 통신망(WPAN) 전송 규격을 위한 IEEE 802.15 표준 규격과 ZigBee 규격, IP 기술을 센서 네트워크에 적용 가능하도록 IETF의 6Lo WPAN, Roll, Core WG에서 표준화 하고 있다.[8] 무선 통신 프로토콜은 Wi-Fi와 UWB, Blue tooth, ZigBee 등이 있다. 센서 네트워크는 Ad-hoc을 기반으로 센서 네트워크를 구축하는 것이 주를 이루고 있다. WSN는 통신 거리에 따라서 광대역 통신망인 WAN, 수백 킬로를 담당하는 MAN , 구내망에 이용하는 LAN, 수십 미터 범위에서 사용하는 PAN 그리고 단거리 무선으로 나누어진다. IEEE 802에서의 무선 네트워크의 영역을 보여주고 있다. 단거리 무선은 RFID, DSRC (Dedicated Short Range Communication), NFC (Near Field Communication) 분야를 응용 예로 볼 수 있고, UWB(IEEE 802.1513a) 및 ZigBee (IEEE 802.15.4)를 들 수 있다. 현재 센서 네트워크용 단말에 사용하는 WPAN의 대부분은 통신속도가 수십 kbps~수백 kbps 정도로 수 미터에서 수백 미터 정도의 통신 거리가 확보될 수 있는 저 전력형으로 구성된다.

또한 대부분의 대기 모드를 갖고 있어 소비전력을 최소화하여 사용된다.

ZigBee는 네트워크 층 이상을 규정한 단거리 무선 통신 프로토콜 규격으로 ZigBee Aliance에서 물리층과 MAC층에 대해서는 IEEE 802. 15.4에 의거하고 데이터 전송속도는 최대 250 kbps이며, 적은 소비 전력으로 전원의 수명을 장기간 확보할 수 있는 잇 점으로 가전 네트워크 등에 이용하고 있다. 산업용 모니터 제어 시스템 센서 네트워크 등에 이용하고 있다. 채널은 16채널의 2.4GHz, 10채널의 915 MHz 및 1채널의 868MHz 에서는 각각 250kbps, 40kbps, 20kbps에 해당한다.



(그림 4) IEEE 802.14.4e MAC 동작모드

WPAN(Wireless Personal Area Network)을 구축하기 위하여 결성된 IEEE 802.15 Working Group은 블루투스 (Bluetooth)를 기반으로 한 IEEE 802.15.1 이나 디지털 카메라나 캠코더 등의 휴대용 멀티미디어 장치를 무선으로 연결하기 위한 IEEE 802.15.3에 비해 상대적으로 성능은 떨어지나 저가이며 저전력 장치들 간에 WPAN을 구성할 수 있도록 하는 IEEE 802.15.4(LR-WPAN)의 표준화를 수행하고 있다. Ad-hoc 네트워크에서는 통신 인프라에 의존하지 않고 각각의 무선 단말 즉 센서 노드에서 데이터를 중계하는 네트워크를 구성하게 된다. 모든 센서 노드는 데이터 중계 기능을 갖고 있고 송신 노드로부터 수신 노드까지 복수의 노드를 경유하여 정보 데이터를 전달한다. 따라서 경로제어 기술을 중요하게 되고, MANET (Mobile

Ad-hoc Network)에서 제안하는 프로토콜은 proactive, reactive 및 하이브리드 형으로 분류할 수 있다.

proactive는 주변 노드를 확인하기 위하여 제어 정보의 송수신을 정기적으로 수행하여 전력 소모가 큰 단점이었고, reactive는 proactive에 비해 전력 소모를 줄인 방안으로서 각 노드에서 통신 요구가 있을 때 동작을 하여 주면 노드를 확인하게 된다. 통신을 하지 않을 때는 동작을 하지 않기 때문에 장기간 구동이 가능한 장점을 지니고 있다. 이 두 가지 방법이 혼재된 것이 하이브리드 형이다.

