논문 2011-1-7

ZigBee 공격노드 시뮬레이션 모델

기장근*

Simulation model for the attack node on ZigBee network

Jang-Geun Ki*

요 약

ZigBee는 저속 데이터 전송, 긴 수명, 저비용 구현 등이 요구되는 무선 응용을 목표로 제정된 프로토콜로, 무선랜 또는 블루투스와 같은 다른 무선 프로토콜들에 비해 구조가 간단하고 저비용으로 구현이 가능하여 최근 무선 제어 감시 응용 등에 널리 사용되고 있으며, 저전력 소모로 인해 적은 용량의 밧데리로도 오랜 시간 동안 동작할 수 있다. 그러나 이러한 간소함과 저비용의 반대급부로 ZigBee는 보안문제에 매우 취약하다. 예를 들어 ZigBee는 공격자가 단순히 이전에 기록된 패킷의 재전송을 수행하는 재연(replay) 공격에 대한 방어 기능이 미약하다.

본 논문에서는 이와 같은 취약한 ZigBee 망의 보안문제를 연구하기 위한 시뮬레이션 환경구축 일환으로 공격자의 시뮬레이션 노드 모델을 개발하였다. 개발된 공격노드 모델은 ZBdump, ZBreplay, ZBassocFlooding 등의 공격 기능을 가지도록 설계되었다. 또한 개발된 공격노드 모델을 사용하는 다양한 시뮬레이션 시나리오를 개발하고 실험함으로써 개발된 공격자 시뮬레이션 노드 모델이 정상 동작함을 검증하였고, 다양한 환경에서의 ZigBee 보안 문제 연구에도 유용함을 보였다.

Abstract

ZigBee is targeted at wireless applications that require a low data rate, long operation life, and low implementation cost. ZigBee protocol is simpler and less expensive than other wireless protocols such as WLAN and Bluetooth. The low cost allows the ZigBee technology to be widely deployed in wireless control and monitoring applications and the low power-usage allows longer life with smaller batteries. But advantages of simplicity and low cost in ZigBee cause security problems. For example, ZigBee offers no protection against replay attacks, in which an attacker simply resends recorded packets to the network.

In this paper, simulation node models of the attacker are developed for implementing environments of study on security of ZigBee networks. The developed node models have the attack functions such as ZBdump, ZBreplay, and ZBassocFlooding. In order to verify the developed models, we designed and constructed several simulation scenarios. The simulation results show that the developed simulation node models are useful for ZigBee security studies in various environments.

한글키워드 : ZigBee 무선망, 보안, 공격 시뮬레이션 모델

1. 서 론

최근 무선망 기술의 발전으로 WLAN,

* 공주대학교 전기전자제어공학부
(email: kjg@kongju.ac.kr)
접수일자: 2011.4.20 수정완료: 2011.5.16

www.kci.go.kr

Bluetooth, ZigBee 등과 같은 다양한 무선 프로토콜들이 개발되어 사용되고 있다. 이러한 무선 프로토콜들은 응용 목적에 따라 상대적인 장단점을 가진다.

ZigBee 프로토콜은 다양한 초저전력 센서를 활용한 무선 제어 망을 구축하는데 많이 활용되고 있다. 예를 들어 댐(dam)에서 물의 흐름을 제어하거나 천연가스 밸브를 제어하는데 사용되기도 하고, 최근 미국 라스베가스에 세워진 MGM CityCenter 빌딩에서와 같이 빌딩 자동제어를 위해 ZigBee 장치들을 사용하거나, 전기 검침기(electricity meters)간 통신을 위해 ZigBee 메쉬 망이 사용되어 지고 있다.

ZigBee 프로토콜의 관점에서 다른 프로토콜들을 비교해 보면, WLAN 프로토콜은 너무 복잡하고 송수신기(transceiver)의 가격이 상대적으로 비싸며, FHSS 방식을 사용하는 Bluetooth는 상대적인 전력소모가 크고 역시 너무 복잡하다. 이에 반해 ZigBee 프로토콜은 초저전력 소비와 저속 데이터 전송이 요구되는 환경에 적합하고 저비용으로 구현이 가능하며, 임베디드 기술의 활용이 매우 용이하다. 그러나 ZigBee의 간소함과 저비용의 반대급부로 발생하는 보안 문제에는 매우 취약한 실정이다. 실제로 많은 ZigBee 벤더 및 사용자들이 ZigBee 자체의 활용에는 많은 관심을 보여주고 있지만 상대적으로 취약한 보안 문제는 단순히 저비용의 한계로 치부하는 경향을 보인다. 그러나 응용에 따라서는 상대적으로 매우 저렴한 센서와 같은 단말노드로 구성된 ZigBee 망일지라도 악의적인 공격에 의해 전체 시스템이 마비되는 매우 중대한 결과를 초래하는 경우가 발생할 가능성이 얼마든지 있다.

