Zigbee 홈 네트워크에서의 DoS를 이용한 인증정보위조공격 탐지[1)]

전효진[1], 김동규[1], 임재성[1], 전상규[2], 양성현[2]

[1]아주대학교 정보통신전문대학원
[2]광운대학교 전기전자공학부

Denial of Service Attack Detection in Zigbee Home Network

Hyojin Jeon[1], Dongkyoo Kim[1], Jaesung Lim[1], Sangkyoo Jeon[2], and SungHyun Yang[2]

[1]Graduate School of Information and Communication Ajou University

[2]Department of Electrical Engineering, Kwangwoon University

요 약

Zigbee 홈 센서네트워크에서의 보안은 최근 떠오르는 중요한 문제 중 하나이다. 네트워크에 침입하거나 기능을 마비시키기 위해 여러 가지 공격방법들이 사용되고 있으며, 그 중 정상 노드로의 DoS(Denial of Service)공격은 네트워크에서 사용 중인 주파수를 알고 있다면 쉽게 수행될 수 있고 그 후 무력화된 노드의 인증정보를 이용해서 더 큰 문제를 발생시킬 수 있다. 본 논문에서는 zigbee 노드에 대한 DoS 공격과 인증정보위조 공격을 효율적으로 탐지해 낼 수 있는 방식을 제안한다.

I. 서론

현재 무선 센서네트워크 분야의 연구는 초기의 군사용 목적에서 벗어나 사용자의 편의를 위한 홈 네트워크에 초점이 맞춰지고 있다. Zigbee 프로토콜은 IEEE 802.15.4를 기반으로 하는 프로토콜로써 가정용 홈 네트워크처럼 규모가 작은 네트워크에 알맞게 초소형, 저 전력, 저 비용을 장점으로 내세우며 등장했다. 반경 30m 내에서 20~250kbps의 속도로 데이터를 전송하며 하나의 무선 네트워크에 최대 255대의 기기를 연결할 수 있다. 위에서 설명한 장점들로 인하여 홈 네트워크 등의 유비쿼터스 컴퓨팅을 위한 핵심 기술로 각광받고 있다.

Zigbee 프로토콜이 발전함에 따라 보안 분야에도 많은 발전이 있어왔지만 아직은 미약한 수준이다. 프로토콜 상의 많은 취약점이 발견되었으며, 이를 이용한 다양한 공격들이 예상되고 있다[2]. Zigbee 상에서 발생할 수 있는 위험한 공격 중의 하나가 서비스 거부공격을 이용한 인증정보위조(Authentication Spoofing) 공격이다. 인증정보위조 공격은 다른 노드의 ID와 key를 알아내어 그 노드인 것처럼 행동하는 것이며 이를 통해 네트워크에 잘못된 정보를 삽입할 수 있고, 이것을 통해 부당한 이득을 취할 수도 있다.

본 논문에서는 모니터링 노드를 이용한 서비스 거부 공격 탐지 기법과, 위장 노드에 대한 탐지 방법을 제공하는 실제 홈 네트워크 구성에 적용 가능한 시스템을 제안하고자 한다.

II. 관련 연구

1. WSN에서의 DoS공격

1) 본 연구는 산업자원부 및 한국산업기술평가원의 성장동력기술개발사업의 연구결과로 수행되었습니다.

지금까지 Wireless Sensor Network에서 발생할 수 있는 DoS공격에 대해서 많은 연구가 진행되어 왔다. DoS는 서비스 거부 공격으로서 공격 대상 노드나 네트워크가 정상적인 서비스를 할 수 없게끔 만드는 것을 의미한다. DoS는 하드웨어 오류, 소프트웨어 버그, 리소스 고갈, 노드 고립 혹은 이런 상황들이 복합적으로 발생할 때 일어난다. 본 논문에서는 네트워크 내부로의 침입여부와 상관없이 발생할 수 있는 Jamming, Flooding공격에 초점을 맞추고 있다.

Jamming[3]은 네트워크에서 사용하는 주파수를 충돌시켜 통신을 방해하는 공격이며, 공격 노드의 전송 범위 내의 모든 노드들을 무력화 시킬 수 있다. Jamming공격을 막기 위한 방법으로는 분산스펙트럼 통신을 사용하는 방법이 있는데 이 방법은 비용적인 문제로 상업적으로 사용하기 어렵다는 단점이 있어 Zigbee네트워크에 적용하기 힘들다.

