한국산학기술학회논문지
Vol. 11, No. 3, pp. 984-990, 2010

USN환경에서 코디네이터 기반의 침입탐지시스템 설계

김황래[1*], 강연이[1]
[1]공주대학교 컴퓨터공학부

Design of a Coordinator-based Intrusion Detection System in Ubiquitous Sensor Network Environment

Hwang-Rae Kim[1*] and Yeon-i Kang[1]
[1]**Division of Computer Engineering, Kongju Nationanl University**

요 약 유비쿼터스 환경 구축을 위해 Zigbee 센서 네트워크 기술이 중요한 역할을 하고 있다. 그러나, Zigbee 기술은 근거리 내에서 환경정보 등을 센싱하여 정보를 전달하기 위한 간단한 작업을 목적으로 설계되었기 때문에, 다양한 공격기술에 의해 네트워크가 손상될 가능성이 매우 높다. 이러한 문제를 해결하기 위해 다양한 방어 기법들이 다수 논문에서 제시되고 있으나, 기존의 Zigbee 공격에 대한 다양한 대응방안들은 기능 구현시 센서노드의 중량화, 고비용화의 문제가 있으며, 이와 같은 문제를 해결하기 위해 Zigbee 네트워크상에서 컴퓨팅 파워가 우수한 코디네이터를 설치하고, 코디네이터을 기반으로 한 침입탐지시스템을 제안한다.
코디네이터 기반 침입탐지시스템은 Zigbee 네트워크의 공격을 탐지하고, 해결하는 새로운 방법을 제시하며, 다양한 분야에 응용이 가능하므로 Zigbee 기술을 실생활에 접목하는데 기여할 것으로 기대된다.

Abstract Zigbee sensor network technology to build a ubiquitous environment has an important role. However, Zigbee technology, sensing environmental information within the local area to deliver the information because it was designed for the purpose of simple tasks, Attack by a variety of technologies that could potentially compromise the network is very high. To solve this problems, many defense mechanisms are presented in a lot of papers. But, to attack the existing Zigbee various response measures for the implementation of the functionality of the sensor nodes very heavy and high expensive problem. To resolve this problems, with superior computing power Zigbee network coordinator to install, based coordinator to intrusion detection systems is proposed.
Coordinator-based IDS(Intrusion Detection System) of the Zigbee network is detected attack, and present a new approach to resolve, possible applications in various fields, so in real life Zigbee technology is expected to contribute to graft.

Key Words : Coordinator-Based IDS, USN, Zigbee, Intrusion Detection System

1. 서론

센서네트워크의 가장 대표적인 기술인 Zigbee 기술은 네트워크 기술 중에 가장 작은 대역폭(250kbps)을 제공하도록 설계된 근거리 내의 센서 노드들 간의 가장 저렴한 통신 기술 중의 하나이다. 설계 초기부터 최소한의 컴퓨팅 파워를 모토로 제시되었기 때문에, 특정 지역에 수천 개의 센서 노드를 배치함으로써 해당 지역을 제어할 수 있는 기술이라 할 수 있다.

Zigbee 기술은 응용분야도 매우 다양한데 최근에는 지능형 홈 네트워크에 대한 관심이 집중됨에 따라, 가정 내 기기들을 원격으로 제어하고 집안 환경을 모니터링하기 위해 홈오토메이션에 적용하기 위한 활발한 시도가 전개되고 있다[1,2].

본 논문은 2008년 공주대학교 학술연구지원사업의 연구비 지원에 의하여 연구되었음.
*교신저자 : 김황래(plusone@kongju.ac.kr)
접수일 09년 10월 16일 수정일 (1차 10년 02월 04일, 2차 10년 03월 02일) 게재확정일 10년 03월 18일

초경량으로 설계되었기 때문에 한정된 리소스를 보유한다는 점이 단점으로 작용하여 다양한 공격 기법들이 제기되고 있다. 이러한 공격기법들은 악의적인 목적으로 Zigbee 망에 적극적으로 개입하여 네트워크를 마비시키거나 더 나아가 인명 또는 재산상의 손실을 초래하는 공격까지 다양하다.

Zigbee 기술이 근거리 내에서 다양한 환경 정보 등을 센싱하여 전달하기 위한 간단한 작업을 목적으로 설계됨에 따라, 다양한 공격기술에 의해 네트워크가 손실될 가능성이 매우 높다.