따라서 본 연구에서는 시뮬레이션을 통한 ZigBee 망 보안 문제 연구의 일환으로 먼저 ZigBee 망 공격용 시뮬레이션 모델을 개발하였다. 시뮬레이션 환경으로는 OPNET이 사용되었으며, 개발된 모델은 일반적인 무선망에서의 공격 툴 기능과 유사한 송수신 패킷 캡처 기능(promiscuous 모드), Assoiciation Flooding 공격 기능, 재연(replay) 공격 기능 등을 갖는다. 개발된 ZigBee망 공격 시뮬레이션 모델을 사용하여 보안관련 연구를 수행할 경우 실제 구현을 통한 연구에 비해 경제적, 시간적 절감 효과를 도모할 수 있다.

본 논문의 구성을 살펴보면 1장의 서론에 이어 2장에서 ZigBee 프로토콜 규격에 관해 기술하였고, 3장에서 개발된 ZigBee 공격용 시뮬레이션 모델에 관해 기술하였다. 4장에서는 개발된 모델의 적용 시나리오 및 시뮬레이션 결과를 나타냈었고, 5장에서 결론을 제시하였다.

2. ZigBee 프로토콜

ZigBee 프로토콜은 저전력 소비와 저속 데이터의 무선 전송이 요구되는 응용 영역에 사용될 목적으로 규정되었으며, 최대 전송속도는 250Kbps이고, 스타(star) 또는 메쉬(mesh) 망 토폴로지를 지원하며, 망 커버리지는 약 10-100미터 정도이다. 표 1에 ZigBee의 대표적인 파라미터 값을 나타내었다. ZigBee 표준은 2004년에 제정된 이후 2006-2007년에 보안관련 기능이 추가 개정되었다.

ZigBee 망의 구성요소는 크게 코디네이터(coordinator), 라우터(router), 단말노드(end device)로 분류된다. 코디네이터는 망에 하나만 존재하며, 라우터는 코디네이터와 함께 라우팅 기능을 사용하고 일반적으로 상시전원을 사용한다. 단말노드는 라우팅에 참여하지 않으며 주로 밧데리 전원을 사용하고 sleep 모드를 지원하며 하나의 라우터(또는 코디네이터)와만 연결을 설정한다.

www.kci.go.kr

표 1. ZigBee 파라미터

Wireless Parameter	ZigBee
Frequency band	2.4 GHz
Physical/MAC layers	IEEE 802.15.4
Range	Indoors: up to 30 m Outdoors (line of sight): up to 100 m
Current consumption	25-35 mA (Tx mode) 3 μA (Standby mode)
Raw data rate	250 Kbps
Protocol stack size	32 KB 4 KB (for limited function end devices)
Typical network join time	30 ms typically
Interference avoidance method	DSSS (direct-sequence spread spectrum)
Minimum quiet bandwidth required	3 MHz (static)
Nodes per network	64 K
Number of channels	16

ZigBee에서는 16비트와 64비트 길이의 2가지 주소가 사용된다. 16비트 주소(망 주소)는 망에 합류(join)할 때 코디네이터나 라우터로부터 할당 받는 주소로 ZigBee 프로토콜의 망(network) 계층에서 사용되며, 코디네이터의 망주소는 0으로 지정되어 있다. 64비트 확장주소(IEEE EUI-64 주소)는 노드의 각 RF 모듈마다 가지는 고유주소이다. ZigBee 망계층에서는 16비트 주소를 이용해 라우팅이 행해지며, 만일 16비트 주소를 모르면 64비트 확장주소를 이용해 16비트 주소를 알아내고(ARP 프로토콜 개념과 같이) 이를 사용한다.