3. 무선 센서 네트워크의 보안 요구사항

센서 네트워크에서는 열악한 주변 환경이 분산 노출되어 있는 센서 노드들이 배치된 물리적 환경이 공격에 그대로 노출되어 전송되는 정보가 변경되거나 유출되어 정보의 기밀성 및 무결성을 쉽게 무너뜨릴 수 있다. 이것은 수집되는 정보의 신뢰성을 떨어뜨리는 결과를 가져온다. 따라서 센서 네트워크의 보안을 강화하기 위한 방법으로 내부적으로 센서 노드의 보안기능을 추가하고 외부적으로 보안위협으로부터 전체 네트워크를 보호하기 위해 네트워크의 모든 부분에 보안 기능을 도입하는 계층적 보안이 필요하다. 센서 네트워크에서 안전한 서비스 제공 및 보안 응용 서비스의 출현을 위해 일반적인 보안 필수 요구사항은 인증, 비밀성, 무결성, 가용성이다. 기밀성, 무결성, 인증, 부인방지를 구현하는 암호학적 방법이 적용되며, 자원제약성이라는 센서 네트워크 환경에 적합한 경량의 저 전력 특성을 가지는 암호 알고리즘이 필요하다. 센서 네트워크에서의 보안 요구사항을 정리하면 첫째, 암호 키를 관리할 수 있는 기능을 제공해야 한다. 둘째, 센서 환경에 적합한 경량화된 암호 및 인증 기능을 제공하고, 셋째, 라우팅 시에 보안 기능을 제공해야 한다. 넷째, 서비스 거부 공격에 강한 구조여야 한다.

3.1. 데이터 비밀성(Confidentiality)

데이터 비밀성은 장치의 분실, 도난, IP sniffing, 장치간 동기화 등에 의해 침해될 수 있다. 비밀성 유지를 위한 기능적 요구사항은 트래픽 데이터 암호화, 키 관리기법 제공, 이동형 장치는 중요한 정보를 암호화, 서버 장치는 저장된 정보를 암호화, 저 전력 암호 알고리즘과 두개체간 인증단계를 통과하면 안전한 비밀 통신채널을 제공할 수 있으므로, 쉽게 비밀성을 보장할 수 있다. 따라서 허가된 노드 외에는 민감한 정보를 접근할 수 없도록 하며, 이것은 비밀 키로 데이터를 암호화한 상태에서 데이터 교환이 이루어져 데이터의 비밀성을 보장해야 한다.

3.2 데이터 인증(Authentication)

데이터 인증은 센서 네트워크 환경하에서 동기화를 수행하는 센서 장치, 장치의 분실 및 도난, Rogue 액세스 포인트 등을 방지하기 위해서는 인증 서비스가 반드시 필요하다. 기존의 인증은 공개키 암호시스템 기반으로 신뢰기관에 의해 발급된 공개키 인증서를 바탕으로 인증하고자 하는 개체의 서명 검증 과정을 통해 이루어진다. USN 환경에서 인증을 보장하기 위해서 요구되는 기능은 상호인증, 동적 키 사용, 무선 구간 키 교환기법이 있다. 인증 방법으로는 Flash ID, Device ID, ESN (Electronic Serial Number)이고, 사용자 인증방법은 PIN (Personal Identity Num -ber), 코드, 패스워드, 생체인식, 스마트카드 등이 있다.

3.3 데이터 무결성 (Integrity)

데이터 무결성은 하나의 개체에서 다른 대체로 가는 메시지가 제 3의 악의적인 개체(공격자)에 의해 방해 받지 않는 것이다. 즉, 상대방 개체와 메시지를 주고받을 때 내용이 변경되지 않는 원본 메시지임을 보장하는 것과 인증 및 키 교환 과정이 어떻게 이뤄지는지 알고 있다면, 메시지 인증 코드 (MAC: Message Authentication Code)와 같은 암호 기법으로 무결성을 보장할 수 있다. 따라서 통신상에서 데이터 무결성은 수신자가 수신한 데이터의 위·변조 여부를 확인하는 것으로 데이터 인증을 통한 데이터 무결성을 보장해야 한다.