이와 같은 문제를 해결하기 위해 다양한 방어 기법들이 국내외 연구자들에 의해 제안되고 있는데, 대부분의 기법들이 알고리즘의 복잡성과 과다한 계산 및 많은 자원을 요구하고 있어, Zigbee 본래 목적인 초경량화를 만족하기에 부족한 실정이다.

본 논문에서도 앞에서 제기된 문제점을 해결하기 위해 Zigbee 네트워크상에서 컴퓨팅 파워가 우수한 코디네이터 기반의 침입탐지시스템을 통해 해결 방안을 제안한다 [4,6,8,11].

본 논문의 구성은 다음과 같다.

2장은 코디네이터 기반의 침입 탐지에 대하여 기술한다.

3장은 제안한 코디네이터 기반의 침입 탐지 시스템 실험 및 성능 평가를 한다.

4장에서는 결론 및 향후 연구방향을 기술한다.

2. 코디네이터 기반의 침입 탐지

Zigbee 기반 홈오토메이션 환경에서 발생할 수 있는 공격시나리오 대해 설명하고, 이러한 공격을 방어하기 위해 코디네이터 기반의 침입탐지시스템의 구조, 데이터베이스, 각각의 공격에 대한 탐지 알고리즘에 대해 기술한다.

서비스 거부 공격 탐지방안는 센서노드에게 많은 양의 계산을 요구, 센서 장치의 고비용화와 많은 배터리 소모를 요구하게 된다. 따라서, 현재의 배터리 기술과 칩 비용 등으로 인해 현장에 적용하기에는 다소 무리가 따른다.

침입탐지 방법은 주요 공격 기술에 대한 침입패턴에 따른 규칙을 분석하여, 해당 규칙에 해당하면 공격으로 간주하는 오용탐지 방식을 채택한다.

침입탐지시스템은 Windows XP기반의 Home Gateway 상에서 웹2.0 환경에서 스크립트 언어인 AZAX로 설계하였고, 패킷 정보를 저장하는 데이터베이스는 My-SQL 기반으로 설계하였다.

2.1 코디네이터 기반 침입탐지시스템 구조

코디네이터 기반 침입탐지시스템은 크게 3가지 요소로 구성된다. 첫째로, 센서노드는 센서 네트워크의 가장 끝단의 정보센싱, 정보전달, Zigbee의 최소화된 기능을 수행한다. 집안 화재를 감시하기 위한 센서노드는 연기와 온도 관련 정보를 수집하는 역할을 수행한다.

둘째로, 코디네이터는 종단의 센서노드와 집안 전체의 보안을 담당하는 침입탐지시스템과의 중간 매개체 역할을 한다. Zigbee에서의 하위 센서노드를 관리하며, 침입탐지시스템으로부터의 의사결정에 따른 적절한 대응을 하위노드에게 실시한다.

셋째로, Zigbee의 침입탐지 기능을 수행하는 Home Gateway 등의 침입탐지시스템이 있다. 침입탐지 단말은 Zigbee 네트워크에서 사용되는 암호키 및 센싱되는 모든 데이터를 DB화하여 관리한다.

[그림 1] 코디네이터 기반 침입탐지시스템 구조

침입탐지는 사전에 분석된 규칙을 기반으로 동작하는 침입탐지 엔진이 주기적으로 전송되는 데이터를 분석하여 판단 및 적절한 대응을 실시하도록 했고, 코디네이터와 시리얼 인터페이스를 동일한 시스템에서 동작하도록 설계하였다.

2.2 코디네이터 관리 데이터베이스

Zigbee 네트워크에서 코디네이터는 다양한 정보를 유지 관리해야 한다. 네트워크에서 각 노드의 인증을 위한 Master Key와 송수신 데이터를 암호화하기 위한 암호화 Key 등의 정보를 유지해야 하고, 각 노드에 도달하기 위한 라우팅 테이블 등을 데이터베이스화하여 관리해야 한다.

본 논문에서는 모든 기기의 인증은 홈오토메이션을 위한 센서노드를 설치하기 전에 침입탐지시스템에 사전으로 등록된 디바이스만 정상적으로 네트워크에 참여하도록 설계하였다. 이는 가정이라는 특수성을 감안하여 한정된 지역내에서 댁내 거주자 또는 서비스 제공자가 특정 서비스 제공을 위해 센서노드의 배치를 사전에 설계가 가능하기 때문이다. 따라서, 새로운 센서노드가 네트워크에 참여하는지의 여부를 탐지하기 위해서 표 1과 같은 데

이터베이스를 관리할 필요가 있다.