그림 1에는 ZigBee 주소할당 및 트리 라우팅 알고리즘을 나타내었다.

트리 라우팅 알고리즘에서 깊이(depth) d에 위치하는 노드의 자식 주소풀(address pool)의 크기는 아래 식으로 계산된다.

$$C_{skip}(d) = \begin{cases} 1 + Cm \cdot (Lm - d - 1), & \text{if } Rm = 1 \\ \dfrac{1 - Rm + Cm - Cm \cdot Rm^{\,Lm-d-1}}{1 - Rm}, & otherwise \end{cases}$$

Cm = 라우터의 최대 자식 단말노드수
Rm = 라우터의 최대 자식 라우터수
Lm = 망의 전체깊이($depth$)

총 노드수는 아래 식으로 계산되며, 참고로 그림 1의 경우 총라우터수 = $1+4+4^2+4^3+\cdots\cdots$ (등비수열) 이며, 초항=a, 등비=r인 등비수열의 합은 $a(1-r^n)/(1-r)$로 계산된다.

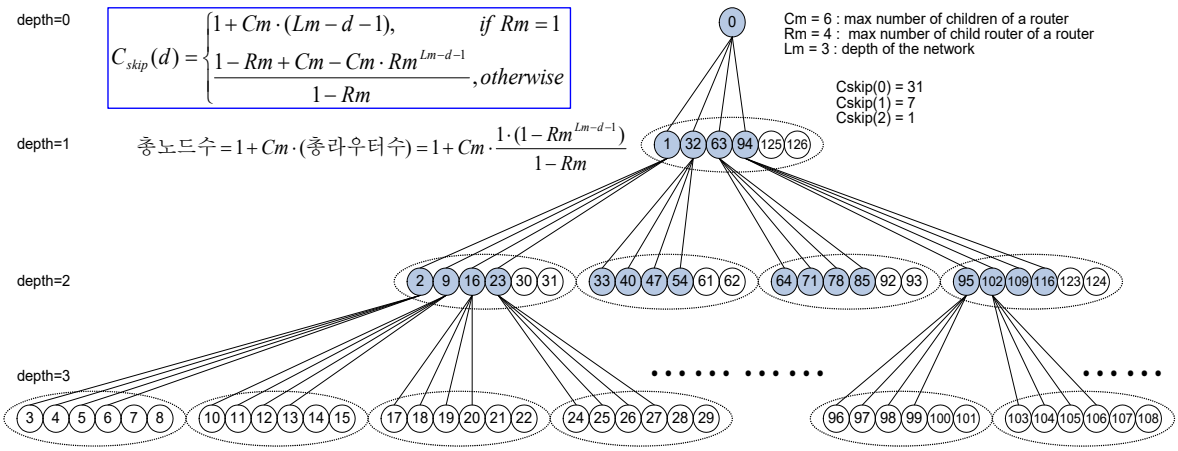

그림 1. ZigBee 주소할당 및 트리 라우팅 알고리즘

www.kci.go.kr

$$\text{총노드수} = 1 + Cm \cdot (\text{총라우터수}) = 1 + Cm \cdot \frac{1 \cdot (1 - Rm^{\,Lm-d-1})}{1 - Rm}$$

만일 깊이 d에 있는 부모노드가 주소 A_{parent}를 가진다면 n번째 자식 라우터의 주소는 $A_{parent} + (n-1) \times C_{skip}(d) + 1$이 되고, n번째 자식 단말노드 주소는 $A_{parent} + Rm \times C_{skip}(d) + n$이 된다.

트리 라우팅 알고리즘에서 목적지 D가 $A < D < A + C_{skip}(d-1)$를 만족하면 라우터 A의 후손(descenent)이 되며, 다음 홉(next hop) 주소는 아래 식에 의해 계산된다.

$$A + 1 + \left\lfloor \frac{D - (A+1)}{C_{skip}(d)} \right\rfloor \times C_{skip}(d)$$

목적지 D가 라우터 A의 후손이 아닌 경우 메시지는 A의 부모를 통해 라우팅 된다.

3. ZigBee 공격 시뮬레이션 모델

ZigBee 보안에 관한 연구를 시뮬레이션을 통해 수행하기 위해 본 연구에서는 OPNET 소프트웨어를 사용하였다.