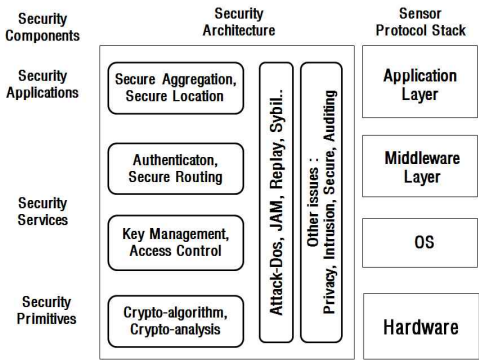
3.4 데이터 가용성 (availability)

데이터 가용성은 센서 네트워크가 센서 노드

가 수집한 정보에 대하여 어떤 방법이라도 요구되는 수준의 안정된 서비스를 수행할 수 있도록 해주는 것이다. 이를 기준으로 센서 네트워크에서 필요로 하는 보안 기능으로는 암호 알고리즘, 키 관리 및 보안 프로토콜, 인증 및 시큐어 라우팅, 시큐어 데이터 집합 등으로 압축할 수 있을 것이다.

4. 무선 센서 네트워크 라우팅 프로토콜

WPAN(Wireless Personal Area Network)을 구축하기 위하여 결성된 IEEE 802.15 Working Group은 블루투스 (Bluetooth)를 기반으로 한 IEEE 802.15.1 이나 디지털 카메라나 캠코더 등의 휴대용 멀티미디어 장치를 무선으로 연결하기 위한 IEEE 802.15.3에 비해 상대적으로 성능은 떨어지나 저가이며 저전력 장치들 간에 WPAN을 구성할 수 있도록 하는 IEEE 802.15.4(LR-WPAN)의 표준화를 수행하고 있다



(그림 5) 센서 네트워크의 보안 구조

무선 센서 네트워크에서 센서 노드간의 통신은 배터리 크기, 센서 노드의 처리 능력, 센서 노드 간 통신 거리 등으로 인하여 많은 제약을 받는다.[8] 무선 센서 네트워크를 위해 만들어진 여러 라우팅(특정 노트까지의 경로를 찾는 방법-네트워크 계층 프로토콜) 프로토콜은 네트워크 구조에 따라 평면 라우팅. 위치 기반 라우팅, 그리고 계층적 라우팅으로 분류할 수 있다.

평면기반 라우팅이란, 모든 노드가 동등한 입장에서 공통된 하나의 라우팅 기법을 사용하는 방식을 의미한다. 위치기반 라우팅이란, 센서 노드의 위치 정보를 기반으로 라우팅 경로를 설정하는 방식을 말하다. 계층기반 라우팅이란, 클러스터링을 기반으로 노드 간의 계층적 단계를 두어 데이터를 전송하는 방식을 의미한다.

4.1. 평면 라우팅(Flat routing)

평면 라우팅 방식은 센서 네트워크에서 가장 많이 채택하는 방식으로 기존의 Ad-hoc 라우팅 프로토콜과 유사하다. Direced diffusion[9]은 수집 노드에서 원하는 감지 정보를 얻기 위해 전체 센서 노드들에게 특정한 질의 패킷을 전송한 후 그 질의에 해당하는 노드들이 반응하여 센싱 데이터를 수집하는 방식이다. diffusion은 감지 데이터들을 기반으로 라우팅 경로를 설정함으로 데이터 중심적 라우팅 프로토콜이라 한다. Directed diffusion 방식은 특정 지역에서 발생하는 어떤 이벤트를 확인하기 위해 데이터를 기반으로 라우팅 패스를 설정하는 on-demand 방식의 라우팅 프로토콜이다.

4.2. 위치 기반 라우팅

일반적으로 센서 네트워크의 애플리케이션 특성상 센서 노드들은 자신의 위치를 알고 있어야 하는 경우가 많다. 위치 기반의 라우팅 연구들은 각 센서 노드들이 이미 자신의 위치를 알고 있다는 가정 하에서 시작된다. greedy based routing : 데이터 전송 시 최종 목적지에 가장 가까운 이웃 노드를 선택하여 그 노드에게 데이터를 보내는 라우팅 기법이다. 가장 간편한 라우팅 기법이지만, 이웃 노드의 위치 정보와 최종 목적지(수집 노드)의 위치 정보를 알고 있을 경우에만 사용할 수 있는 라우팅 기법이다.

4.3. 계층 기반 라우팅

각 노드들이 일정 집합을 구성하고 임의의 헤더를 선출하여 헤더가 직접 혹은 다른 헤어와의 협업을 통해 센싱 데이터를 수집 노드에게 전달하는 방식이다. clustering : LEACH는 네트워크에 존재하는 모든 노드들의 에너지 소모를 균등하게 하기 위해 분산 클러스터를 구성하여 데이터를 전달하는 라우팅 기법이다.

