무선 센서 네트워크에서 MAC 주소기반의 불법 노드의 침입탐지시스템 구현

성기택* · 김관형**

*동명대학교 정보보호학과

**동명대학교 컴퓨터공학과

Implementation of MAC address based illegal node IDS(Intrusion detection system) in Wireless Sensor Networks

*Ki-Taek Seong, **Gwan-Hyung Kim

*Dept. of Information Security, Tongmyung Univ.

**Dept. of Computer Eng., Tongmyung Univ.

E-mail : ktseong@tu.ac.kr

요 약

본 논문에서는 무선 센서네트워크 환경에 적용할 수 있는 외부 노드의 침입을 탐지하는 방법을 제안하였다. 센서노드의 무선통신을 지원하는 네트워크 장치에 고유하게 부여된 MAC 주소를 이용하여 외부로부터의 허락되지 않는 노드의 네트워크 내부로의 침입을 감지하는 방안을 제안하였다. 실제 센서노드를 이용한 침입탐지 시스템을 개발, 실험을 통하여 효율성을 확인하였다.

키워드

WSN, WSN security, MAC address, intrusion detection system

Ⅰ. 서 론

센서 네트워크는 유비쿼터스(ubiquitous) 컴퓨팅을 위한 일종의 ad-hoc 네트워크로 소형, 저전력 소비와 함께 다수의 센서들로 구성된 노드로서 네트워크를 형성하는 장치이다[1]. 센서 네트워크를 구성하는 노드의 수가 수개에서 수천개 등 응용분야에 따라 많을 수 있고, 각 센서 노드들은 제한된 전력과 컴퓨팅 능력을 가지며, 경우에 따라 노드들의 네트워크로의 참여/배재됨에 따라 센서 네트워크의 토폴로지가 자주 변화될 수 있다는 특성을 갖는다. 이러한 센서 네트워크는 센서를 통한 정보감지 및 감지된 정보를 처리하는 기능을 수행함으로써 전장에서의 이상징후 감시와 같은 군사적 목적뿐만이 아니라 건축구조물의 이상 감지, 사람이 접근하기 어려운 열악한 환경에서의 상태 모니터링과 같은 산업분야에도 다양하게 응용되고 있다. 센서노드 자체가 사용자의 상시 접근이 어려운 환경에 분포되는 특성에 따라 외부에 쉽게 노출 될 수 있으며 이에 따라 네트워크 자체는 보안문제에 쉽게 노출될 수 있다.

본 논문에서는 무선 센서 네트워크가 갖는 보안 취약성 중에서도 외부 노드의 접근을 감지하는 방법에 관하여 기술하였다. 특히 센서 노드의 필수 구성요소인 무선 통신장치의 특징인 MAC (media access control) 주소의 특성을 이용하여, 수시로 변경되는 네트워크 토폴로지 변경을 위한 라우팅 시도 시 불법의 노드가 라우팅에 참여하는 것을 방지하는 방법을 제안하였다.

논문의 구성은 다음과 같다. 2장에서는 센서 네트워크 보안 관련 분류 및 이에 대응하는 해결방안을 소개하고, 3장에서는 센서 네트워크 보안에 다양하게 응용가능한 외부 불버노드의 감지를 위한 방법에 관하여 설명하고 이에 대한 구현결과를 4장에 보였으며, 결론과 함께 향후 연구진행에 대한 내용은 5장에 기술하였다.

Ⅱ. 관련연구

센서 네트워크의 보안 취약성 및 방지 방안은 다음과 같이 분류된다[2].

1) 도청

도청의 경우 센서 네트워크에서는 노드 간 통신이 IEEE 802.15.4 LRWPAN 등과 같은 무선통신으로 이루어지므로 통신 범위 내에서 어떤 노드라도 통신 규약만 지키면 통신이 가능하여 도청이 용이하므로 정보에 대한 기밀성이 제공되어야 한다.

