DOI: 10.3745/KIPSTC.2010.17C.1.1

IEEE 802.15.4기반 센서 네트워크에서 슬립거부 공격의 취약성 분석 및 탐지 메커니즘

김 아 름[†] · 김 미 희[††] · 채 기 준[†††]

요 약

IEEE 802.15.4 표준기술[1]은 센서 네트워크에서 저전력을 위한 기술로 LR-WPANs(Low Rate-Wireless Personal Area Networks)의 물리계층과 MAC계층을 규정한다. 이 표준은 무선 센서, 가상 선(Virtual Wire)과 같은 제한된 출력과 성능으로 간단한 단거리 무선 통신을 필요로 하는 폭넓은 응용에 활용되고 있지만 보안 측면의 연구는 현재 미비한 상태로 다양한 공격에 대한 취약점을 내포하고 있다. 본 논문에서는 802.15.4 MAC계층의 슬립거부(Denial of Sleep) 공격에 대한 취약성을 분석하고 이를 탐지하는 메커니즘을 제안한다. 분석 결과, 슈퍼프레임 구간 변경, CW(Contention Window)값 변경, 채널스캔 및 PAN 연합과정 등에서 슬립거부 공격의 가능성을 분석할 수 있었고, 이 과정 중 일부에서는 표준에서 정의한 인증과 암호화 기능이 적용되어도 공격 가능함을 알 수 있었다. 또한 본 논문에서는 분석된 취약점 중에 채널스캔 및 PAN 연합과정에서 Beacon/Association Request 메시지 위조를 통한 슬립거부 공격의 탐지 메커니즘을 제안한다. 제안된 메커니즘은 메시지 요청 간격, 요청 노드 ID, 신호 세기 등을 모니터링하여 공격을 식별하여 탐지한다. QualNet 시뮬레이션 툴을 사용하여 공격의 영향 및 제안된 탐지 메커니즘의 탐지 가능성과 성능의 우수성을 입증할 수 있었다.

키워드 : 센서 네트워크, IEEE 802.15.4, 슬립거부 공격, 탐지

Vulnerability Analysis and Detection Mechanism against Denial of Sleep Attacks in Sensor Network based on IEEE 802.15.4

Areum Kim[†] · Mihui Kim[††] · Kijoon Chae[†††]

ABSTRACT

IEEE 802.15.4[1] has been standardized for the physical layer and MAC layer of LR-PANs(Low Rate-Wireless Personal Area Networks) as a technology for operations with low power on sensor networks. The standardization is applied to the variety of applications in the shortrange wireless communication with limited output and performance, for example wireless sensor or virtual wire, but it includes vulnerabilities for various attacks because of the lack of security researches. In this paper, we analyze the vulnerabilities against the denial of sleep attacks on the MAC layer of IEEE 802.15.4, and propose a detection mechanism against it. In results, we analyzed the possibilities of denial of sleep attacks by the modification of superframe, the modification of CW(Contention Window), the process of channel scan or PAN association, and so on. Moreover, we comprehended that some of these attacks can mount even though the standardized security services such as encryption or authentication are performed. In addition to, we model for denial of sleep attacks by Beacon/Association Request messages, and propose a detection mechanism against them. This detection mechanism utilizes the management table consisting of the interval and node ID of request messages, and signal strength. In simulation results, we can show the effect of attacks, the detection possibility and performance superiorities of proposed mechanism.

Keywords : Sensor Network, IEEE 802.15.4, Denial of Sleep Attack, Detecion

1. 서 론

현재 사회는 사용자가 네트워크나 컴퓨터를 시, 공간에 구애받지 않고 자유롭게 사용할 수 있는 환경인 유비쿼터스 시대가 도래 하면서 기반기술로서 센서 네트워킹 기술의 중요성이 강조되고 있다. 센서 네트워크는 유무선 네트워크 인프라에 소형의 다양한 센서 노드를 설치하고 이를 통해서

※ 이 논문은 2008년도 정부(교육과학기술부)의 재원으로 한국과학재단의 지원을 받아 수행된 연구임(NO.R01-2008-000-20062-0).
† 정 회 원 : 이화여자대학교 컴퓨터공학과 석사
†† 정 회 원 : 미국 North Carolina State University Postdoc Researcher
††† 종신회원 : 이화여자대학교 컴퓨터공학과 교수
논문접수 : 2009년 8월 28일
수 정 일 : 1차 2009년 11월 10일
심사완료 : 2009년 11월 10일

주변 환경에 대한 다양한 정보를 수집하여 이를 분석하는 역할을 수행한다. 현재 군사, 의료, 차량 등 다양한 응용분야에서 활용되고 있으며 이에 대한 연구도 활발히 진행 중에 있다. 이와 같은 센서 네트워크 기술 연구에 있어서 기반 기술 연구와 함께 센서를 통해 수집된 정보를 안전하게 처리하고 관리할 수 있는 센서 네트워크의 보안 메커니즘이 연구되어 적용되어야 한다.

센서 네트워크는 고유한 특성으로 보다 많은 공격에 대한 취약점들이 존재하여 보안에 취약하다는 문제점을 갖는다. 이러한 센서 네트워크 보안기술은 키 관리 연구[2, 3]나 인증 메커니즘[4]에 대한 연구가 주를 이루었다. 그러나 일반 네트워크와 달리 센서 네트워크에서의 센서 노드는 쉽게 포획이 가능하고 암호화를 사용하는 인증 메커니즘도 노드의 메모리, 배터리 한계 등의 제약이 있기 때문에 완벽한 암호화 기술이나 키 관리 메커니즘을 구현하기 어렵다. 이를 악용하여 공격자들은 손쉬운 서비스거부 공격을 통해서 간단하게 센서 네트워크를 공격하여 기능을 무력하게 만들 수 있다. 따라서 센서 네트워크의 보안을 보장하기 위해서 이러한 서비스거부 공격처럼 간단하지만 강력한 공격에 대한 안전한 메커니즘이 개발되어야 한다. 이를 위해서는 우선 센서 네트워크상에서 존재하는 공격의 특징을 분석해 보고 이에 대한 대응방법에 대한 연구가 필요하다.

본 논문에서는 저 가격, 낮은 전송속도, 그리고 긴 배터리 수명을 요구하는 분야의 표준으로서 센서 네트워크에서 대부분 적용되고 다양한 표준의 기반이 되는 IEEE 802.15.4 LR-WPAN(Low Rate Wireless Personal Area Networks)의 분석을 통해 LR-WPAN기반 센서 네트워크 환경에서 가능한 서비스거부 공격을 살펴본다. 또한 그의 특화된 공격인 슬립거부 공격에 대한 취약점을 분석하고 공격을 모델하며, 이를 탐지하는 메커니즘을 제안한다. 슬립거부 공격이란 노드가 Sleep 상태로 변환되는 것을 방해하여 노드의 에너지 소비를 가속화 시키는 방법으로 MAC계층에서 주로 발생하는 서비스거부 공격의 한 형태이다. 예를들어 공격자가 거짓의 SYNC 패킷과 같은 위조 패킷을 생성하여 주기적으로 Receive 상태의 노드에게 전송하게 되면 노드는 계속 Active 상태에 머물게 하여 불필요한 에너지 소모를 유발한다. 특히 이 공격은 제한된 에너지를 갖고 있는 센서 네트워크에 치명적인 공격이라 할 수 있다[5].