4.4 센서 네트워크에서의 키 관리 기술

키 관리 기술은 센서 네트워크 환경에서 제한된 자원으로 효율적이고 안전한 키 설립 방법을 설계하는 것이다. USN 환경에서 센서 노드들 사이의 안전한 통신을 위해서는 키가 반드시 필요하다. 키는 암호 기술을 기반으로 하여 키의 생성, 분배 및 활용 등까지 모든 부분을 신뢰 기법이다. single network-wide key는 키는 가장 단순한 방법으로 하나의 single key가 모든 노드들에게 미리 설치된다. 모든 노드들은 이 키를 사용하여 메시지를 암호화, 복호화 하게 된다. 이 방법은 메모리의 공간을 적게 사용한다는 장점이 있지만 공격자의 공격을 받기 쉽다는 단점이 있다.

pair-wise key establishment 기법은 무선 센서 네트워크에서 가장 효율적인 키 설립 방법으로 모든 노드가 유일한 키를 가진다. 센서 네트워크의 노드가 n개 있을 때 각 노드는 n-1 개 키를 가진다. 각 노드는 다른 모든 노드들의 신원을 확인할 수 있다. 예를 들어 센서 네트워크의 모든 노드의 개수가 10,000개라면 각 노드는 9,999개 키를 저장하는 메모리를 필요로 한다. 센서 노드의 자원은 제한되어 있기 때문에 이 기법은 작은 규모의 네트워크에 적합하다. Trusted Base Station (키 분배센터) 기법은 통신하는 두 노드 사이의 세션 키를 신뢰할 수 있는 base station에서 두 노드에게 보내는 방법을 사용한다. 이 방법을 중앙 집중 키 분배 센터 (KDC : Key Distribution Center) 라고 부르기도 한다. 신뢰된 베이스 스테이션(trusted base station)은 적은 메모리를 요구하고 노드의 응답을 완벽하게 제어한다. 그러나 베이스 스테이션이 공격자의 목표가 될 수 있다는 단점이 있다.

5. 공격 유형에 따른 키 관리 적용 고려사항

센서 네트워크 환경에 가해질 수 있는 공격 형태를 다양한 관점에서 분류하고, 각 공격 유형을 방어하기에 적절한 키 관리 기법을 분석한다. 각 노드들이 일정 집합을 구성하고 임의의 헤더를 선출하여 헤더가 직접 혹은 다른 헤어와의 협업을 통해 센싱 데이터를 수집 노드에게 전달하는 방식이다.

5.1 공격 유형별 키 관리 기술 적용

무선 센서 네트워크 환경에서 발생할 수 있는 네트워크 공격 유형으로 도청, 데이터 변조, 서비스 거부, 라우팅 공격 등이 있다. 센서 노드는 열악한 환경에 노출되어 주변 환경 정보를 감지하여 처리하기 때문에 외부로부터 물리적인 공격을 받을 수 있다. 따라서, 센서 네트워크에 가해질 수 있는 다양한 공격에 대한 보안 요구사항을 살펴본다. 또한 다양한 키 관리 기법 중 사전 키 분배 기법의 기본으로 하여 공격 유형에 따른 키 관리 기술의 특성을 분석한다.

5.2. 키 관리를 위한 고려 사항

센서 네트워크를 위한 키 관리를 위해서는 센서 네트워크를 위한 키 관리를 위해서는 다음과 같은 사항을 고려해야 한다. 우선 센서 노드들이 랜덤하게 배치되기 때문에 네트워크 토폴로지 정보를 사전에 획득하기 어려우며, 센서 노드는 제한된 자원을 가지고 있기 때문에 경량화된 암호 알고리즘이 필요하다. 또한 센서 노드의 잘못된 동작과 에너지 소모 등으로 인해 센서 노드의 추가적 설치가 필요한 경우가 발생할 수 있기 때문에 키의 추가 및 제거가 용이해야 한다. 그리고 센서 네트워크가 실외에 설치될 경우 물리적 공격으로 인한 노드 탈취의 문제를 고려해야 하며 마지막으로 확장성도 함께 고려해야 한다.