본 논문에서 개발된 ZigBee 공격용 시뮬레이션 노드 모델의 구조(좌측 그림) 및 ZBattacker 모듈의 프로세스 모델(우측 그림)은 그림 2와 같다.

그림 2의 좌측에 나타낸 노드모델에서 802_15_4_mac 모듈은 정상적인 ZigBee 노드로 동작하기 위해 network_layer 모듈과 wireless_tx/rx 모듈사이에 송수신되는 패킷을 전달하면서 ZigBee MAC(Media Access Control) 기능을 수행할 뿐만 아니라, ZigBee 공격노드로 동작하기 위해 wireless_rx 모듈로 부터 수신되는 모든 패킷을 복사하여 ZBattackter 모듈로 전달하고, ZBattacker 모듈로 부터 전달받은 공격용 패킷을 wireless_tx 모듈로 전달하는 역할을 수행한다.

노드모델에서 ZBattacker 모듈은 사용자 설정 속성 값에 따라 ZBdump, ZBassocFlood, ZBdump 등의 공격 기능을 수행하며, 필요에 따라 공격용 패킷을 생성해 802_15_4_mac 모듈로 보낸다. ZBattacker 모듈의 프로세스 모델은 그림 2의 우측에 나타내었다.

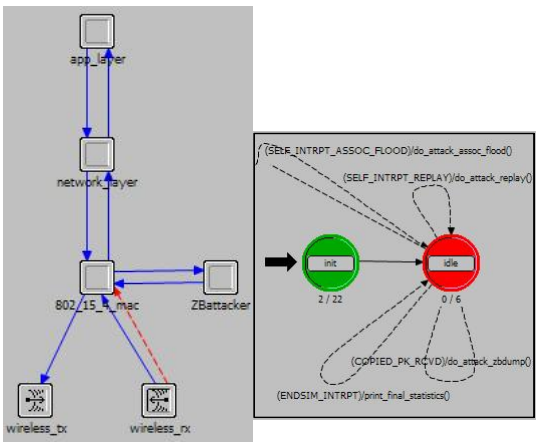

그림 2. ZigBee 공격용 시뮬레이션 노드 모델 구조 및 프로세스 모델

ZBdump 기능은 일반 인터넷 망에서의 tcpdump 또는 libpcap 기능과 유사하게 망에서 송수신되는 모든(또는 원하는) ZigBee 패킷들을 캡쳐(capture)하여 저장하는 기능을 수행하며, 저장된 패킷 정보는 다른 공격을 위한 기초자료로 활용될 수 있다.

ZBassocFlood 기능은 가상노드에 대한 Association Request 메시지를 코디네이터에 대량으로 보냄으로써 코디네이터가 다른 실제 단말노드의 합류를 더이상 받아들이지 않도록 방해하는 공격 기능을 수행한다.

ZBreplay는 이미 캡쳐된 패킷 정보를 이용한 재연(replay) 공격 기능을 수행한다. 일반적으로 재연 공격에 따른 영향은 트래픽의 성격, 즉 응

www.kci.go.kr

용에 따라 달라진다. 본 연구에서 수행되는 replay 공격은 응용에 대한 사전지식을 요하지 않도록 하기 위해 단순한 replay 공격만을 수행하도록 설계되었다.

4. 시뮬레이션 결과 및 분석

본 논문에서 설계, 개발된 ZigBee 공격 시뮬레이션 모델의 유용성을 검증하기 위하여 다양한 시나리오에 대한 시뮬레이션을 수행하였다.

그림 3은 Association Flooding 공격 시뮬레이션을 위한 OPNET 네트워크 모델 예이다. 그림의 위쪽에 위치한 직비망(ZigBee Network) 1은 코디네이터 Coord1과 2개의 단말노드 ZBdev1, ZBdev2로 구성되어 있으며, 코디네이터 Coord1의 최대 허용 단말노드 수는 10으로 설정하였고 시뮬레이션 초기에 2개의 단말노드 ZBdev1, ZBdev2가 코디네이터 Coord1이 구성한 ZigBee 망에 합류하도록 구성되었다. 코디네이터 Coord2에 속한 Attacker 노드는 시뮬레이션 시작시간 0초부터 100초 사이에 코디네이터 Coord1쪽으로 이동한 후, 100초부터 매 10초마다 한번씩 association request 메시지를 코디네이터 Coord1에게 보내도록 설정하였다. 이와 같은 시나리오에 대한 시뮬레이션 결과를 그림 4에 나타내었다. 그림 4는 Attacker 노드의 association flooding 공격에 따른 코디네이터 Coord1의 허용 단말노드 수 변화를 보여주고 있다. 그림에서 알 수 있드시 시뮬레이션 초기에 2개의 단말노드가 망에 합류함으로써 코디네이터 Coord1의 허용 단말노드 수가 10에서 8로 줄어듬을 볼 수 있으며, Attacker 노드가 코디네이터에 접근하여 association flooding 공격을 수행하는 시간 100초 부터 매 10초마다 코디네이터의 허용 단말 수는 하나씩 줄어들어 결국 0이 됨을 볼 수 있다.