해결 방안 : 무선 통신에서 암호알고리즘을 적용하거나(예: CC2420 칩의 경우 AES-128 등의 다양한 암호방법을 제공)[3], 센서 네트워크 개발 시 사용되는 운영체제에서 제공하는 보안 모듈(예 : TinyOS에서의 TinySec[4])을 적용하는 것 등이다.

2) 데이터의 위변조

네트워크 라우팅을 할 때 노드에 대한 인증기능이 없는 경우 외부의 불법 노드가 네트워킹에 참여하게 되어 데이터 위변조의 위험에 노출된다.

해결방안 : 통신 데이터의 기밀성 및 무결성을 보장하기 위해 암호화 알고리즘을 사용할 수 있다. 이때 키 분배문제가 대두된다. 센서 네트워크의 특성상 에너지 효율적인 키 배분방식에 관한 연구가 진행되어 왔으며 대표적인 키 분배 알고리즘으로서 사전 키 분배방식, 공개키 암호화 알고리즘을 통한 키 분배방식, 인증 센터를 이용한 키 분배방식 등이 있다.

3) 라우팅 공격

센서 노드에 대한 인증 기능이 없을 경우 불법 노드가 네트워크에 참여하여 라우팅 정보를 훼손시켜 본래의 네트워크 기능을 마비시키거나 외부 공격 노드를 네트워크의 일부로 참여시킬 수 있다.

해결방안 : 노드 인증방법에 대한 연구가 진행되고 있으며, 대표적인 인증 방식은 SPINS(Security Protocols for Sensor Networks) 보안구조이다[5]. 이 방법은 데이터의 기밀성을 제공하기 위한 SNEP(Secure Network Encryption Protocol) 구조와 브로드캐스팅되는 데이터의 인증을 제공하기 위한 uTESLA 스킴으로 구성되어 인증키를 이용한 데이터의 무결성 인증을 통한 노드 인증기법이다. 전자통신연구소(ETRI)에서는 공개키 암호프로토콜을 이용하여 센서 노드간 인증을 수행하며 인증에 통과한 노드만 상호 통신이 가능한 방법을 개발하였으며 이를 이용하여 새로운 노드가 들어올 경우 인증을 수행하여 보안 네트워크를 구성할 수 있다.

4) 물리적 공격

센서 네트워크는 외부환경에 노출되어 운영되므로 물리적인 손상, 탈취 등의 공격에 취약하다.

해결방안 : 물리적 손상, 절취와 같은 물리적 공격은 tempering 회로 등을 적용하여 대처가능하다.

센서 네트워크를 구성하는 노드에 대하여 위장 또는 다른 외부노드가 접근하는 것을 구분한다면 전술한바와 같이 도청, 데이터의 위변조, 나아가 라우팅 공격 등에 효과적으로 대응할 수 있다. 따라서, 센서 네트워크를 구성하는 모든 노드와 그 이외의 노드를 구분하는 방안을 제안한다

Ⅲ. 제안하는 방법

3.1 MAC address

MAC 주소는 OSI 통신규약 7계층 중 물리계층 다음의 데이터 링크계층에서 정의된 주소로서, 실제 데이터 전송이 이루어지고 있는 망에서 서로를 인식하기 위하여 사용하는 구분자 역할을 한다. IEEE 802.15.4 ZigBee MAC의 경우 64bit의 주소비트를 할당하여 최대 65535개 노드를 구분할 수 있다[3].

1 byte	8 bytes	4 bytes	1 byte	2 bytes
Flags	Source Address	Frame Counter	Key Sequence Counter	Block Counter

그림 1. CC2420 칩에 정의된 MAC주소 필드(Source address)

이 MAC 주소는 벤더주소 32bit, 자체 주소 32bit로 구성되어 있으며 MAC 주소의 유효성은 브로드캐스팅 도메인에서만 유효하다.