[표 1] 인증 관련 데이터베이스

필 드	타입	설 명
노드 ID	Char	데이터를 송신 노드 ID
인증Key	Char	디바이스 인증관련 고유 Key String
용도	Int	온도 센싱, 보일러 제어, 연기탐지 등

이외에 공격자의 Zigbee 네트워크 침투를 감지하기 위해 모든 패킷에 대한 정보를 관리하고 있어야 한다. 이러한 정보는 탐지하고자 패턴에 따라 별도의 데이터베이스를 유지하여 효율성을 높일 수 있다.

[표 2] DoS 공격 탐지용 데이터베이스

필 드	타입	설 명
노드 ID	Char	데이터를 송신 노드 ID
도착시간	Int	해당 데이터가 도착한 시간
센싱 데이터	Int Char	해당 센서 노드가 전송하는 데이터(온도, 연기, On/Off 등)

본 논문에서 고려하고 있는 DoS(Denial of Service) 공격에 대한 침입 탐지를 위해서는 표 2와 같은 데이터베이스를 유지해야 한다.

위의 표 2는 정상적인 노드의 제어권을 획득하여 Zigbee 네트워크에 지속적인 데이터를 전송하는 DoS를 탐지하기 위해 필요한 데이터베이스이다. 이외에 또 다른 DoS 공격 중 하나인 특정 노드에 대한 재밍을 통한 DoS 공격이 있다. 이를 탐지하기 위해서 표 3과 같은 데이터베이스를 필요로 한다.

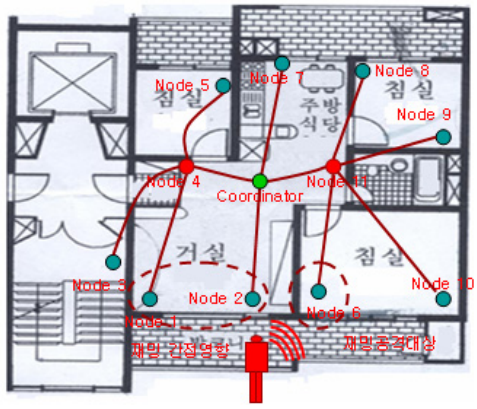
[표 3] 재밍공격 탐지 데이터베이스

필 드	타입	설 명
노드 ID	Char	데이터를 송신 노드 ID
Channel 1	Int	채널 1의 RSSI값
Channel 2	Int	채널 2의 RSSI값
…	Int	…
Channel 16	Int	채널 16의 RSS값

2.3 침입탐지 알고리즘

본 장에서는 Zigbee 네트워크에서 서비스 유지에 가장 치명적으로 작용할 수 있는 DoS 공격을 중심으로 하는 침입탐지 엔진을 제안한다.

재밍공격은 Zigbee와 동일한 주파수 대역에서 간섭신호를 계속 보내, 통신을 원하는 센서노드가 네트워크에서 사용중인 해당 채널을 할당받지 못하도록 하는 공격이다. 그림 2에서처럼 노드 1, 2번 사이에 있는 침입자가 네트워크에서 사용중인 채널을 모니터링하여 해당 채널로 무선 신호를 계속 발생시키면, Node 6은 주기적인 데이터 전송을 위한 채널을 할당받지 못하게 된다. 이러한 상태에 빠지게 되면, Node 6은 계속해서 채널 할당을 받기 위한 시도를 계속하게 되고, 결국 극심한 배터리 고갈 등으로 인해 네트워크에서 영구적으로 배제될 수 있다.



[그림 2] 재밍공격

이러한 재밍공격을 탐지하기 위해서는 네트워크에 참여중인 모든 노드가 약속된 주기별로 모든 채널의 RSSI(Received Signal Strength Indicator)값을 코디네이터에게 전송하고 코디네이터에서는 각 채널의 신호세기의 변화량과 임의 노드의 데이터 전송시 지연시간을 고려함으로써 가능하다. 모든 센서노드는 모든 채널의 RSSI 값을 주어진 간격으로 전송한다고 가정하자.