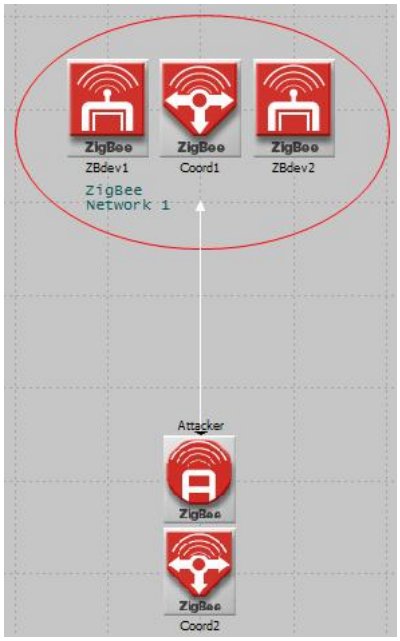

그림 3. Association Flood 공격 시나리오에 대한 네트워크 모델

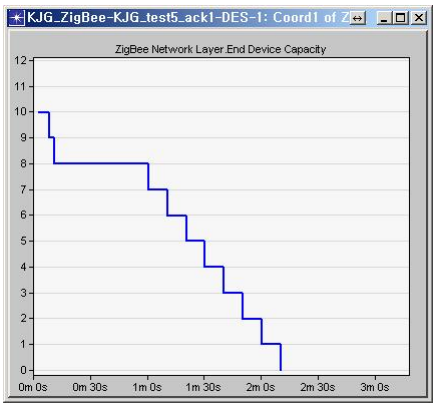

그림 4. Association Flood 공격에 따른 코디네이터의 허용 단말노드 수 변화

그림 5는 ZBdump와 Replay 공격 시뮬레이션을 위한 OPNET 네트워크 모델 예이다. 그림에서 2개의 단말노드 ZBdev1, ZBdev2는 코디네이터 Coord1에게 시뮬레이션 시간 20초부터 90초까지 초당 1패킷을 각각 송신하도록 설정되었다. Attacker 노드는 ZBdump 기능을 이용해 송수신

www.kci.go.kr

되는 패킷을 캡쳐해 저장한 후, Replay 공격을 이용해 시뮬레이션 시간 60초부터 90초 사이에 저장된 데이터 패킷을 시뮬레이션 시간 120초부터 송신함으로써 Replay 공격을 수행하도록 설정하였다.

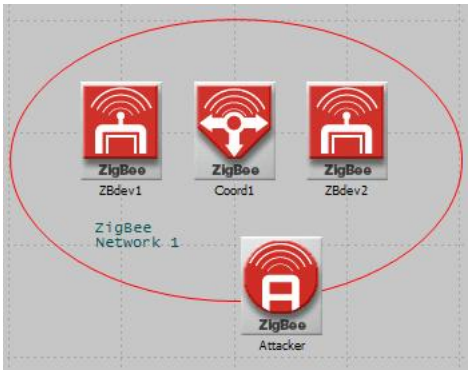

그림 5. ZBdump / Replay 공격 시나리오에 대한 네트워크 모델

그림 6에는 시간 변화에 따른 코디네이터의 초당 수신 패킷 수와 단말노드 ZBdev1, ZBdev2의 초당 송신 패킷 수를 나타내었다. 그림에서 확인할 수 있듯이 시간 20초부터 90초 사이에는 코디네이터가 ZBdev1, ZBdev2가 보내는 데이터 패킷을 수신함을 볼 수 있고, 120초부터 150초 사이에는 ZBdev1, ZBdev2가 데이터를 송신하지 않음에도 초당 2패킷을 수신함을 볼 수 있는데 이는 Attacker가 Replay 공격으로 송신한 데이터 패킷을 수신함을 의미한다.