센서 네트워크 토플러지가 Star형인 경우 브로드 캐스팅 도메인에 따른 MAC 주소의 유일성이 보장되며, 계층적 구조의 토플러지 경우 고유의 ID(CC2420의 경우 16bit의 PAN Identifier)를 사용하여 구분한다. 또한 센서 네트워크에서 일단 라우팅이 완성되었다는 것은 MAC 주소 또는 PANID를 사용했다는 의미이며 라우팅에 참여한 노드의 MAC 주소는 응용에 따라 베이스 스테이션(BS:Base Station) 또는 모든 노드가 될 수 있다.

결론적으로 라우팅이 완료된 센서 네트워크에서는 네트워크에 참여하는 모든 노드에 때한 MAC 주소 또는 PANID 정보를 저장가능하다.

3.2 제안하는 방법

본 연구에서 제안하기 위하여 다음과 같은 전제조건을 제시한다.

가. 적용하는 센서 네트워크는 단일 또는 복수개의 BS와 다수의 일반 노드로 구성되어 있다.
나. 모든 BS는 사용하고자 하는 센서 노드에 대한 MAC 주소 정보를 저장하고 있다.

제안하는 방법의 흐름도는 그림 2.와 같다.

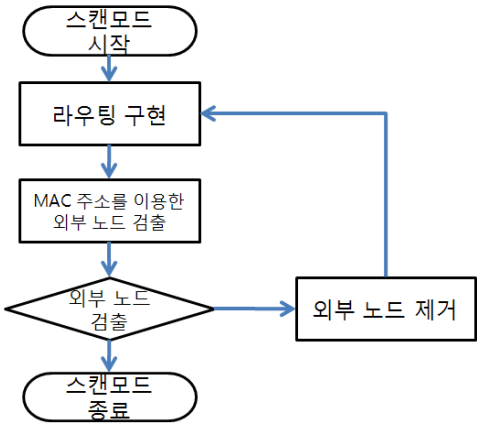

그림 2. 외부노드 탐지기능 흐름도

센서 네트워크는 에너지 효율성을 높이기 위하여 수시로 네트워크 토폴러지를 변경하기 때문에 라우팅 절차도 빈번하게 이루어진다. 제안한 방법은 이와 같이 라우팅이 시작되는 시점에 시작된다. 제안된 방법에 의하면 초기 노드가 분포된 상태에서 외부의 노드가 있다하더라도 일단 라우팅은 구현하지만 데이터의 전송은 이루어지지 않는다. 실질적인 데이터의 전송은 외부 노드 스캔모드가 종료된 이후에 이루어진다.

Ⅳ. 구현 및 고찰

제안한 방법의 효율성을 확인하기 위하여 실시한 실험환경은 다음과 같다.

- 허가된 센서 노드
  Node1(MAC) : F0-DE-F1-19-20-49
  Node2(MAC) : E3-03-22-19-A1-F2
  Node3(MAC) : 00-E1-30-A1-20-0F
- 비허가 센서 노드
  Node3(MAC) : 1C-12-55-A1-20-14
- PC 운영 환경 : 윈도우XP, 모니터링 : C#
- 라우팅 프로토콜 : TreeRouting

TreeRouting 프로토콜은 계층적 네트워크 토플러지 생성을 위한 프로토콜로서 주기적으로 주변에 자신의 존재를 알리고 이를 이용하여 상위부모노드를 선택하는 간단한 알고리즘의 라우팅 프로토콜이다[6].

제안한 개념을 구현하기 위하여 4개의 센서 노드를 사용하였다. 특정 하나를 BS로 설정하였으며 BS는 PC와 직렬연결을 통한 센서 네트워크 동작을 모니터링 하도록 하였으며, 나머지 노드는 일반 노드로서 사용하였다. 그림 3. 실제 구성한 실험환경이다.