IEEE 802.15.4 MAC계층의 슬립거부 공격에 대한 취약성 분석 결과, 비컨(beacon) 메시지의 변조를 통한 슈퍼프레임 구조 변경, CW값 변경을 통한 CSMA-CA(Carrier Sense Multiple Access-Collision Avoidance) 구간 변경, MAC 헤더 필드 변경, 채널스캔 및 PAN 연합동작, GTS 할당동작에서 위조된 메시지 전송 등으로 슬립거부 공격의 취약성 및 가능성을 분석할 수 있었다. 특히 이러한 취약점의 일부는 표준에서 보안 서비스로 제공하고 있는 인증이나 암호화 서비스가 적용이 되어도 공격이 가능함을 알 수 있었다.

본 논문에서는 분석된 취약점 중에 표준에서 정의한 보안 서비스로도 대응이 안되는 채널스캔 및 연합동작에서의 위조된 메시지에 의한 슬립거부 공격에 대한 탐지메커니즘을 제안하였다. IEEE 802.15.4에서 디바이스는 채널 스캔을 통하여 사용 가능한 채널을 선택하고 팬 코디네이터에 의해 구성된 네트워크에 연합하여 팬 코디네이터와 디바이스 간의 동기화를 맞추고 팬 코디네이터가 필요한 패킷을 전송한다. 이 과정에서 Beacon Request와 Association Request 메시지 위조를 통한 슬립거부 공격이 이루어질 수 있는 경우를 분석하고 이런 공격을 팬 코디네이터에서 요청메시지 주기와 요청 노드ID, 요청 노드의 신호세기를 모니터링하여 공격을 식별하고 탐지하는 메커니즘을 제안하였다. QualNet 시뮬레이션 툴[6]을 통해 분석된 공격의 영향을 보이고, 제안된 탐지 메커니즘 적용 시 연합 성공 시간, 센싱 지연, 에너지 소모량, 메시지 변화량 등을 비교하여 본 메커니즘의 우수성을 보였다.

본 논문은 다음과 같은 순서로 구성되어 있다. 1장의 서론에 이어 2장에서는 센서 네트워크에서의 서비스거부 공격 취약점 및 대응 기술 연구 동향과 IEEE 802.15.4 LR-WPAN 표준 기술을 살펴본다. 3장에서는 2장의 IEEE 802.15.4 기술 분석을 기반으로 센서 네트워크에서 이루어질 수 있는 슬립거부 공격의 취약성을 분석하고 공격을 모델링하며, 일부 슬립거부 공격에 대한 탐지 메커니즘을 제안한다. 4장에서는 공격 모델이 네트워크에 미치는 영향을 분석하고 제안한 메커니즘을 적용 시 개선된 성능을 비교 분석한다. 마지막으로 5장에서 본 논문의 결론과 향후 연구 방안에 대해 기술한다.

2. 기존 연구

2.1 센서 네트워크에서 서비스거부 공격 취약점 및 대응기술 연구 동향

본 절에서는 최근에 진행되고 있는 센서 네트워크에서의 서비스거부 공격의 취약점 및 대응기술을 기술한다. 센서 네트워크상에서의 다양한 위협들 중 주요 공격으로 서비스거부(DoS: Denial of Service) 공격이 존재한다. 서비스거부 공격은 센서의 배터리 한계점을 악용하여 쉽게 무선 센서 네트워크의 안전성을 무너뜨릴 수 있다. 서비스거부 공격의 종류와 현재 연구되고 있는 대응 방안들을 계층별로 분류하여 보면 다음과 같다.

• 물리 계층

물리 계층에서 가장 주요한 재밍 공격[7]은 constant jamming, deceptive jamming, random jamming, reactive jamming으로 나누어 볼 수 있다. constant jamming은 공격자가 파형 생성기나 일반적인 무선 디바이스를 사용하여 끊임없는 라디오 신호를 보낸다. 공격자는 채널을 점유함으로써 노드의 합법적인 트래픽을 방해할 수 있다. deceptive jamming은 랜덤 비트를 보내는 대신 공격자가 전송되는 패킷 사이에 어떤 간격도 없도록 채널에 규칙적인 패킷을 끊임없이 삽입한다. 그 결과 일반적인 통신자들은 네트워크 내에 합법적

인 트래픽으로 인식하여 계속 Receive 상태에 머물 것이다. Random jamming의 경우 라디오 신호를 계속 보내는 대신에 Jamming과 Sleep 상태로 번갈아 변환시킨다. Jamming 상태에서는 constant jamming과 deceptive jamming이 발생하고 이 기간 동안 큰 에너지 소비가 발생한다. reactive jamming은 채널이 유휴 상태일 경우에는 공격자는 활동하지 않는다. 라디오 신호 전송이 시작되어 채널에서 센서가 Active 상태이고 트래픽이 감지됐을 경우에만 공격자는 재밍신호를 전송한다. 그러므로 Reactive jammer가 가장 탐지하기 어렵다. 재밍 공격을 식별하기 위한 기술[8]로는 Received Signal Strength Indicator(RSSI), Packet Delivery Ratio (PDR) 을 이용한 통계적 분석이 제안되었고, 앞서 설명한 재밍 공격 탐지에서 이런 기술들은 결합[9]시켜 활용하는 경우 더욱 신뢰할 수 있는 결과를 가져올 수 있다.

다른 공격으로는 노드 간섭이나 노드 파괴를 들 수 있다. 이 경우, 안전하지 못한 지역에 배치된 노드 파괴를 막을 수는 없지만 노드를 숨기거나 위장시켜서 이런 위협을 경감시킬 수 있다.

• 링크/MAC 계층

Interrogation 공격은 RTS/CTS(Request to send/Clear to send) 핸드쉐이크를 활용하는 공격으로, 공격자는 타겟이 된 이웃 노드로부터 CTS를 받기 위해 RTS 메시지를 반복하여 보냄으로써 노드의 자원을 고갈시킨다. Antireplay와 링크 계층에서의 더욱 강화된 인증으로 공격을 경감시킬 수 있다.

MAC계층에서의 슬립거부 공격은 공격자가 노드가 Sleep 상태로 변환되는 것을 방해하여 노드의 에너지 소비를 가속화시키는 방법이다. 센서 네트워크에서 제안된 주요 MAC 프로토콜들로 S-MAC[10], T-MAC[11], B-MAC[12], G-MAC[5] 등이 존재하는데 각 MAC 프로토콜들에 대해 슬립거부 공격의 취약점이 내포되어 있다. S-MAC에서 공격자는 거짓의 SYNC 패킷을 고안해서 주기적으로 보낼 수 있고, 이렇게 되면 노드는 계속 깨어있게 된다. 패킷 인증과 링크계층의 인증은 이 공격에 대한 예방이 가능하다. T-MAC은 S-MAC을 기반으로 하여서 동일한 특성을 그대로 가지고 있다. 공격자는 브로드케스팅이나 리플레잉(replaying)을 이용하여 네트워크의 adaptive time-out duration보다 짧은 간격으로 끊임없이 스트림을 전송하여 노드를 계속 깨어있게 할 수 있다. B-MAC에서 슬립거부 공격은 노드가 이웃 노드의 전송 패킷을 엿듣는 특성을 이용하여, 공격자가 인증되지 않은 스트림을 끊임없이 전송하거나 재생된 브로드캐스팅 패킷을 보낼 수 있다. 그러면 노드는 idle listening 상태가 되어 불필요한 전력소모를 유도할 수 있다. G-MAC은 클러스터 내 전송을 동등하게 조절하기 위해 설계된 MAC 프로토콜로써 경쟁 구간, GTIM(Gateway Traffic indication message)구간과 비경쟁 구간으로 나뉘어진다. 공격자가 브로드캐스트 메시지로 GTIM을 가득 채우면 모든 노드는 브로드캐스트 트래픽으로 인해 Receive 상태에 머무른다.