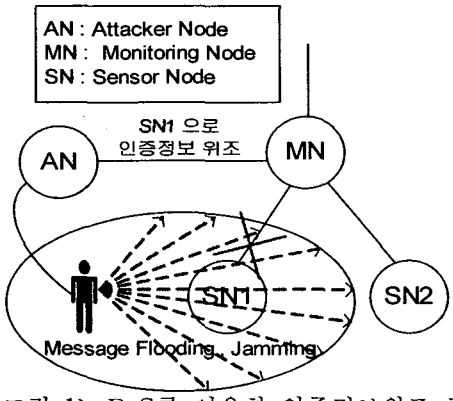
Flooding[3]은 공격 노드가 끊임없이 패킷을 전송함으로써 정상적인 노드들이 패킷을 전송할 기회를 뺏는 공격이다. 이를 막기 위한 방법으로써 Rate Limiting[3]이 있다. 이것은 네트워크에서 한 노드의 주파수 사용빈도가 일정 수준 이상으로 높아지면 해당 노드의 패킷전송을 허용하지 않는 방법이다. 하지만 Zigbee에서는 네트워크의 대역폭을 관리하는 노드가 없기에 Rate Limiting을 직접 적용시키기에는 무리가 따른다.

2. Zigbee 네트워크의 보안 취약점

Zigbee 네트워크에서는 새로운 노드가 참여할 때 안전한 통신을 위해 사용하는 네트워크 키를 PAN Coordinator로부터 전송받아야 한다. 하지만 Zigbee 스펙에 따르면 적당한 보안 메커니즘이 구현되어있지 않기에 네트워크 키는 평문 형태로 새로운 노드에게 전송되고 있다.[2] 공격 노드가 정상 노드인 것처럼 네트워크에 참여하거나 정상 노드가 네트워크에 참여할 때 감청을 하고 있다면 쉽게 키를 알아낼 수 있으며 이는 심각한 문제를 야기할 수 있다.[2]

III. 공격 모델

본 논문에서 초점을 맞추고 있는 Zigbee 네트워크에서 발생할 수 있는 공격모델은 <그림 1>과 같다.



<그림 1> DoS를 이용한 인증정보위조 공격

Zigbee 네트워크는 2장에서 설명한 것처럼 새로운 노드가 네트워크에 참여할 때 네트워크에서 공통적으로 사용하는 네트워크 키를 평문 형태로 전송하는 취약점을 가지고 있다. 이것을 이용하면 공격 노드는 가상의 노드를 네트워크에 등록시켜 네트워크에서 사용하고 있는 키와 공격대상 노드의 정보에 대해 알아낼 수 있다. 이 정보들을 알고 있을 경우 공격자는 자신의 노드를 정상노드로의 위장하는 것이 가능해 진다. 공격자는 접근 목표인 정상 노드A를 DoS공격으로 마비시키고, 공격자 자신의 노드를 노드A로 위장시킨다. 위장된 악의적 노드는 주위 다른 노드로부터 받거나 자신이 감지한 정보를 조작하여 거짓 정보를 PAN Coordinator에게 전송한다. PAN Coordinator는 거짓 정보로 인해 화재경보를 발생시키거나, 공격자로부터 물리적인 침입이 발생하였는데도 알지 못하게 되는 위험한 상황이 발생한다.

IV. 제안 기법

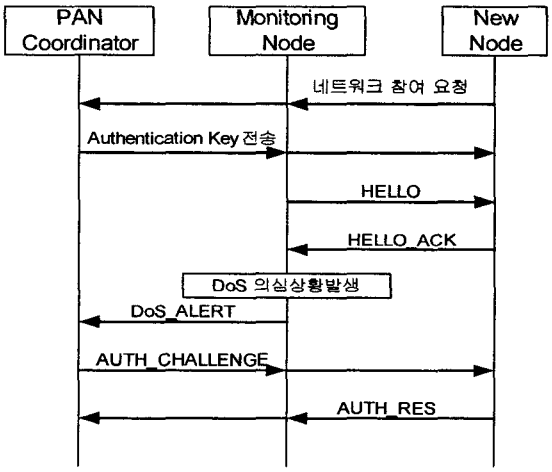
1. 필요한 가정

본 시스템을 위한 가정은 다음과 같다.