5. 결 론

최근 무선망 기술의 발전으로 WLAN, Bluetooth, ZigBee 등과 같은 다양한 무선 프로토콜들이 개발되어 사용되고 있다. 이러한 무선 프로토콜들은 응용 목적에 따라 상대적인 장단점을 가진다.

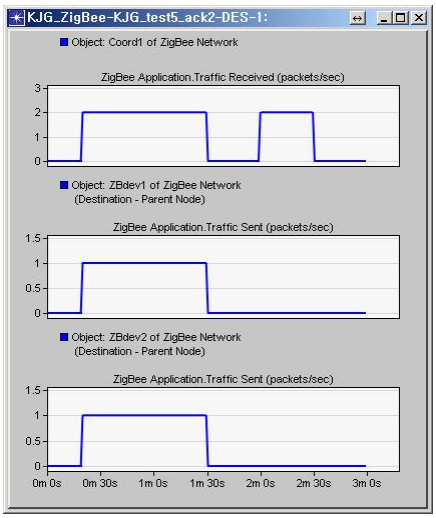

그림 6. Replay 공격에 따른 코디네이터 수신 데이터 및 단말노드 송신 데이터 변화

ZigBee 프로토콜은 저속 데이터 전송, 저전력 소비, 저비용 구현 등이 요구되는 무선망 구축에 많이 사용되고 있다. 그러나 이러한 ZigBee의 간소함과 저비용 장점의 반대급부로 발생하는 보안 문제는 매우 취약한 실정이다. 실제로 많은 ZigBee 벤더 및 사용자들이 ZigBee 자체의 활용에는 많은 관심을 가지고 있지만 상대적으로 취약한 보안 문제는 단순히 저비용의 한계로 취급해 버리는 경향을 가지고 있다. 그러나 응용에 따라서는 상대적으로 매우 저렴한 센서와 같은 단말노드로 구성된 ZigBee 망일지라도 악의적인 공격에 의해 전체 시스템이 마비되는 매우 중대한 결과를 초래하는 경우가 발생할 가능성이 얼마든지 있다.

본 논문에서는 ZigBee의 취약한 보안 문제를 시뮬레이션을 통해 연구할 수 있는 환경 구축을 위해 ZigBee 망 공격용 시뮬레이션 노드 모델을 개발하였다. 시뮬레이션 환경으로는 OPNET이 사용되었으며, 개발된 공격 노드 모델은 일반적인 무선망에서의 공격 툴 기능과 유사한 송수신 패킷 캡쳐 기능(promiscuous 모드), Assoiciation

www.kci.go.kr

Flooding 공격 기능, 재연(replay) 공격 기능 등을 가지도록 설계되었다.

개발된 공격 노드 모델의 유용성을 검증하기 위해 다양한 시나리오를 개발하고 이에 따른 시뮬레이션을 수행하여 공격 노드 모델의 정상 동작 여부를 확인하였다.

개발된 ZigBee망 공격 시뮬레이션 모델을 사용하여 보안관련 연구를 수행할 경우 실제 구현을 통한 연구에 비해 경제적, 시간적 절감 효과를 도모할 수 있을것으로 기대된다.

참 고 문 헌

[1] ZigBee Specification 2007, http://www.zigbee.org/
[2] IEEE Std 802.15.4-2006, Wireless MAC and PHY Spec. for WPANs
[3] OPNET, http://www.opnet.com, 2011
[4] Joshua Wright, "KillerBee: Practical ZigBee Exploitation Framework", http://www.willhackforsushi.com/presentations/toorcon11-wright.pdf

저 자 소 개

기장근 (奇長根)

1986.2 고려대학교 전자공학과졸업
1988.2 고려대학교 전자공학과 석사
1992.2 고려대학교 전자공학과 박사
2002.6-2003.6 Univ. of Arizona 방문교수
2010.6-2011.8 Univ. of Arizona 방문교수
1992.3-현재 : 공주대학교 공과대학 전기전자제어공학부 교수

<주관심분야>통신프로토콜,이동통신시스템

www.kci.go.kr