• 네트워크 계층

스푸핑, 재생 공격[13] 등 다양한 공격이 발생 가능하고 인증과 antireplay 등으로 예방할 수 있다. Hello flood 공격은 노드가 사용하려는 라우터에 공격자가 끊임없이 hello 패킷을 전송하는 플러딩 방식을 이용하여 이뤄진다. 이로 인하여 노드들은 hello 패킷 때문에 바로 옆의 노드와 직접 통신할 수 없게 됨으로써 에너지 소모가 가속화된다. Pairwise 인증과 지리정보를 활용한 라우팅을 통해 Hello flood 공격을 경감시킬 수 있다. 또한 발생 가능한 homing 공격은 공격의 타겟이 되는 노드를 식별하기 위하여 트래픽 패턴을 분석하는 것이다. 헤더 인증과 더미 패킷을 활용하여 공격을 경감시킬 수 있다.

• 전송 계층

이 계층에서는 TCP SYN(synchronize) flood 공격[14]이 발생할 수 있는데, 공격자는 다수의 연결 요청을 보내어 타겟의 연결버퍼를 오버플로우 시킬 수 있다. 대응책으로는 SYN cookies를 활용할 수 있다. 비동기화 공격 또한 전송계층에서 발생할 수 있는 공격으로 공격자는 위조된 패킷을 전송함으로써 두 노드 사이에 활성화 되어 있는 연결을 방해한다. 이는 패킷 인증으로 공격을 예방할 수 있다.

• 응용 계층

공격자는 대량의 데이터 전송을 시도하여 네트워크의 대역폭을 소비하고 노드의 에너지를 소모를 유발 시킬 수 있다[14]. 효율적인 데이터 애그리게이션과 rate-limiting 방법이 이러한 공격에 어느정도 대응할 수 있다. 그 밖에도 path 기반의 서비스거부 공격 등이 발생할 수 있고 인증과 antireplay를 통해 공격에 대한 예방이 가능하다.

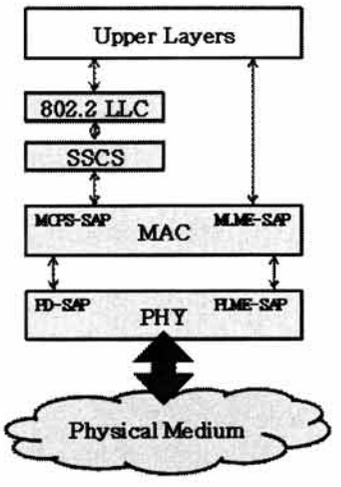
2.2 IEEE 802.15.4 LR-WPAN 기술

2.2.1 IEEE 802.15.4 LR-WPAN 개요

IEEE 802.15.4 표준기술[1]은 무선 센서 네트워크 또는 무선 에드혹 네트워크에 적용될 수 있는 기술로서, 10m의 POS(Personal Operating Space) 영역 동작에서 제한적 에너지 소모가 요구되는 고정형, 휴대형 또는 이동형 디바이스의 저속 데이터 전송속도의 무선통신 능력을 위해 (그림 1)과 같이 물리계층과 MAC부계층을 정의한다.

물리계층은 PLME(Physical Layer Management Entity)를 통해 물리계층 데이터 서비스와 물리계층 관리 서비스를 제공한다. 물리계층 데이터 서비스는 물리적 채널을 통해 PPDU(PHY Protocol Data Units)의 전송과 수신을 가능하게 하다. 물리계층의 기능으로는 무선 영역의 활성화 및 비활성화, 현재 사용하는 채널에서 에너지 검출, 노드 사이의 전송특성을 나타내기 위한 LQI(Link Quality Indication)사용, 채널 주파수 선택, CSMA-CA를 사용하기 위한 CCA (Clear Channel Assessment) 지원, 데이터 송신 및 수신 등이 있다.

MAC계층은 MLME-SAP(MAC Sublayer Management



(그림 1) LR-WPAN 디바이스 구조

Entity Service Access Point)을 통해 MAC 데이터 서비스와 MAC 관리 서비스를 제공한다. MAC 데이터 서비스는 물리계층 데이터 서비스를 통해 MPDU(MAC Protocol data units)의 전송과 수신을 가능하게 한다. MAC 계층의 기능으로는 채널 접속, 비컨 관리, GTS(Guaranteed Time Slots) 관리, ACK 프레임 전달, 프레임 유효성 검사 등이 있다.

상위 계층은 네트워크 구성과 관리, 메시지 라우팅을 제공하는 네트워크 계층과 디바이스에 맞는 기종을 제공하는 응용계층으로 구성된다. LLC(Logical Link Control)는 SSCS (Service Specific Convergence Sublayer)계층을 통하여 MAC부계층에 접근이 가능하다.

IEEE 802.15.4를 따르는 시스템은 다양한 컴포넌트로 이루어지며 가장 기본이 되는 것이 디바이스이다. 디바이스 타입으로는 FFD(Full Function Device)와 RFD(Reduced Function Device)가 존재하며 FFD는 FFD 또는 RFD 모두와 통신 가능하며 팬 코디네이터, 코디네이터, 디바이스 세 가지 타입이 될 수 있다. RFD의 경우에는 FFD에 한하여 통신 할 수 있고 디바이스 타입만이 될 수 있으며 최소의 리소스와 메모리 용량을 갖는다. WPAN을 구성하는 디바이스 중 하나 이상은 팬 코디네이터로 작동하기 위해 FFD이여야 한다.

디바이스 간 데이터 전송은 3가지가 존재한다. 첫 번째는 디바이스가 코디네이터에게 데이터를 전송하는 것이고 두 번째는 디바이스가 코디네이터로부터 데이터를 수신하는 것이다. 마지막 세 번째는 데이터를 두 개의 동등 디바이스 사이에서 전송하는 것이다. 스타 토폴로지는 데이터가 코디네이터와 디바이스 사이에서만 교환되기 때문에 두 가지 전송 타입만 사용할 수 있지만, 상호 동일계층 토폴로지에서는 세 가지 타입 모두를 사용할 수 있다.

2.2.2 IEEE 802.15.4 LR-WPAN 기본 구조

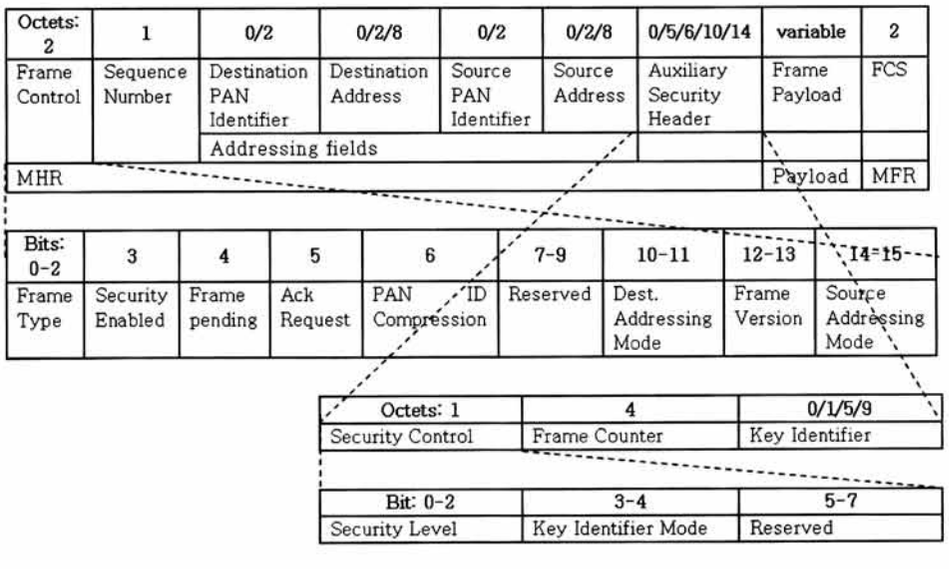
• IEEE 802.15.4의 MAC 프레임 포맷

802.15.4에서 기본적으로 네 가지 프레임 구조에 대해 <표 1>과 같이 정의하고 있다.