센서 네트워크는 다양한 분야에 적용될 수 있기 때문에 기본적으로 알려진 다양한 공격 방법에 내성을 가져야 한다. 특히 공격자가 키 생성 및 분배 과정에서의 트래픽 분석을 통해 키의 생성 정보 및 네트워크 환경 정보를 쉽게 획득할 수 있기 때문에 중요한 메시지는 암호화를 통해 전달되어야 한다. 또한 물리적인 공격을 통해 탈취한 노드로부터 노드에 저장된 키의 정보, 네트워크 토폴로지, 베이스 스테이션의 위치 등과 같은 중요 정보를 획득할 수 있다. 따라서 센서 노드가 탈취되더라도 그 영향을 최소화하며 노드의 배치 이후에는 칩 디버깅을 통한 정보 획득이 불가능해야 하다.

5.3. 공격 유형에 따른 키 관리 적용 방법

다음에서는 공격 유형과 그에 대응하는 적절한 기 관리 기법 간의 관계를 설명한다. 도청은 센서 노드 간 통신을 모니터링 함으로써 정보를 획득하는 공격이므로 데이터를 암호화해서 주고받음으로써 방어할 수 있다. 데이터 위변조 또한 특정 노드로부터 변조된 메시지를 받지 않도록 상호 노드 간 암호화키를 설정하여 메시지를 인증하는 방법을 이용하여 방어할 수 있다. 따라서 각 노드마다 다른 키를 설립하는 Pairwise키나 Random pairwise 키 기법 등을 이용할 수 있다. Radom pairwise 키는 pairwise의 비효율적인 메모리 문제를 해결하지만 노드 캡처에 대한 저항성을 가지는 키 관리 기법으로 확장성이 있기 때문에 대규모의 네트워크에서도 사용할 수 있다. 서비스 거부 공격이나 라우팅 공격 등은 정상적인 노드로부터 전파 방해, 선택적 전달 등의 공격을 통해 다른 노드들에게 비정상적인 정보를 전달하는 방식이다. 이 경우 공격자가 아닌 정상적인 노드만이 네트워크에 참여하는 방식을 사용한다. 또한 물리적인 공격으로 인해 노드가 탈취되었을 경우 이를 대체할 노드 추가가 용이한 확장성이 있는 키 관리 방법을 선택할 수 있다. 라우팅 공격의 경우에는 키 관리 기법 이외에도 LEAP를 사용하면 HELLO flood 공격과 웜홀 (Wormhole) 공격을 제외한 대부분의 외부 공격에 내성을 가지고 있기 때문에 공격을 막을 수 있다.

마스터 키 관리 기법은 마스터키를 이용해 pairwise키를 생성하고 사용한 마스터키를 주기적으로 교체하는 방법을 이용하여 공격을 막을 수 있다. 하지만 공격자가 마스터키를 지우기 전에 노드를 탈취할 수 있으며 이 경우에 공격자가 모든 pai-wise 키를 생성할 수 있기 때문에 노드 탈취에 약하다는 단점이 있다. 따라서 피해를 최소화하기 위해서는 센서 개수가 적은 소규모 네트워크에서 마스터키를 계속 교체하는 방식 을 이용하는 것도 하나의 방법이 될 수 있다.

이러한 분석을 바탕으로 센서 네트워크의 형태에 따른 키 관리 기법을 6절에서 설명한다.

프로토콜 스택은 응용 계층, 전송 계층, 네트워크 계층, 데이터 링크 계층, 물지적 계층, power management plane, mobility managemen t plane, 그리고 task management plane으로 구성된다.

감지 역할에 따라서 다른 종류의 소프트웨어를 응용 계층에서 설계하고 사용할 수 있다. 전송 계층은 센서 네트워크 응용프로그램이 필요로 한다면, 데이터의 계속적인공급을 유지하는 것을 도와준다. network layer는 전송 계층에 의해 공급된 데이터를 전송하는 것을 처리한다. 환경의 잡음이 심하고 센서 노드들이 움직일 수 있기 때문에, MAC 프로토콜은 전력을 알고 있고 이웃들의 브로트캐스트 충돌을 최소화 할 수 있어야 한다. physical layer는 간단하지만 변조와 전송과 받는 기술을 활성화 시키는데 필요한 것들을 다룬다. 추가적으로, power, mobility, 그리고 task management plane들은 센서 노드들 사이에 전력과 이동 그리고 역할 분배를 관찰한다. 응용 계층은 감지 역할에 따라서 다른 종류의 소프트웨어를 설계하고 사용할 수 있도록 해준다. 우리가 아는 바로는, 비록 많은 센서 네트워크의 응용분야가 정의되고 제안되었지만, 센서 네트워크에 대한 잠재적인 응용 계층 프로토콜은 아직 개발되지 않은 부분으로 남아있다. 이 논문에서는, 센서 네트워크 응용분야와 다른 계층을 관련해서 제안된 계획을 기반으로 하는 센서네트워크에 필요한 3가지 응용 계층 프로토콜, 센서 관리 프로토콜, task assignment and advertisement protocol 그리고 sensor query and data dissemination protocol를 조사한다.