[표 4] 재밍공격후 데이터베이스

번호	노드 ID	채널 11	채널 12	---	채널 26
1	Node 1	53	47		40
2	Node 7	3	1		2
3	Node 4	2	4		1
4	Node 6	3	3		3
5	Node 2	76	56		50
6	Node 3	2	1		3
7	Node 8	4	2		3
8	Node 9	1	3		2
9	Node 11	3	1		3
10	Node 10	4	2		1

재밍 간접영향

* Node 6는 재밍의 직접 공격대상으로 전송 불가 RSSI 값 : 1~255

코디네이터에는 다음과 같은 정보가 데이터베이스에 저장될 것이다. 재밍공격 발생으로 인한 특징은 전체 노드 중, 일부 노드의 데이터 전송이 되지 않거나 채널 할당을 늦게 받아 지연이 되는 현상이 초래하며, 공격 받는 주변 노드의 RSSI값이 높아지는 현상이 나타난다. 표 4에서 1, 2번 노드의 RSSI값이 주변값보다 높아지는 현상이 나타나게 된다.

[표 5] 재밍공격시 패킷 지연 예

번호	노드 ID	도착시간	데이터(예 온도)
1	Node 1	20090905150015	26
2	Node 7	20090905150002	26
3	Node 4	20090905150004	24
4	Node 6	20090905150002	26
5	Node 2	20090905150025	25
6	Node 3	20090905150002	26
7	Node 8	20090905150003	24
8	Node 9	20090905150004	26
9	Node 11	20090905150002	25
10	Node 10	20090905150002	26

* 공격대상 노드의 주변노드인 1, 2는 15, 25초 정도의 지연 발생

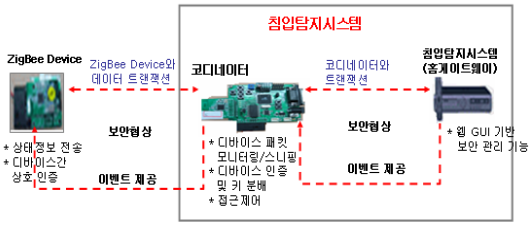
표 5은 재밍공격 발생시 패킷 전송시간이 지연되는 상황의 데이터베이스 내용을 보여 주고 있다. 이러한 상황에 의거하여, 아래와 같은 알고리즘을 통해 재밍공격을 탐지할 수 있다. 매 패킷별로 도착하는 RSSI값이 정해진 임계치를 넘어서고 지연시간이 정해진 시간을 넘어서면 재밍 카운트(J_C)를 증가시켜서 재밍 카운트 값이 임계치를 넘어서면 재밍공격으로 판단하는 것이다.

```
//도착한 패킷에서 현재 채널의 RSSI값을 추출
Packet_Rssi_ext()
{
    Rs=패킷;
    if(Rs >= Tr) then
      { J_C++;  // 도착한 패킷의 지연시간 계산
        if(지연시간 >= TI) then
          J_C++;
      }
     if(J_C >= Tj) then
       침입대응;
 }
```

3. 실험 및 성능평가

코디네이터 중심의 침입탐지시스템 상에서 DOS 공격을 실시하여 탐지가 이루어지는 시험한 결과에 대해 설명하고, 기존 프로토콜 기반의 공격탐지방안과 탐지기법과의 배터리 소모량 관점에서 성능을 평가한 결과를 기술한다.

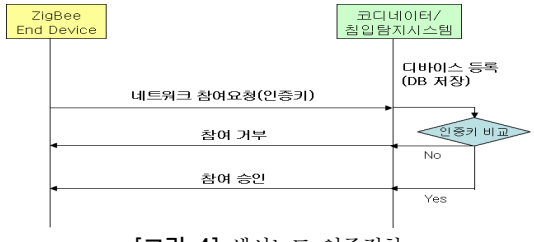
3.1 실험 환경



[그림 3] 침입탐지시스템 구성도

Zigbee 기반 침입탐지시스템의 성능을 평가하기 위해 댁내의 센싱 정보를 전송하는 Zigbee 디바이스와 악의적인 공격을 탐지하는 침입탐지시스템을 구현하였다. 침입탐지시스템은 윈도우 기반의 Home Gateway를 기반으로 구현되었으며, 전체 Zigbee 네트워크에 대한 침입 대응을 모두 처리하도록 하여 센서노드의 리소스를 최소화했으며, 보안 관련 프로세싱을 최소화되도록 설계하였다.