각 프레임은 MHR(MAC Header), MAC Payload, MFR (MAC Footer)으로 이루어져 있다. (그림 2)는 일반적인 MAC 프레임의 형태로 프레임 컨트롤 필드와 시퀀스 번호 필드, 그리고 주소 필드, 프레임 페이로드 필드와 에러검출 필드로 구성된다. 프레임 컨트롤 필드는 프레임 타입과 그

〈표 1〉 MAC 프레임의 종류

프레임	용도
Beacon Frame	코디네이터가 비컨을 전송 시 사용
Data Frame	모든 데이터 전송 시 사용
Acknowledgement Frame	성공적인 프레임 수신을 확인 할 때 사용
MAC Command Frame	Mac에 대한 관리를 위한 전송 시 사용



(그림 2) MAC 프레임 포맷

〈표 2〉 MAC 부계층의 가능한 보안 레벨

Security level identifier	Security Control field b2 b1 b0	Security attributes	Data confidentiality	Data authenticity (including length M of authentication tag, in octets)
0x00	'000'	None	OFF	NO (M=0)
0x01	'001'	MIC-32	OFF	YES (M=4)
0x02	'010'	MIC-64	OFF	YES (M=8)
0x03	'011'	MIC-128	OFF	YES (M=16)
0x04	'100'	ENC	ON	NO (M=0)
0x05	'101'	ENC-MIC-32	ON	YES (M=4)
0x06	'110'	ENC-MIC-64	ON	YES (M=8)
0x07	'111'	ENC-MIC-128	ON	YES (M=16)

외의 여러 컨트롤 플래그를 포함한다. <표 2>는 (그림 2)의 Security Level 값에 따라 적용되는 보안 레벨에 관련된 표이다. 표의 내용대로 기본적으로 암호화 서비스와 인증 서비스를 제공할 수 있다.

• IEEE 802.15.4의 MAC 프리미티브

MAC은 상위 계층으로 2개의 SAP을 통해 두 가지 서비스를 제공한다. MAC 데이터 서비스는 MCPS-SAP(MAC Common Part Sublayer)을 통해 접속되며, MAC 관리 서비스는 MLME(MAC Layer Management Entity)-SAP을 통해 접속된다. 이들 서비스는 SSCS나타 LLC와 물리계층과의 인터페이스를 제공한다. 제공하는 MAC 프리미티브는 <표 3>과 같다.

• IEEE 802.15.4의 보안 기능

IEEE 802.15.4에서의 MAC부계층에서는 해당 계층으로의 유입 및 유출 프레임에 대해서 상위 계층의 요구에 따라 선택적으로 보안 서비스들을 제공할 수 있다. 데이터 기밀성, 데이터 인증, 재연방지라는 보안서비스를 제공하기 위해, 키 테이블, 유출 프레임에 대한 최소 보안요구 레벨테이블, 디바이스테이블 등과 같은 각 노드에서 관리하는 보안관련 PIB(PAN Information Base) 속성을 정의하고 있다. 또한 (그림 2)의 SecurityEnabled 값이 TRUE로 설정되어 있는 유입 및 유출 프레임들에 대해 설정된 PIB 속성 값에 따라 보안 서비스를 수행할 수 있도록 간략한 보안절차를 제공하고 있다. 보안절차에는 유출 프레임 보안 및 키 검색 절차와 유입 프레임 보안 및 보안요소 추출 절차가 수행된다. 이어서 Key lookup 절차 및 Device lookup 절차와 블랙리스트 확인 절차가 이루어지고 유입 보안수준 확인 및 키 사용정책 확인 절차가 진행된다.

3. 슬립거부 공격에 대한 분석 및 탐지 메커니즘

3.1 슬립거부 공격 유형 분석

3.1.1 기본 동작

• 채널 스캔

모든 디바이스들은 정해진 채널 목록에 대하여 수동 스캔과 Orphan 스캔을수행할 수 있다. FFD는 에너지검출 스캔과 능동 스캔을 추가로 수행할 수 있다. 디바이스의 MLME는 채널스캔 시작을 MLME-SCAN.request 프리미티브를 통해 지시받고 채널들은 낮은 채널 번호에서 높은 번호순으로 스캔된다. MLME-SCAN.confirm 프리미티브를 통해 스캔의 결과를 보고한다.

〈표 3〉 MAC 프리미티브

MAC 데이터 서비스	MCPS-DATA	MAC계층과 PHY계층 간에 데이터 패킷 교환
	MCPS-PURGE	전송 열에 대기중인 MSDU를 버퍼에서 지움
MAC 관리 서비스	MLME-ASSOCIATE/DISASSOCIATE	네트워크 연관 및 탈퇴
	MLME-SYNC/SYNC-LOSS	단말기 사이의 동기화 제공
	MLME-SCAN	RF 채널을 찾음
	MLME-COMM-STATUS	통신 상태를 알림
	MLME-GET/SET	MAC PIB 파라미터를 설정하고 수정
	MLME-START/BEACON-NOTIFY	비컨 관리
	MLME-POLL	비컨 없이 동기화 시킴
	MLME-GTS	GTS 관리
	MLME-RESET	PAN을 시작하기 전에 리셋 요청
	MLME-ORPHAN	통신이 두절된 단말기 관리

• PAN의 시작과 재 정렬

PAN은 MLME-RESET.request 프리미티브를 보내어 먼저 MAC부계층 리셋을 수행하고, 능동채널 스캔과 적절한 PAN 식별자를 선택 후에 FFD에 의해서만 시작된다.

• 가입

디바이스는 먼저 채널 스캔을 수행한 다음에 가입을 시도할 수 있는데, 능동 채널 스캔이나 혹은 수동 채널 스캔을 수행한다. 채널 스캔의 결과는 적절한 PAN을 선택하는데 사용된다. 가입할 PAN을 선택한 다음에 차 상위 계층은 MLME-ASSOCIATE.request 프리미티브를 통해 가입에 필요한 정보들을 보낸다. 코디네이터는 가입이 허용되는 디바이스에 한하여 가입을 허용한다. 이와 유사하게 디바이스는 현재 가입을 허용하는 코디네이터를 통해서만 PAN에 가입하는 것을 시도한다. 만약 가입 허용이 불가로 설정된 코디네이터가 가입요청을 수신하면 이는 무시된다.

• 탈퇴

탈퇴 절차는 MLME-DISASSOCIATE.request를 차 상위 계층에서 MLME로 보냄에 의해서 시작된다. 코디네이터가 가입된 디바이스 중의 하나가 PAN에서 떠나기를 원하면, 코디네이터의 차 상위 계층은 MLME-DISASSOCIATE.request 프리미티브를 MLME로 보내고, MLME는 탈퇴통보 명령어를 보낸다.

• 동기화

비컨 사용 PAN의 경우 동기화는 비컨 프레임을 수신하고 디코딩하여 수행된다. 비컨 비사용 PAN의 경우 동기화는 디바이스가 데이터 수신을 위해 코디네이터를 폴링하는 것으로 수행된다. 비컨 사용 PAN의 경우 동작하는 모든 디바이스는 비컨 동기화를 획득할 수 있다. 디바이스는 MLME-SYNC.requset 프리미티브를 통해 비컨 획득에 대한 시도를 지시받고 비컨 획득하기를 시도한다.