Sensor management protocol(SMP): SMP는 낮은 계층의 하드웨어나 소프트웨어를 센서 네트워크 관리 응용 프로그램에 알기 쉽게 해준다. 시스템 관리자는 SMP를 사용하여 센서 네트워크와 소통한다. SMP는 데이터 집합에 관련된 규칙을 설명하고 센서노드를 특성을 기반으로 이름을 지정하고 모은다. 그리고 location finding 알고리즘과 센서노드들의 시간동기와 관련하여 데이터를 교환하고 센서들을 이동시키고 센서네트워크 환경설정과 노드의 상태를 묻고 센서 네트워크와 데이터 통신의 주 분배와 보안의 인증을 재 설정해주는 역할을 하는 소프트웨어를 제공하는 관리 프로토콜이다.

Task assignment and data advertisement (TADAP): 센서 네트워크의 또 다른 중요한 작동은 관심사 전파이다. 사용자는 그들의 관심사를 센서 노드 혹은 노드들의 부분 집합 혹은 전

체 네트워크에 보낸다. 이 관심사는 어떤 현상이나 일이 발생하는 것에 대한 어떤 특성에 관한 것일 것이다. 다른 접근방식은 센서 노드들이 가능한 데이터를 유저에게 알리는 것이다. 그리고 유저는 관심 있는 데이터를 요구한다. 사용자 소프트웨어에 관심사 전파에 대한 효율적인 인터페이스를 제공하는 application layer 프로토콜은 다음에 설명될 라우팅과 같은 낮은 계층에 유용하다. Sensor query and data dissemination protocol (SQDDP): SQDDP는 유저 응용프로그램에게 문제 문의, 문의에 대한 응답, 들어오는 응답을 모으는 인터페이스를 제공한다. 이러한 문의는 일반적으로 특별한 노드에는 전달이 되는 것이 아니라 특성을 기반으로 혹은 장소 기반으로 이름을 지어서 문의한다. Sensor query and tasking language(SQTL)는 서비스들의 아주 큰 집합을 제공하는 응용프로그램으로 제안되었다. SQTL은 3가지 타입의 일을 지원한다. 3가지는 receive, every, 그리고 expire의 3가지 키워드로 정의된다. receive 키워드는 센서 노드가 메시지를 받을 때 센서 노드에서 발생되는 일을 정의한다. every 키워드는 타이머나 타임아웃 때문에 정기적으로 발생하는 일을 정의한다. 그리고 expire키워드는 타이머가 만료되었을 때 발생하는 일을 정의한다. SQTL이 제공되지만, 다른 종류의 SQDDP는 다양한 응용분야를 위해 개발 될 수 있다. SQDDP의 사용은 각각 응용분야에 유일 할 것이다.

Transport layer는 시스템이 인터넷이나 다른 외부 네트워크를 통하여 접근 될 수 있도록 계획될 때 필수적으로 필요하게 된다. 현재 윈도우 전송 메커니즘인 TCP는 센서 네트워크의 극단적인 특성에 맞지 않다. TCP분배는 인터넷과 같은 다른 네트워크에 센서네트워크를 소통시킬 때 필요하게 될 것이다. 이런 접근 방식에서 TCP연결은 Sink node들에서 끝나고 특별한 전송 계층 프로토콜이 Sink노드와 센서 노드들 간에 통신을 다루게 된다. 그런 결과로 유저와 Sink노드간의 통신은 internet혹인 위성을 경유한 UDP 혹은 TCP이다. 반면에, 각 센서노드는 제한된 메모리를 갖기 때문에 싱크와 센서노드들 간의 통신은 순전히 UDP 형태의 프로토콜에 의해 행해질 것이다 TCP와 같은 프로토콜과는 달리 센서네트워크의 끝과 끝 통신은 전체적인 어드레싱을 기반으로 하지 않을 것이다. 이러한 계획은 특성기반의 이름 화를 고려해야하고 이는 데이터 패킷의 목전지를 가르칠 때 사용된다. 전력소비와 확장성 그리고 데이터 중심의 특성과 같은 요인들은 센서 네트워크가 전송 계층 프로토콜에서 다른 처리를 필요로 하게 한다. 그러므로 이러한 요구사항들은 새로운 타입의 전송 계층 프로토콜의 필요성을 강조한다.