- PAN Coordinator는 공격받지 않아야 한다.
- 물리적인 노드의 획득은 불가능하다.
- 인증정보 위조 공격은 홈 네트워크 초기 구

성 시에는 발생하지 않는다.

- 새로운 노드는 네트워크 참가 시에 PAN Coordinator와 인증키를 서로 공유하며, 이 키는 각 노드마다 임의의 값을 이용해 서로 다르게 설정된다. 이것은 PAN Coordinator로부터 인증확인 메시지가 왔을 때에만 사용되고 홈 네트워크의 고정된 센서들은 초기에 네트워크가 생성된 후 전원에 문제가 생기지 않는다면 계속 연결을 유지하고 있는 특성을 지니고 있기에 다른 노드들과의 통신 중 도청으로 인해 유출되지 않는다.



< 그림 2 > 메시지 흐름도

2. DoS 공격 탐지

Zigbee 네트워크는 트리구조로 형성되어있으며 PAN Coordinator, 라우팅 노드, 센서 노드들로 이루어져 있다. 노드간의 라우팅은 트리 라우팅을 따른다. 본 시스템에서는 PAN Coordinator와 단말 센서 노드를 제외한 라우팅 노드들을 모니터링 노드로 지정한다.

네트워크의 전체적인 메시지 흐름은 <그림 2>와 같다. 모니터링 노드는 자신의 전송 범위 내의 트래픽을 살피고 주기적으로 트리 구조상의 자식노드에 해당하는 센서 노드들에게 주기적으로 HELLO 메시지를 전송한다. HELLO 메시지를 받은 자식 노드들은 의무적으로 HELLO_ACK 메시지를 전송해야하며 이를 바탕으로 노드의 상태를 파악 할 수 있다.

모니터링 노드는 HELLO_ACK 메시지를 받지 못한다면 DoS공격으로 의심하고 자신의 부모노드에게 DoS_ALERT 메시지를 보내고, 자신이 DoS공격을 받고 있다면 DoS_ALARM 메시지를 전송한다. 이 메시지들은 트리라우팅을 통해 PAN Coordinator 에게 전달되어야 한다.

DoS_ALERT	{Node ID}
DoS_ALARM	{Node ID}
AUTH_CHALLENGE	{Node ID, nonce}
AUTH_RES	{Node ID, $E_{\text{Authentication Key}}$ (nonce)}

<그림 3> 메시지 형식

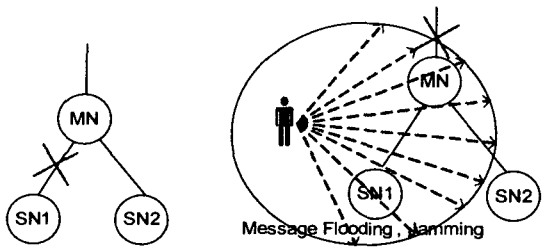
3. DoS, 인증 위조공격 대응방법

PAN Coordinator는 DoS_ALERT 메시지를 받으면 해당 노드에 대한 응답으로 nonce값을 생성하고 이 값을 AUTH_CHALLENGE 메시지에 담아 전송한다. 센서 노드는 AUTH_CHALLENGE를 받으면 즉시 사전에 공유한 인증키로 nonce값을 암호화하여 AUTH_RES를 만들어 PAN Coordinator에게 보내야 한다. 이것은 네트워크 자체의 문제로 해당 노드와 잠시 연결이 끊어진 상태와 DoS 공격으로 대상 노드를 무력화 시키고 공격 노드를 삽입하는 인증위조공격의 경우를 구분하고 인증위조공격으로 부터 네트워크를 보호하기 위함이다. 네트워크 문제로 인해 짧은 시간 동안 연결이 끊긴 경우라면 정상적으로 nonce를 암호화 해 보내기에 다시 통신을 재개할 수 있다. 그러나 해당 노드로부터 아무런 응답이 없거나 Authentication Key로 메시지를 복호화 했을 때 잘못된 nonce값이 나온다면 PAN Coordinator는 센서 노드에게 문제가 발생한 것으로 판단하고 모니터링 노드에게 LEAVE 메시지를 전송하여 해당 노드를 네트워크에서 격리시키거나 관리자에게 경보메시지를 보내 센서 노드의 물리적인 점검을 유도한다. 이와 달리 DoS_ALARM 메시지를 받는다면 확인 과정 없이 즉시 관리자에게 경보메시지를 보낸다.