• GTS할당 및 관리

GTS는 팬 코디네이터에 의해서만 할당되고 GTS는 팬 코디네이터와 PAN에 가입된 디바이스간의 통신에만 사용된다. 슈퍼프레임에서 용량이 충분하다면 팬 코디네이터는 동시에 7개까지 GTS를 할당할 수 있다.

3.1.2 가능한 슬립거부 공격 유형 분석

802.15.4의 기본 동작과 슈퍼프레임 구간 내에서 가능한 슬립거부 공격들을 <표 4>와 같이 분석하였고, 각 취약점들이 앞 절에서 설명한 표준 보안서비스를 적용하지 않은 경우(None)와 적용한 경우(In Security)로 나누어 공격의 가능성을 표기하였다.

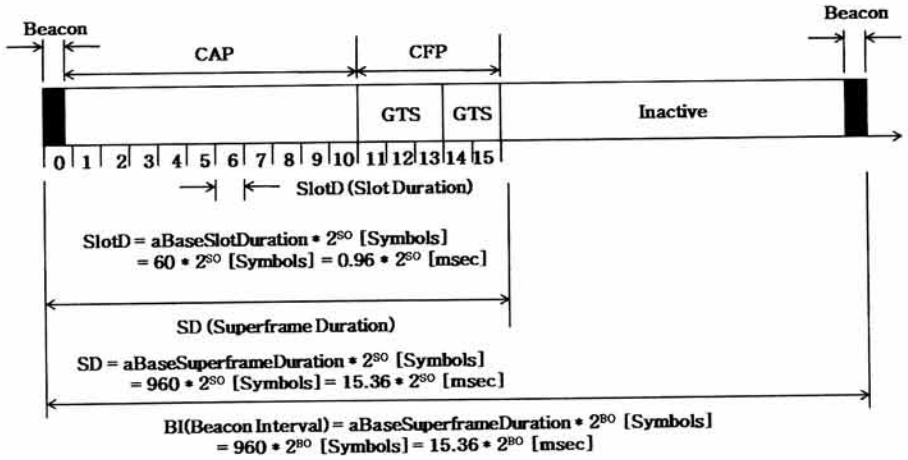
• 슈퍼프레임 구간 변경

슈퍼프레임을 제공하는 802.15.4의 센서 네트워크상에서는 슈퍼프레임의 구간을 결정짓는 BO(macBeaconOrder)와 SO(macSuperframeOrder)를 통해 슬립거부 공격을 수행할 수 있다. 슈퍼프레임 구간 내에서 BO는 총 슈퍼프레임 구간을

〈표 4〉 802.15.4기반 센서네트워크의 동작 내에서 가능한 슬립거부 공격

Weak point	None	In Security
Superframe: BO(macBeaconOrder)	O	-
Superframe: SO(macSuperframeOrder)	O	-
CSMA-CA: CW	O	O
MAC 헤더: Frame Pending	O	O
MAC 헤더: Ack Request	O	O
Active 채널스캔: Beacon Request	O	O
Orphan 채널스캔: Orphan Notification	O	-
Association: Association Request	O	O
Association: Association Response	O	-
GTS allocation: GTS Request	O	-
GTS allocation: Beacon(with GTS descriptor)	O	-

O: 공격 가능, -: 공격 불가능



(그림 3) IEEE 802.15.4 슈퍼프레임 구조

결정하고, SO는 그 구간 내의 Active구간의 크기를 결정한다. 그렇기 때문에 SO가 BO와 같은 값을 갖는다면 디바이스 들은 Inactive구간을 갖지 못하고 계속 Active구간에 머물러 있게 된다.

• CW값 변경에 의한 CSMA/CA 변형

CSMA/CA 알고리즘은 다수의 디바이스가 공유된 채널을 사용하기 위해 채널 사용 여부를 체크하고 충돌을 회피할 수 있도록 하는 알고리즘으로서, 경쟁접근 기간인 CAP (Contention Access Period) 동안 데이터나 제어 프레임을 전송하기 전에 사용한다.

모든 기기는 CSMA/CA를 수행함에 있어서 각각의 전송 시도 시, NB(Number of Backoff), CW(Contention Window), BE(Backoff Exponent)라는 3개의 변수를 보유하고 관리한다. 디바이스가 송신 데이터를 가지고 있으면, 먼저 [0, 2^{BE}-1] 범위에서 백오프 값을 랜덤하게 선택하여 백오프를 수행한다. BE는 백오프를 위한 지수 값이며, 이 값은 백오프 선택 범위를 결정한다. NB는현재의 전송을 시도하는 동안 수행된 백오프 수이며, 0으로 초기화 되고 최대 백오프 수를 제한하기 위해 사용된다. CW는 전송을 시작하기 전에 채널 사용 여부를 체크하는 수를 나타내며, 각 전송 이전에 2로 초기화하고 체크할 때 1씩 감소하여 0이 되면 전송을 수행하며, 채널이 사용 중이면 2로 리셋 된다. 즉 채널을 사용하기 전에 채널 사용 여부를 2번씩 체크하게 하여 충돌을 방지하게 한다.

표준의 CSMA/CA 알고리즘에서 CW가 2로 설정되어 있기 때문에 사용 가능한 채널을 두 번 확인하게 된다. 이 때 공격자가 CW를 1로 설정하여 사용 가능한 채널을 한번만 체크하도록 하면 다른 디바이스보다 빠르게 채널을 사용할 수 있다. 이 경우 일반 디바이스는 계속 채널 할당을 못 받게 되고 반복되는 채널 확인을 통해 데이터 전송을 하지 못하고 에너지 소모를 가져오게 된다[15].

• MAC 헤더 필드 변경

MAC 헤더의 프레임 컨트롤 필드 중 Frame Pending은 송신자가 수신자에게 더 보낼 데이터가 있을 경우에 사용되는 부분으로 이것이 1로 설정되어 있으면 수신자는 데이터 요청 커맨드를 전송하게 된다. 공격자는 중간에서 설정된 것을 바꾸어 보낼 수 있다. Frame Pending이 1로 설정되어 있는 것을 0으로 바꾸어 보내는 경우 수신자는 자신이 받을 데이터가 있다는 것을 알 수 없고 송신자는 보낼 데이터의 전송을 계속 유보하게 된다. 반대로 Frame Pending이 0으로 설정되어 있는 것을 1로 설정하여 보내면 수신자는 새로운 데이터 요청 커맨드를 전송한 뒤 응답을 기다리지만 송신자는 자신이 보낼 데이터가 없기 때문에 무시하게 된다.

동일한 발상으로 공격자는 MAC 헤더의 프레임 컨트롤 필드 중 Ack Request 필드 값도 중간에서 변경 가능하다. Ack Request 필드 값을 1에서 0으로 바꾸어 보내면 송신자는 Ack을 요청하였기 때문에 Ack을 기다리게 되고 응답이 오지 않으면 Ack 요청을 재시도하게 된다.

• 채널스캔 동작

디바이스는 PAN을 시작하기 전에 채널스캔을 시행한다. 능동 채널스캔과 Orphan 스캔 동작에서 디바이스는 각각 Beacon Request와 Orphan Notification을 팬 코디네이터에게 끊임없이 전송함으로써 디바이스와 팬 코디네이터의 에너지 소모를 유발할 수 있고 PAN에 다른 디바이스들이 연합하는 것을 방해하여 전체적인 네트워크의 에너지 소모를 가져올 수 있다.