네트워크 계층은 보통 다음과 같은 원칙을 따라 디자인 된다. 보통 전력 효율이 중요한 고려사항이다. 센서 네트워크는 대부분 데이터 중심적이다. 데이터 집합은 그것이 센서 노드들 간의 협력적인 노력을 방해하지 않을 때 유용하다. 가장 이상적인 센서 네트워크는 특성기반의 주소화와 지역 정보를 가진다. 다음의 접근방식 중 하나는 에너지 효율적인 전송을 선택하는데 사용 될 수 있다.

데이터 링크 레이어는 데이터 줄기의 멀티플렉싱, 데이터 프레임 감지, 매체접근 그리고 에러 제어가 있다. 이것은 네트워크 통신에서 믿을 수 있는 점대 점과 점대 많은 점 통신을 보장한다. 물리 계층은 주파수를 선택, 캐리어 주파수 발생, 신호 감지, 변조와 데이터 부호화에 책임을 가진다. 장거리 무선 통신은 에너지와 수행 복잡성관점에서 봤을 때 비용이 많이 든다. 센서 네트워크를 물리계층에서 설계하는 할 때, 에너지 최소화는 가장 중요하게 여겨지고 덧 붙여서 부패, 분산, 반사, 회절, 다중통로, 페이딩 등도 중요하다. 좋은 변조 계획의 선택은 센서네트워크에서 믿을 수 있는 통신을 하기 위해 아주 중요하다. Binary와 M-ary 변조가 있고 M-ary 변조는 낮은 시작 전력을 가지는 시스템에 대해서만 많은 이득을 얻는다. Ultrawideband (UWB) 혹은 impulse radio(IR)은 베이스밴드 펄스레이더와 시스템과 측정시스템에 사용되어 왔으며 현재도 집안 무선 네트워크와 같은 응용분야에 중요한 관심사로 여겨지고 있다. UWB의 주요 이점은 여러 길에 대한 탄력이다. 낮은 전송 전력, 간단한 수신회로는 UWB를 센서 네트워크의 매력적인 참여요소로 만든다.

6. 결론 및 향후과제

센서 네트워크는 초경량, 저전력의 많은 센서

들로 구성된 무선 네트워크이다. 수많은 센서 노드들로 구성되는 무선 센서 네트워크 환경에서 데이터 유통 정보의 도청, 데이터 위조 및 서비스 거부 등 네트워크 공격에 노출되는 문제점이 있다. 본 논문에서는 센서 네트워크의 안전한 통신을 위하여 키 분배와 관리를 효율적으로 할 수 있는 프로토콜이 중요하다. 본 논문에서는 외부 공격유형에 따른 키 관리 적용방법과 무선 센서 네트워크를 공격하는 방법, 보안 프로토콜을 다루었다, 효과적인 라우팅과 키 관리 프로토콜을 연구하기 위하여 각종 자원에 극심한 제약을 가지는 센서 네트워크상에서 암호화 키 관리 프로토콜을 제안하였다. 향후 연구과제로는 기존에 제안된 키 관리 프로토콜과 키 설정 메카니즘의 성능분석을 통해 그 효율성을 증명하는 연구가 필요하다.

참 고 문 헌

[1] I.F.Akyildiz, W.Su, Y.Sankurasubramaniam, E.Cayirci "Wireless sensor networks: a survey" Computer Networks December 2002 pp. 393-422

[2] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," In IEEE Symposium on Reserch in Security and Privacy, may 2003, pp. 197-213.

[3] R. Juang H. Oki Y. Wang M. Martonosi L. Peh D. Rubenstein "Energy-Efficient computing for Wildlife Tracking: Design Tradeoffs and Early Experiences with ZebraNet" in Proceedings of ASPLOSX October 2002.