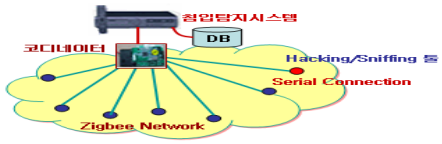
최초 네트워크 진입시 자신의 인증키값이 침입탐지시스템에 수동으로 저장되어야만 네트워크 참여가 가능하다. 새로운 노드가 네트워크에 참여하기 위해서는 먼저 댁내 홈오토메이션 관리자 또는 사용자에게 통보하여 인증키 값을 웹기반 UI상에서 입력하는 사전절차를 거쳐야 하며, 새로운 노드가 인증키를 포함한 네트워크 참여 요청을 하게 되면, 침입탐지시스템에서 사전에 저장된 디바이스 인증키 DB에서 키 정보 매칭여부를 검색하여, 사전에 인증된 노드일 경우에 네트워크 참여를 승인하게 된다.



[그림 4] 센서노드 인증절차

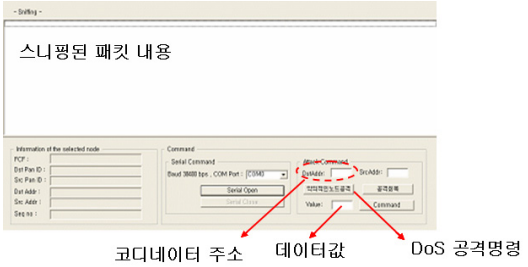
3.2 DoS 공격 실험 결과

DoS 공격을 테스트하기 위해 하나의 코디네이터와 10개의 센서노드로 구성된 네트워크 환경을 설계하였으며, 코디네이터는 침입탐지시스템이 구동되는 Home Gateway 상에서 동작하도록 설계하였다. 실제 댁내환경에서의 모습을 구축한 후, 악성정보를 지속적으로 발생시키기 위해 Zigbee 환경의 공격툴인 “Zigbee Hacking/Sniffing" 툴을 정상노드 중에 하나에 시리얼로 연결하여, 공격메시지를 지속적으로 전송하도록 하였다.



[그림 5] DoS 공격 탐지 실험 모델

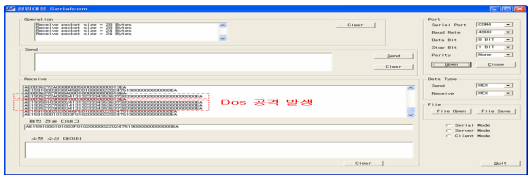
Zigbee 해킹툴의 UI로 Zigbee 네트워킹에서 돌아다니는 패킷들을 모니터링을 하는 패킷 스니핑 기능을 수행한다. Sniffing 부분은 패킷 데이터를 모니터링하는 것을 나타내며, Information of the selected node에서는 Zigbee Mac 데이터 포맷인 FCF, PAN ID, Dst Addr, Src Addr, Seq no. 등의 정보를 읽어 들일 수 있다.



[그림 6] 해킹/스니핑 툴 UI

Command부분에서는 시리얼 포트를 선택하는 부분으로 구성되어 있으며, 시리얼 포트와 Zigbee 노드가 연결되어 있다. 시리얼 포트를 통하여 Zigbee 노드들의 패킷 데이터들이 스니핑되며, “악의적인 노드 공격”을 통하여 DoS 공격을 실시한다. Dos 공격의 패턴은 MAC(Medium Access Control)계층에서의 CSMA/CA의 속성을 이용한 SIFS 간격 설정 변경을 통하여, 대량의 데이터를 연속적으로 보내는 형태를 하였다. DoS 공격을 통하여 정상적으로 동작하는 노드가 동작이 불가능한 상태로 들어가며, 이 상황에 악의적인 노드가 정상 노드인척 가장하고, 비정상적인 센싱 정보 등을 전송하게 된다.

그림 6의 해킹/스니핑 툴에서 DoS 공격 명령을 지속적으로 발생시키면, 코디네이터의 IDS의 일부인 관리자 모드 콘솔에는 그림 7과 같은 전송된 패킷정보가 화면상에 디스플레이 되며, 특정 시간에 특정 노드로부터 패킷이 지속적으로 송신되는 것을 볼 수 있다.



[그림 7] 코디네이터 관리자모드 콘솔

이와 동시에 IDS 내부의 침입탐지 엔진이 가동하게 되며, 탐지엔진에서는 정해진 주기보다 패킷 전송이 많기 때문에 DoS 공격이 발생한 것으로 판단하게 된다. DoS 공격으로 의사결정이 이루어지면, IDS 상에 메시지를 보여주어 사용자의 명령을 대기하게 된다. 이 환경에서 500회의 재밍공격을 시도한 결과 100%의 공격 탐지율을 보여 주었다.