• 연합 동작

디바이스가 PAN에 연합하기 위한 동작에서 디바이스는 팬 코디네이터에게 Association Request 메시지를 전송한다. 이 메시지를 받은 팬 코디네이터는 Association Request 메시지에 대한 Ack을 보내고 그 후, Association Response 메시지를 전송한다. 이 경우에도 공격자가 반복적인 Association Request 메시지 전송을 통해서 코디네이터의 에너지 소모와 다른 디바이스들의 PAN 연합을 방해하여 네트워크의 성능을 저하시킬 수 있다. 또한 송신되는 Association Response 메시지를 재밍공격으로 수신을 방해하여 연합 요청을 재시도하게 하여 원활한 연합을 수행하지 못하고 에너지 낭비를 유발할 수 있다.

• GTS 할당 동작

디바이스가 GTS 요청을 원하면 GTS를 관리하는 팬 코디네이터에게 GTS Request를 보내게 된다. 이 메시지를 받은 팬 코디네이터는 메시지에 대한 Ack을 보낸 후 비컨에 GTS descriptor를 실어서 디바이스에게 전송하게 된다. 이에 대한 공격으로 공격자는 다른 노드의 주소로 소스 주소를 스푸핑하여 많은 GTS Request를 전송할 수 있고, 그러면 불필요한 GTS가 할당되어 낭비될 수 있으며, GTS 고갈을 유도하면 실제 GTS가 필요한 노드에게는 할당되지 못하게 될 수 있다. 또한 공격자는 위조된 비컨 메시지의 GTS descriptor를 변조하여 전송함으로써 GTS 사용을 할 수 없도록 하거나 두개 이상의 노드에게 하나의 GTS를 할당하도록 알려주어 충돌을 야기하고 에너지 낭비를 유발시킬 수 있다.

이처럼 IEEE 802.15.4를 기반으로 하는 센서 네트워크에서 가능한 슬립거부 공격은 다양하게 존재한다. 특히 보안 서비스가 적용되는 경우에도 공격자의 CW값 변조는 막을 수 없으며, MAC헤더는 기본적으로 암호화나 인증 범위에서 제외되어 보호될 수 없고, Beacon Request나 Association Request는 연합이 수행되기 전 전송되는 메시지이므로 보안 서비스가 적용될 수 없다. 또한 슬립거부 공격은 간단하게 이루어질 수 있지만 이 공격을 통해서 디바이스와 팬 코디네이터가 Sleep 상태로 변환되지 못하고 Active 상태에 머물게 된다. 이런 네트워크 상태는 팬 코디네이터 노드의 에너지 소모는 물론이고 디바이스 노드의 에너지 소모에도 영

향을 미치게 되고 이는 결국 네트워크 전체의 성능을 저하시키거나 네트워크 전체의 오류를 유발 시킬 것이다. 따라서 MAC계층에서 발생할 수 있는 슬립거부 공격이 발생했을 경우에 대비하여 네트워크에 미치는 영향에 대한 연구와 이를 탐지할 수 있는 방안의 연구가 필요하다.

3.2 슬립거부 공격 모델링

서비스거부 공격 중 특화된 공격인 슬립거부 공격은 MAC계층에서 쉽게 발생할 수 있는 공격으로 간단한 공격을 통해 디바이스나 팬 코디네이터의 에너지를 고갈시키고 네트워크 장애까지 유발할 수 있다. 이에 본 절에서는 3.1절에서 분석한 공격 중 IEEE 802.15.4에서 제공하는 보안 기능 적용과 관계없이 발생할 수 있는 MAC계층의 슬립거부 공격 중, 연합동작과 스캔동작에서의 공격을 모델링 한다.

3.2.1 연합(Association) 동작 내의 슬립거부 공격

디바이스는 가입할 PAN을 선택한 다음 MLME-ASSOCATE. request 프리미티브를 통해 가입에 필요한 정보들을 보내는 것을 시작으로 PAN에 가입하기 위해 (그림 4)와 같이 동작한다.

이에 공격자는 다음과 같이 프레임을 생성하여 공격할 수 있다. MAC 프레임 포맷의 서브 필드인 프레임 컨트롤 필드의 프레임 타입은 <표 5>와 같이 5가지로 구분된다.

공격자 노드는 프레임 타입의 필드를 011로 설정하여 MAC command를 프레임으로 설정하고 그 후 프레임 포맷이 형성되면 Payload 내의 Command 프레임 식별자의 서브 프레임을 설정한다. <표 6>은 MAC command 프레임의 식별자와 RFD의 송수신 가능 여부를 나타내었다.

Association Request 메시지를 이용한 슬립 거부 공격을 위해 Command 프레임 식별자를 0x01로 설정하여 MAC command 중에서도 연합을 요청하는 메시지를 생성한다.

〈표 5〉 프레임 타입 서브필드 값

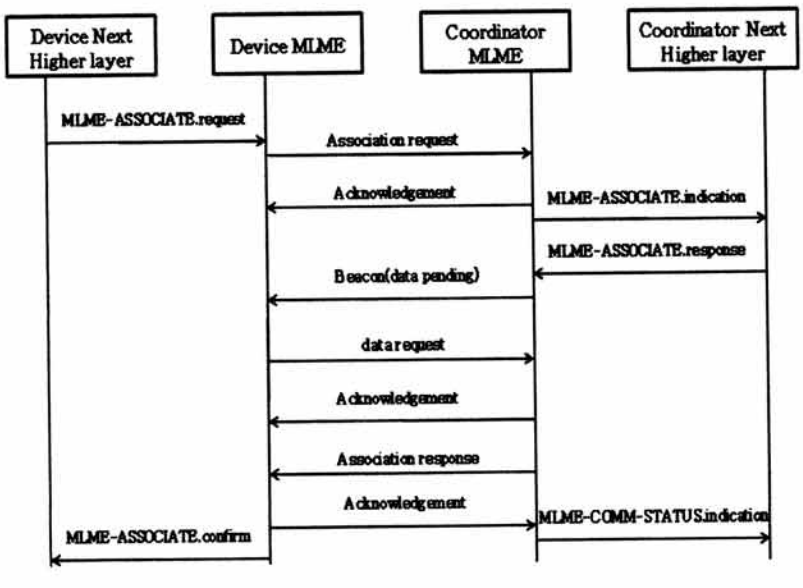
Frame type value b2 b1 b0	Description
000	Beacon
001	Data
010	Acknowledgment
011	MAC command
100-111	Reserved

〈표 6〉 MAC command 프레임

Command frame identifier	Command name	RFD	
		Tx	Rx
0x01	Association request	O	
0x02	Association response		O
0x03	Disassociation notification	O	O
0x04	Data request	O	
0x05	PAN ID conflict notification	O	
0x06	Orphan notification	O	
0x07	Beacon request		
0x08	Coordinator realignment		O
0x09	GTS request		
0x0a-0xff	Reserved		

O: 수행 가능

IEEE 802.15.4의 표준에서 Association request command로 설정된 프레임은 기본적으로 추가적인 메시지 정보의 여부를 나타내는 Frame pending을 0으로 설정하게 되어있어 메시지를 보낸 후 바로 추가적인 재전송이 이루어 지지 않는다. 하지만 슬립거부 공격을 위해 공격자 노드는 끊임없이 Association Request 메시지를 팬 코디네이터에게 재전송한다. 또한 초기 PAN에 연합 단계이기 때문에 Security Enabled 필드 역시 1로 설정되어 있지 않아도 무방하다.