그림 3 실험장치

메인 프로그램 수행에 앞서 먼저 사용될 센서 노드의 무선 통신 장치의 MAC 주소를 저장하고 등록되지 않은 센서 노드를 추가하여 라우팅을 시도하였다. 그림 4는 노드 모니터링을 통한 라우팅 참여여부를 나타내었다.

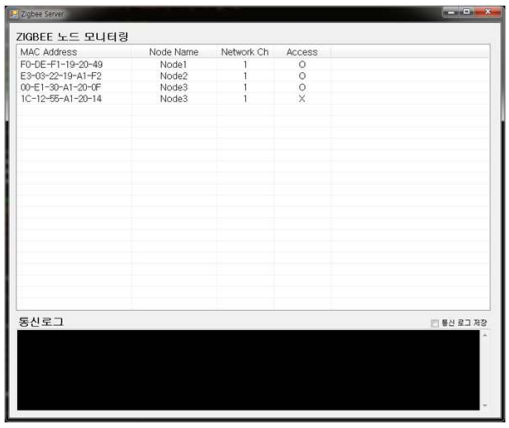

그림 4. 허가되지 않은 MAC에 대한 감지화면

그림에서 MAC address는 64bit에 16진수로 표시한 MAC 주소, Node Name은 MAC 주소에 해당하는 노드 논리적 ID 이름이며, Network Ch는 무선 통신에 사용되는 채널 번호를 표시한 것이다. MAC 주소 "1C-12-55-A1-20-14"는 등록되지 않은 주소이므로 Access 되지 않음을 나타내고 있으며 이 노드는 결과적으로 라우팅에 참여할 수 없으며 이를 모니터링 함에 따라 외부 노드의 접근을 감지하는 탐지 기능이 구현됨을 알 수 있다.

Ⅴ. 결론 및 향후 연구 방향

본 연구에서는 센서 네트워크를 구성하는 노드의 무선통신 장치가 갖는 MAC 주소의 고유성을 이용하여 허가 되지 않은 노드의 접근을 감지하여 네트워크에 참여를 배제하는 침입탐지 시스템

을 위한 방법을 제시하고 이를 구현하여 효용성을 확인하였다. 본 연구에서 제안한 방법은 단순히 MAC 주소만 사용하였지만 대량의 노드가 사용될 경우 브로드 캐스트 영역내에 주소의 중복을 100% 막을 수 없는 단점이 있다. 또한 운영 중간에 새로운 CHILD 노드가 접근할 경우 PARENT 노드 입장에서 새로운 노드의 MAC 주소를 BS로 보내고 또한 결과 값을 받기 위하여 여러 Hop을 거친 무선통신이 수행되어야 하므로 부가적인 에너지 소모가 발생된다.

향후에는 무선통신장치에서 사용하는 PANID를 이용하여 보다 실질적인 구분자로서 활용성을 검토할 것이며 이를 바탕으로 구분자를 암호화 키로 활용한다면 보다 나은 정보의 보안성을 높이데 기여할 수 있을 것이다.

참고문헌

[1] Zhijun Li, Guang Gong ,"Survey on Security in Wireless Sensor", Journal of KIISC, Vol. 18 No.6(B), Dec. 2008 p233-p248

[2] 김호원, 이석준, 오경희, “센서 네트워크 보안 기술 개발 동향”, 정보보호학회지 제 18권 제2호, 2008.4

[3] CC2420 datasheet, “CC2420, 2.4GHz IEEE 802.15.4 / ZigBee-ready RF Transciver", Chipcon

[4] Chris Karlof, Naveen Sastry, David Wagner, "TinySec : A Link Layer Security Architecture for wireless Sensor networks", Sensys 2004

[5] A.Perrig, R. Szewczyk, V. Wen, D. Culler, and J.D. Tygar, "SPINS: Security Protocols for Sensor Networks", Proc. of the 7th ACM/IEEE Int. Conf. on MobiCom, 2001

[6] (주)한백전자 기술연구소, “유니쿼터스 센서네트워크 시스템”, p.426-443, 2005