ZigBee 센서네트워크에서 효율적인 키 연결 알고리즘

서대열*, 김진철**, 오영환*
*광운대학교 전자통신공학과 **한전KDN(주)
seody80@hanmail.net, kjc@kdn.com, yhoh@daisy.kwangwoon.ac.kr

Effective Key Establishment Algorithm used ZigBee Sensor Network

Daeyoul Seo* Jinchul Kim**, Younghwan Oh*
*Kwangwoon University **Korea Electric Power Network Co.,Ltd.

요 약

IEEE 802.15.4 표준은 Low-Rate WPAN 환경에서 디바이스들의 PHY 계층과 MAC 계층을 정의하고 있다. 이러한 표준 기술을 기반으로 산업화를 위한 응용서비스 개발은 ZigBee Alliance에서의 표준화 작업을 통해 진행되고 있으며 네트워크, 보안 등의 기술적 요구사항 및 동작순서 등을 정의하고 있다. 하지만 ZigBee 네트워크에서 coordinator는 디바이스들의 전송 빈도가 낮은 패킷들도 받아야 하고 처리도 해주어야 하기 때문에 그에 따른 전력소모가 상당히 높다. ZigBee Alliance에서는 보안에서 가장 핵심인 trust center 역할을 coordinator가 하도록 정의하고 있다. 새롭게 PAN에 조인하는 디바이스마다 coordinator와 키 연결을 해야 하기 때문에 coordinator는 부하가 집중되고, 악의 있는 디바이스에게 직접적으로 위험에 노출되는 단점이 있다. 본 논문에서는 새롭게 PAN에 조인하는 디바이스가 child 노드와 parent 노드끼리 키 연결을 하는 child-parent 키 연결 알고리즘을 제안하였다.

I. 서론

유선통신 분야에서의 데이터 고속화와 같이 무선 통신 분야에서도 데이터의 고속화에 초점을 맞추어 수 Mbps에서 수 십 Mbps의 데이터 전송률을 가지는 근거리 무선 LAN 기술이 개발되어지고 있고, 이와 더불어 단거리 무선 PAN(Personal Area Network)에서도 데이터 전송률이 고속화되면서 수백 Kbps에서 수백 Mbps에 이르고 있다. 이와 같이 무선의 고속화와 편이성에 의해 무선의 효용성이 증가 되면서 다양한 분야에서 적용되고 있다. 이와 같이 무선의 고속화와 편이성에 의해 무선의 효용성이 증가 되면서 다양한 분야에서 적용되고 있다. 그러나 응용분야에 따라 현재까지의 기술 규격으로는 저속, 저가, 저전력이 소모되는 응용분야의 요구사항을 만족하기에는 적절치 못한 상태이다. 특히 저 전력이 요구되는 응용분야에서는 802.. 11의 무선 LAN 기술은 적절치 못하다.

무선 PAN에서 대표적인 기술인 블루투스는 원래 유선의 대체로서 인식되었으나 점점 복잡해지는 특성과 저전력 소모 응용에 적절치 못하여 이같은 복잡성으로 인해 초기의 목표를 상실하고 있다. 이들 기술은 배터리의 수명에서도 한계가 있어서 설치 후 여러 차례의 배터리의 교환이 요구된다. 그러므로 IEEE 802.11 무선 LAN이나 블루투스는 저속의 저가, 저 전력의 응용에는 적합하지 못하다.

이러한 문제점을 해결할 수 있는 기술로 ZigBee[1,2,3,4,5,6] 기술이 있다. 저가, 저 전력의 빠른 데이터 전송 기술을 자랑하는 ZigBee는 이미 주목을 받고 있다. 이들 업체는 Honeywell과 Eaton사와 같은 산업 제어 및 홈 오토메이션 업체들에서부터 Mattel사와 같은 장난감 업체에 이른다. 시스템에 ZigBee를 구현하는 비용이 2달러도 안 되기 때문에 네트워크에 더 많은 노드들을 저렴하게 설치할 수 있으며, 구현 측면에서 ZigBee 프로토콜은 블루투스나 802.11 무선 LAN 프로토콜보다 훨씬 간단하게 구성할 수 있다.[7,8]

본 논문에서는 ZigBee 보안에 대해서 알아보고 새롭게 P