(그림 4) PAN에서의 연합 동작

공격자는 생성한 Association Request 메시지를 팬 코디네이터에게 끊임없이 반복적 전송함으로써 다른 정상 디바이스 노드가 PAN에 가입되는 시간을 늦추고 디바이스 노드가 끝까지 가입하지 못하는 경우를 발생시킬 수 있다. 또한 팬 코디네이터가 공격자의 끊임없는 연합 요청에 대한 Ack이나 연합 요청에 대한 응답 메시지를 전송함으로써 팬 코디네이터 자신의 에너지를 낭비를 유발시킬 수 있다.

3.2.2 능동 스캔 동작 내의 슬립거부 공격

능동 스캔은 상위 계층으로부터 채널 스캔 요청을 받은 후, 디바이스가 비컨이 전송되어 오는 것을 기다리지 않고 스스로 Beacon Request 메시지를 팬 코디네이터에 전송함으로써 비컨을 요청한다. 그 동작은 (그림 5)와 같다.

이에 공격자는 Beacon Request 메시지를 다음과 같이 생성한다. 스캔 동작 내의 슬립거부 공격을 위해 MAC 프레임 포맷의 프레임 컨트롤 필드를 011로 설정하여 MAC command 프레임으로 설정하고 그 후 프레임 포맷이 형성되면 Payload 내의 Command 프레임 식별자의 서브 프레임을 설정한다.

Beacon Request 메시지를 이용한 슬립거부 공격을 위해 command 프레임 식별자를 0x07로 설정하여 MAC command 중에서도 비컨 전송을 요청하는 메시지를 생성한다. IEEE 802.15.4의 표준에서 Beacon request command로 설정된 프레임은 기본적으로 추가적인 메시지 정보의 여부를 나타내는 Frame pending을 0으로 설정하게 되어있어 메시지를 보낸 후 바로 추가적인 재전송이 이루어 지지 않는다. 하지만 슬립거부 공격을 위해 공격자 노드는 끊임없이 Beacon Request 메시지를 팬 코디네이터에게 재전송 하도록 한다. 또한 Security Enabled 필드 역시 IEEE 802.15.4의 표준에서 0로 설정하도록 되어 있으므로 제공되는 보안 기능이 적용되지 못한다.

공격자는 생성한 Beacon Request 메시지를 팬 코디네이터에게 끊임없이 반복 전송함으로써 다른 정상 디바이스 노드의 능동 채널 스캔이 이루어 지지 못하도록 방해한다. 또한 팬 코디네이터는 공격자로부터의 끊임없는 비컨 요청에 대한 비컨을 전송함으로써 팬 코디네이터 자신의 에너지를 낭비하게 되고, IEEE 802.15.4에서의 네트워크 동작의 기본인 채널 스캔이 제대로 이루어지지 않음에 따라 PAN에 가입되지 못하고 네트워크에서 동작하지 못하는 희생노드가 발생한다.

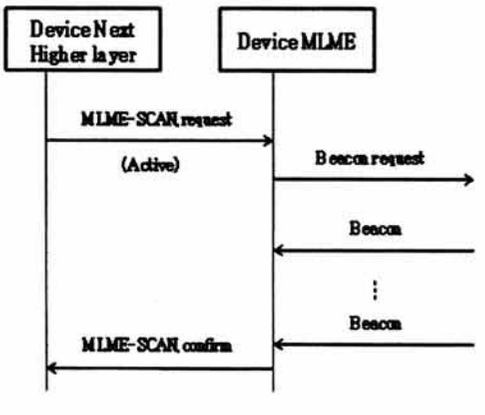
3.3 제안한 공격 탐지 메커니즘

이 장에서는 3.2절에서 모델링한 공격자를 탐지하는 메커니즘을 제안한다. 우선 제안하는 메커니즘을 위한 기본적인 가정사항은 다음과 같다. 무선 센서 네트워크의 환경은 안정적고, 각 디바이스와 팬 코디네이터의 위치, 공격자의 위치는 고정되어 있다고 가정한다. 각 디바이스의 신호세기는 고유하여 팬 코디네이터는 신호세기로 어느정도 노드를 식별할 수 있으며, 보안기능은 IEEE 802.15.4를 기반으로 한다. 각 디바이스의 신호세기를 고유한 노드의 특징으로 삼는 것은 노드의 신호세기를 통해 위치를 측정하는 연구[16, 17]들과 신호세기를 노드의 인증이나 키생성을 위해 사용한 최신 연구[18, 19]를 통해 충분히 가능한 가정으로 볼 수 있다.

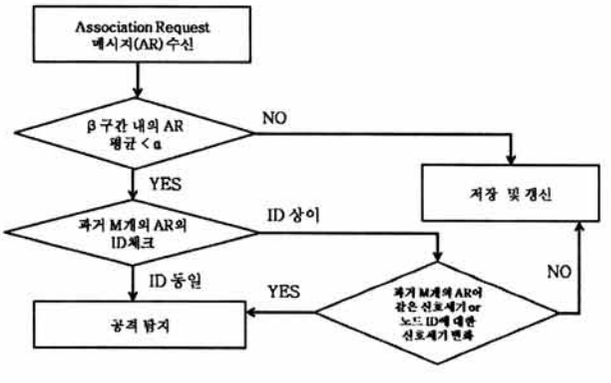
위의 가정사항을 기반으로 다음과 같이 팬 코디네이터는 공격을 탐지한다. 코디네이터는 디바이스에게 받은 정보들을 바탕으로 (그림 7)과 같은 정보를 저장하고 갱신하며 디바이스의 메시지 전송이 공격인지 아닌지 판단한다. 코디네이터의 탐지 메커니즘 동작은 (그림 6)과 같이 수행된다.

(그림 6)의 탐지 메커니즘에서 사용되는 파라미터 값 M은 한 PAN 내의 노드의 수에 준하여 결정하고, β 구간이란 초기 PAN이 형성되는데 걸리는 시간에 기준하여 결정한다. 또한 α는 초기 PAN이 형성될 때 β 구간 내에 전송된 Association Request 메시지의 평균 interval을 기준으로 결정한다.

팬 코디네이터는 네트워크의 동작이 시작되면 (그림 7)과 같은 연합된 디바이스의 ID와 해당 노드로부터의 수신 신호세기를 저장하여 관리한다. 또한 팬 코디네이터가 Association Request(AR) 메시지를 수신하게 되면 (그림 6)에서처럼 β 구간 동안의 AR 평균을 갱신하고 이를 α와 비교하여 α보다 크다면, (그림 7)의 테이블을 갱신한다. 그러나 α보다 작다



(그림 5) 능동 스캔 동작



(그림 6) 팬 코디네이터에 의한 공격자 노드 탐지 메커니즘 동작

노드 ID	신호세기

과거 M개 AR 송신 노드의 ID	과거 M개 AR 송신 노드의 신호세기

β 구간의 AR 평균

(그림 7) 팬 코디네이터에 저장 되는 관리 정보

면, 즉, AR 메시지 전송 주기가 일정 구간 β 내의 평균 주기의 임계치 값 보다 낮게 되면 메시지 전송이 너무 많아지는 것이므로 AR 메시지에 의한 공격을 의심하고, 다시 과거 M개의 AR ID를 체크하하여 ID가 동일한 ID라면 공격을 탐지하게 된다. 그러나 ID가 다르다면 ID까지 변조하여 수행한 공격의 가능성을 타진하기 위해 과거 M개의 AR이 같은 신호세기이거나 AR 메시지의 노드 ID에 대한 신호세기가 변화되었다면 공격을 탐지하게 된다. 즉 전자의 공격 탐지는 동일한 ID를 가지고 다수의 AR 메시지 전송에 의한 공격에 대한 탐지이고, 후자의 공격 탐지는 다수의 ID를 이용해 다수의 AR 메시지를 생성하여 전송하는 공격에 대한 탐지이다.