3.3 성능 평가

본 논문에서 제시한 코디네이터 기반의 IDS 기법의 성능은 유사 기법들이 현재 존재하지 않기 때문에 직접적인 비교 평가가 어려운 실정이라서, 기존의 프로토콜 기반의 공격탐지 기법을 채택하여 Zigbee 노드의 배터리 사용량을 간접적으로 성능을 평가해 보았다.

각 센서노드의 배터리 사용량은 다음과 같이 계산할 수 있다.

$$\{\ \text{전류소모량} = Tx_{\text{소모량}} + Rx_{\text{소모량}} + MCU_{idle}\ \}$$

Tx소모량은 이웃 노드에게 패킷을 전송할 때 소비되는 배터리 양을 의미하며, 전송되는 패킷에는 정상적인 정보 전달을 위한 것과 공격노드를 탐지하기 위한 추가적인 패킷이 있을 수 있다. MCU소비량은 패킷을 송수신하고 송신 및 수신된 패킷을 기반으로 가공/처리에 소비되는 배터리 양을 의미한다.

배터리 소모량 분석을 위해 본 논문에서 구현한 노드와 유사한 플랫폼인 MicaZ 모트를 기반으로 한다. MicaZ 모트의 경우, 패킷을 전송할 시에 21.0㎃를 소비하며, 이 수치는 1시간동안 Tx를 동작시켰을 때에 소모되는 전류량이다. 따라서, 1초 동안 패킷을 전송하는 경우 소모되는 전류량은 $\frac{21.0}{3600} = 0.006$㎃이다. MicaZ의 경우 한 패킷의 크기는 39바이트이며, MicaZ 기반의 패킷 전송 실험을 통해 1초에 약 300패킷 정도가 전송되는 것을 확인하였다. 이는 MicaZ의 물리적인 속도가 250kbps이지만, 애플리케이션에서 네트워크, MAC 계층을 통과하는 데에 걸리는

시간으로 인해 93.6kbps 정도의 속도가 나오는 것이다. 따라서, 하나의 패킷을 전송하는 데에 걸리는 시간은 $\frac{1}{300}=0.003$초이며, 하나의 패킷을 전송하는 데에 소모되는 전류량은 $0.006\text{mA/초}\times 0.003\text{초}=0.000018\text{mA}$이다.

[9] 기법은 네트워크상의 각 노드들이 이웃노드들에게 주기적으로 임의 채널을 통해 메시지를 보내 응답하는지 여부에 따라 공격여부를 판단한다. 이 기법에서 각 노드에 연결되어 있는 평균 노드의 수를 m이라 하면, 각 노드는 추가적으로 m번의 패킷을 전송하게 된다. m번의 패킷을 전송하는 데 소모되는 전류량은 $0.000018\text{mA}\times m$ 만큼 필요로 한다. 이러한 탐지 패킷을 1시간에 b번 보낸다고 가정하면 1시간 동안 공격탐지를 위해 소모되는 전류량은 $0.000018\text{mA}\times m\times b$ 이다. 또한, 공격탐지를 하지 않는(코디네이터 기반 탐지) 경우에 소모되는 전류량(1시간에 a번 데이터를 송신한다고 가정하면)은 $0.000018\text{mA}\times a$이다.

데이터 수신(Rx)의 경우, Zigbee 노드는 Rx를 이웃노드로부터 패킷을 수신할 때만 잠시 껐다 켠다고 가정하면, 1패킷을 보낼 때 걸리는 시간동안 Rx를 켜는 것과 동일한 현상이 발생한다고 할 수 있다. 하지만, 일반적으로 데이터 수신을 위해서는 양 노드간의 싱크 과정이 필요하므로, 데이터 수신에 소요되는 시간은 0.004초로 가정한다. 따라서, Rx 소비량이 1시간에 23.3mA이며, 1초당 소모되는 전류량은 $\frac{23.3}{3600}=0.006\text{mA}$이다. 이러한 Rx를 매 패킷을 송신할 때마다, Tx할 때 걸리는 시간만큼만 켜 둔다고 가정하면, 1번의 패킷 전송에 대한 수신을 위해 $0.006\text{mA/초}\times 0.004\text{초}=0.000024\text{mA}$가 소모된다. 따라서, 공격탐지를 위해 소요되는 Rx 전류 소모량은 $0.000024\times b\times m\text{mA}$이며, 정상적인 네트워크 행위를 위해 소모되는 전류량은 $0.000024\times a\text{mA}$이다.