[3] N. Xu S. Rangwala K. Chintalapudi D. Ganesan A. Broad R. Govindan D. Estrin "A Wireless Sensor Network for Structural Monitoring" In Proceedings of the ACM Conference on Embedded Networked Sensor Systems November 2004.

[4] Adrian Perrig, Robert Szewczyk, Victor Wen, David Culler, J. D. Tygar, "SPIN: Security Protocols for Sensor Networks", Mobile Computing and Networking 2001.

[5] Chris Karlof and David Wagner "Secure Routing in Wireless Sensor Networks: Attacks and Counter-measures" First IEEE International Workshop on Sensor Network Protocols and Applications May 2003.

[6] 김미희, 채기준 " 계층적인 센서 네트워크에서 확장성을 제공하는 분 산 키 관리 방법" 한국컴퓨터종합학술대회 논문집 Vol. 33, No 1(C) 2006. pp 334-335

[7] H. Abrach S.Bhatt J. Carlson H. Dui. Rose A. Sheth B. Shucker J. Dent R. Han "MANTIS: System Support for Multimodal Network of In-Situ Sensors" Proceeding Of 2nd ACM Workshop on Wirless Sensor Networks and Applications (WSNA' 03) San Diego CA Sep 2003.

[8] 정운철, 박태준, 신창섭 "무선 센서 네트워크 전송 기술 표준화" 전자통신동향분석 제25권 제4호 Aug 2008. pp 27-28

[9] H. Han A. Perrig D. Song "Random Key Predistribution Schemes for Sensor Networks" IEEE Symposium on Security and Privacy 2003.

[10] J. Hill R. Szewczyk V. Wen D. Culler J.D.Tygar "SPINS : Security Protocols for Sensor Networks" Wireless Networks Journal (WINET) 8(5):521-534 Sep 2002.

[11] Anthony D. Wood John A. Stankovic "Denial of Service in Sensor Networks" IEEE Computer October 2002.

[12] C. Intanagonwiwat et. Al. "An Application-Specific Protocol Architecture for Wireless Microsensor Networks" IEEE/ACM Transactions on Networking Vol.11 No.1 Feb. 2003 pp. 2-16.

[13] 전자통신동향분석 제20권 제1호 2005년 2월 Research Trend for Sensor Network Security 나재훈(J.H. Nah) 채기준(K.J. Chae) 정교일(K.I. Chung)

[14] Sencun Zhu Sanjeev Setia and Sushil Jajodia "LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks" Proc. of the 10th ACM Conference on Computer and Communication Security(CCS) 2003.

[15] [무선 센서 네트워크 보안 관리 지침
(정보통신단체표준) Guidelines for Security Management of Wireless Sensor Network
제정일: 2010.12.23

[16] H. Chan A. Perrig and D. Song "Random Key-Assignment for Secure Wireless Sensor Networks" Proc. of the 1st ACM Workshop on the Security of Ad Hoc and Sensor Networks(SASN) 2003.

[17] D. Liu and P. Ning "Establishing Pairwise Keys in Distributed Sensor Networks" Proc. of the 10th ACM Conference on Computer and Communication Security(CCS) 2003.

[18] D. Liu and P. Ning "Location-Based Pairwise Key

Establishments for Static Sensor Networks" Proc. of the 1st ACM Workshop on the Security of Ad Hoc and Sensor Networks(SASN) 2003.

[19] G. Jolly Kuscu and P. Kokate "A Low-energy Key Management Protocol for Wireless Sensor Networks" Proc. of the 8th IEEE International Symposium on Computers and Communications June 2003.

박 성 곤

1980년 : 광운대학교 전자공학과(공학사) 1984년 한양대학교 전자공학과 (공학석사). 1997년 충북대학교 컴퓨터공학과(공학박사)

1980년~1983년: (주) LG전자 정보통신기기사업부

1983년~1986년: (주) 쌍용정보통신 연구소

1991년~2006년: 원주대학 컴퓨터과학과

2007년~현재: 강릉원주대학교 멀티미디어공학과 교수

관심분야 : 정보보호(Personal Information), 유비쿼터스 컴퓨팅(AR), 디지털컨텐츠(DRM)