V. 제안 기법 분석

이 장에서는 제안된 시스템이 여러 공격 상

황에 대응하는 방법을 분석한다.



(a) 센서 노드 단절 (b) 모니터링 노드로의 DoS

<그림 4> 발생 가능한 DoS상황

1. 네트워크 문제로 인한 센서노드의 단절

<그림 4>의 (a)와 같이 알 수 없는 문제로 인하여 센서노드가 네트워크로부터 단절된 상황이라면 모니터링 노드는 해당 센서노드에게 보낸 HELLO메시지에 대한 응답을 받을 수 없기에 문제가 발생했다는 것을 인지할 수 있다. 그 원인이 공격에 의한 것일 수도 있기에 모니터링 노드는 DoS_ALERT 메시지를 생성하여 보낸다. 이에 대한 대응으로 PAN Coordinator는 해당 노드에게 DoS_CHALLENGE 메시지를 보내는데 이에 대한 응답을 받을 수 없기에 해당 노드는 네트워크에서 제외된다.

2. 센서 노드로의 DoS공격과 인증정보위조

<그림 1>의 경우에는 공격 노드는 정상적인 센서 노드를 DoS공격으로 마비시키고 자신이 목표 노드인 것처럼 행동한다. 이때 모니터링 노드는 짧은 시간동안 HELLO메시지에 대한 응답을 받지 못하게 된다. 모니터링 노드가 DoS_ALERT메시지를 PAN_Coordinator에게 보내면 위장 노드는 PAN_Coordinator로부터 인증 메시지를 받게 되며, 위장 노드는 네트워크 키는 알고 있지만 Authentication Key를 알지 못하기에 nonce값을 알아낼 수 없고 올바른 응답 메시지를 보낼 수 없다. 이로 인해 인증정보 위조공격이 발생한 것을 알 수 있다.

3. 모니터링 노드로의 DoS공격

<그림 4>의 (b)처럼 공격 노드가 모니터링 노드에게 DoS공격을 한다면 HELLO 메시지를 보낼거나 응답을 받을 수 없다. 모니터링 노드는 자신이 CSMA의 Contention Access Period 동안 다른 메시지와의 충돌로 인해 어떠한 메시지도 받거나 보내지 못했다면, DoS상황으로 인식하고 부모노드에게 DoS_ALARM을 보낸다. 이 때 DoS공격으로 인해 정상적인 방법으로는 어떠한 전송할 수 없으므로 DoS_ALARM 메시지를 Beacon 프레임에 삽입하는 방법을 사용하면 PAN_Coordinator에게 전달될 수 있고 관리자는 공격이 발생하고 있음을 알게 된다.

VI. 결론

홈 네트워크에서 악의적인 노드의 네트워크 침입을 탐지하는 것은 중요한 사안중 하나이다. 더욱이 Zigbee 에서는 아직 보안에 대한 명확한 기준이 설립되어 있지 않고, 그와 관련된 연구도 초기단계이기 때문에 Zigbee를 기반으로 만들어진 홈 네트워크에서는 제한적인 보안 메커니즘을 제공할 수밖에 없다.

본 논문에서는 효과적으로 Zigbee 홈 네트워크에서 발생할 수 있는 DoS공격과 인증위조 공격을 탐지하는 시스템을 제시하여 보다 안전한 홈 네트워크를 보였으며, 현실적인 홈 네트워크 구현의 한 방법으로 고려해 볼 수 있을 것이다.

[참고문헌]

[1] Zigbee alliance. http://www.zigbee.org.

[2] Naveen Sastry, David Wagner, Security considerations for IEEE 802.15.4 networks, Proceedings of the 2004 ACM workshop on Wireless security

[3] Anthony D. Wood, John A. Stankovic, "Denial of Service in Sensor Networks," Computer, vol. 35, no. 10, pp. 54-62, Oct., 2002.

[4] ZigBee Security Layer Technical Overview, http://www.zigbee.org/en/events/documents/December2005_Open_House_Presentations/ZigBee_Security_Layer_Technical_Overview.pdf