마지막으로 패킷 전송이 이루어지고 있지 않은 Idle 상태의 전류 소모량은 1초당 $\frac{0.027}{3600}=0.000007\text{mA}$이다. 또한, 1시간동안 Active인 시간은 Tx와 Rx 각각 공격탐지 기법을 적용할 경우에 $0.003\times m\times b$초, $0.004\times m\times b$초이며, 정상적인 통신이 이루어질 경우에 $0.003\times a$초이다. 따라서, 1시간동안 Idle 시간은 각각 $3600-0.003\times m\times b-0.004\times m\times b$, $3600-0.003\times a$초이며, Idle 시간동안 소모되는 전류량은 $(3600-0.003\times m\times b-0.004\times m\times b)\times 0.000007\text{mA}$, $(3600-0.003\times a)\times 0.000007\text{mA}$이다.

그러므로, 공격탐지 기법을 채택하지 않은 정상적인 네트워크에서의 전류 소모량(C1)과 DoS 공격탐지기법을 채택한 경우의 전류소모량(C2)은 다음과 같다.

$$C_1=(0.000042\times a)+((3600-0.003\times a)\times 0.000007))$$

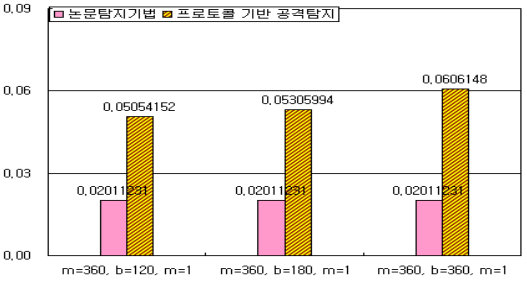
$$C_2=(0.000042\times m\times b)+((3600-0.003\times m\times b-0.004\times m\times b)\times 0.000007))$$

위 수식에 따라, 정상적인 네트워크 환경에서의 전송주기인 a와 공격탐지 기법에서의 전송주기인 b 및 평균 이웃노드의 수인 m의 값에 따라 1시간동안 소모되는 전류량은 표 6와 같다.

[표 6] 전류소모량 성능비교

조건	논문탐지기법	프로토콜기반 공격탐지	추가 소모율
a=360, b=120, m=1	0.02011231	0.05054152	74.9%
a=360, b=180, m=1	0.02011231	0.05305994	81.2%
a=360, b=360, m=1	0.02011231	0.06061480	99.9%

표에서 보는 바와 같이 정상적인 네트워크에서 매 10초마다 데이터 수집(a=360)을 하고, 공격탐지가 매 30초마다(b=120) 실행된다고 가정할 경우에 배터리는 74.9%가 추가적으로 소모된다. 하지만, 일반적으로 공격탐지는 정상적인 패킷이 발생할 때마다 수행되어야 즉시 대응이 가능하기 때문에 매 10초마다(b=360) 공격을 탐지할 경우에 배터리 소모량이 배로 발생한다는 것을 알 수 있다.



[그림 8] 이웃노드가 1일 경우 전류 소모량

그림 8은 프로토콜 기반 탐지기법과 논문탐지기법을 적용했을 때의 전류소모량과 추가 소모율을 비교한 것이며, 통상적으로 이웃노드의 공격여부를 판단하기 위해 검사패킷을 보낼 때, DoS 공격 등의 공격기술에 대해 하나의 패킷을 보내 검지가 가능하므로 DoS 공격탐지에서의 전류소모량을 프로토콜 기반 공격탐지 기법의 전류소모량과 동일하다 할 수 있다.

4. 결론

본 논문에서는 기존 USN 네트워크의 침입을 탐지하

고 적절한 대응을 위해 센서노드가 아닌 컴퓨팅 파워가 우수한 코디네이터에서 수행하도록 하는 방안에 대해 제시하고 설계하였다. 제안한 알고리즘은 DoS 공격을 탐지하는 방안을 포함하며, DoS 공격은 정해진 주기를 벗어나서 패킷을 보내는지의 여부에 따라 공격을 판단하여 탐지한다.

Zigbee 네트워크상에서 발생할 수 있는 침입패턴에 대한 분석을 기반으로 네트워크상의 모든 패킷을 분석함으로써 침입여부를 판단하고 공격노드를 네트워크에서 배제하는 등의 대응방안을 기술하였다.

성능 평가 결과, 본 논문에서 제안하는 코디네이터 기반의 공격탐지 기법을 탑재한 경우 보다, 이웃노드에 지속적으로 검사 패킷을 보내는 프로토콜 기반의 공격 탐지기법을 적용할 경우에 검사 패킷을 보내는 주기에 따라 최소 74.9%에서 99.9%까지 추가적으로 배터리를 소모하는 것을 알 수 있었다. 이는 Zigbee 노드에 프로토콜 기반 공격탐지 기법을 탑재할 경우에 배터리 운용 시간이 절반으로 줄어든다는 것을 의미하며, 결국 잦은 배터리 고갈로 인해 배터리를 자주 교체해야 하므로 유지보수 비용이 배로 발생한다는 것을 의미한다.

본 논문에서 제안한 코디네이터 침입탐지시스템을 사용해 침입에 적극 대응할 수 방안이 될 수 있고 향후에는 댁내 환경이 아닌 대규모 USN 네트워크가 형성될 것으로 예상되는 실외환경에 Zigbee 네트워크 응용이 보편화될 것으로 예측되며, 이러한 환경은 일반 가정보다 더욱 열악한 보안 환경을 보이게 될 것이다. 따라서, 이러한 개방 환경에서의 침입패턴 분석과 이를 바탕으로 하는 침입탐지시스템에 대한 연구가 필요할 것으로 판단된다.

참고문헌

[1] 이규호, 임재성, 김동규, 전상규, 양성현 “지그비 홈 네트워크에서의 다중신원(Multiple Identities) 노드 탐지”, 정보보호학회, 2006.

[2] William C. Craig, "Zigbee:Wireless Control That Simply Works", ZMD America, Inc.

[3] 김황래, "모바일 인터넷에서 이동성 패턴을 이용한 핸드오프 기법", 한국산학기술학회 논문지 Vol7. No.6, pp. 919-925. 2006.

[4] 김신효, 강유성, 정병호, u-센서 네트워크 보안 기술 동향, 전자통신동향분석 제20권 1호, 2005.

[5] John Paul Walters, Zhengqiang Liang, "Wireless Sensor Network: Survey", Security in Distributed Grid and Pervasive Computing, Auerbach Publications, 2006.

[6] 최재원, 이광휘, “A data Transfer Mechanism with Reliability in WSNs", 창원대학교 정보통신기초기술연구지원사업(B1220-0501-0128)

[7] 박종준, 이인환, 조현중, 주성순, 홍상기, 박상준, “Technical Trend of Sensor Node Middlewares”. 전자통신동향분석 제22권 제3호 2007.

[8] Qinghua Zhang, Pan Wang, Dougls S. Reeves, Peng Ning, "Defending against Sybil Attacks in Sensor Networks", Distributed Computing Systems 25th IEEE Conference, 2005, pp. 185-191.

[9] 전효진, 김동규, 임재성, 전상규, 양성현, “Zigbee 홈 네트워크에서의 DoS를 이용한 인증정보위조공격 탐지”, 정보보호학회, 2006.

[10] 김황래, 박진섭, "인터넷에서 정보시스템의 생존성 관리 모델", 한국산학기술학회 논문지 Vol7. No.6, pp. 1185-1193, 2006. 12.

[11] Bob Heile, "Wireless Sensors and Control Networks: Enabling New Opportunities with Zigbee, Zigbee Alliance, 2006.

김 황 래(Hwang-Rae Kim) **[정회원]**

- 1982년 9월 : 중앙대학교 전자계산학과 이학사
- 1991년 2월 : 중앙대학교 대학원 컴퓨터공학과 공학석사
- 2007년 9월 : 대전대학교 대학원 컴퓨터공학과 공학박사
- 1983년 3월 ~ 1994년 2월 : 한국전자통신연구원 선임연구원
- 1994년 3월 ~ 현재 : 공주대학교 컴퓨터공학부 교수

<관심분야>
컴퓨터네트워크, 네트워크보안, 네트워크생존성관리

강 연 이(Yeon-i Kang) **[정회원]**

- 2004년 8월 : 단국대학교 산업정보대학원 석사
- 2010년 현재 : 공주대학교 컴퓨터공학부 박사과정
- 2009년 9월 ~ 2010년 2월 : 단국대학교 강사
- 2008년 9월 ~ 현재 : 공주대학교 강사

<관심분야>
네트워크 보안, 임베디드 시스템, 네트워크 프로그램