이 탐지 메커니즘은 Association Request 메시지에 대해 Ack이 오지 않거나 전송에 성공하지 못하는 경우 메시지를 재전송하여 연합을 요청하는 일반적인 경우에는 공격으로 탐지하지 않는데, 왜냐하면 이 때에는 그 전송 주기가 공격에서처럼 빨라지지 않고 한꺼번에 Association Request 메시지의 전송이 폭주하지는 않기 때문이다. 또한 한 공격자가 다른 노드 ID를 이용하여 공격의 경우에도 각각의 노드들이 위치와 상황이 다르기 때문에 다른 노드 ID간의 같은 신호세기를 갖는 것은 매우 미비한 경우이므로 앞에서 가정한 것처럼 공격을 탐지하는 요소로 신호세기를 사용하여 물리계층의 정보를 활용할 수 있다.

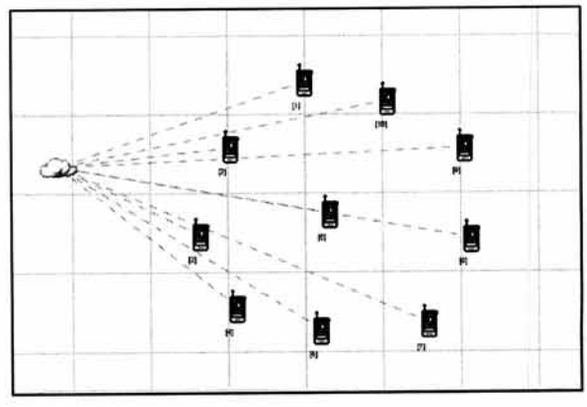
이와 동일하게 Beacon Reqeust 메시지에 의한 공격 탐지를 위해 (그림 7)과 같이 동일한 정보를 관리하고 (그림 6)과 같은 동일한 메커니즘이 적용될 수 있다.

4. 시뮬레이션 및 결과 분석

4.1 시뮬레이션 환경

시뮬레이션은 QualNet 4.5 버전의 센서 모듈을 이용하여 IEEE 802.15.4의 무선 센서 네트워크 환경에서 진행하였다.

기본적으로 하나의 PAN은 (그림 8)과 같이 센서 노드 10개로 구성되어 있다. 모든 노드는 FFD로 설정되어 있고 이 가운데 5번 노드는 팬 코디네이터 노드로서 PAN을 시작하고 구성한다. 팬 코디네이터 노드인 5번 노드를 제외한 모든 노드들은 공격자로 정의하면 공격자 노드가 될 수 있다. 각각의 노드는 고유의 신호세기를 갖고 있고 네트워크는 안정적인 환경으로서 물리적 장애 등이 존재하지 않는다고 가정하였다. 시뮬레이션 공간은 120m x120m이고, 시뮬레이션은 50초간 지속된다. 라우팅 모델은 AODV를 사용하였고,



(그림 8) 시뮬레이션 환경

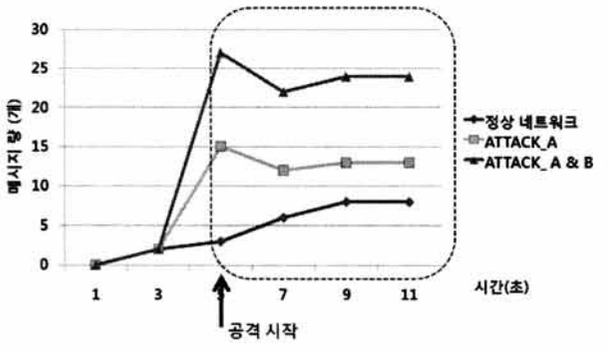
에너지 모델은 MICAz모델을 가정하였다.

기본 센서 모듈에 앞장에서 소개한 공격자 모델과 탐지 모델을 추가 구현하고 시뮬레이션 하였다. 공격자 모델로서 ATTACK_A(Association Request를 이용한 연합 동작 내의 슬립거부 공격)와 ATTACK_B(Beacon Request를 이용한 능동 스캔 동작 내의 슬립거부 공격)라는 프로토콜을 구현하여 추가하였다. ATTACK_A와 ATTACK_B 프로토콜은 지정한 디바이스 노드, 즉 공격자 노드가 팬 코디네이터인 5번 노드에게 초기 네트워크 셋업 시의 Request 메시지 평균 interval보다 훨씬 짧은 시간인 0.25초 간격으로 각각 Association Request와 Beacon Request 메시지를 전송한다. 또한 ATTACK_A&B는 ATTACK_A 프로토콜과 ATTACK_B 프로토콜을 같이 동작시켜 강력한 공격을 시행한다.

탐지 모델은 기본 IEEE 802.15.4 코드의 코디네이터 수행 모듈에 앞 장에서 기술한 탐지를 위한 관리 정보 테이블을 생성하여 관리하도록 하고 이를 기본으로 탐지 메커니즘을 수행하도록 하는 코드를 추가하였다. 탐지 메커니즘에서 사용하는 파라미터 β 값은 초기 PAN이 형성되는데 걸리는 시간을 측정하여 이를 기반으로 5초로 설정하였고, α값은 초기 PAN이 형성될 때 β 구간 내에 전송된 Association/BeaconRequest 메시지의 평균 interval을 기준으로 0.7초로 설정하였으며, M은 노드수에 따라 10이라고 설정하였다.

4.2 결과 및 분석

(그림 9)는 시간에 따른 Association Request 메시지 수를 보여준다. 정상 네트워크일 경우에는 메시지 수가 완만하게 증가하지만 ATTACK_A와 ATTACK A&B 의 공격자 노드가 있는 경우에는 Association Request 메시지 수가

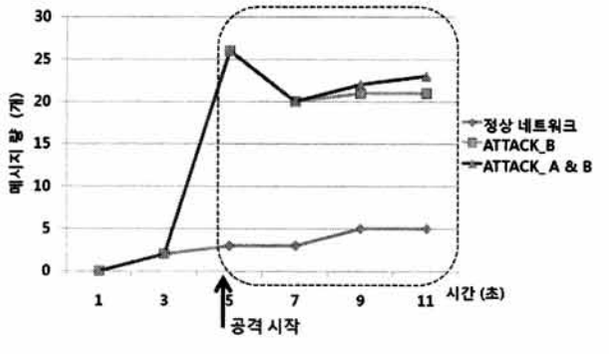


(그림 9) 공격 후 Association Request 전송 메시지 수

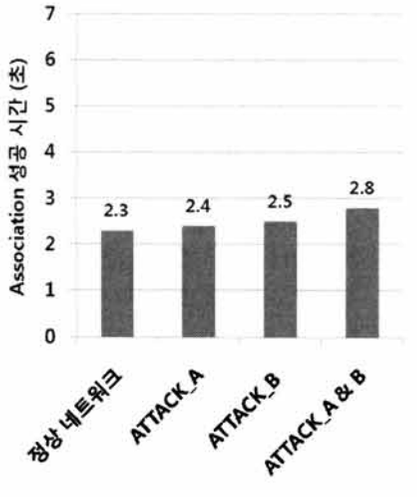
현저하게 늘어나는 것을 비교하여 볼 수 있다.

(그림 10)의 Beacon Request 메시지 수도 비슷한 양상을 보여준다. 이를 통해 정상 네트워크상에서 request 메시지는 최소한의 전송을 하는 반면 공격이 들어간 경우 정상 네트워크의 5배에 가까운 메시지를 같은 시간 내에 보내는 것을 볼 수 있다.

(그림 11)은 하나의 PAN에 각 디바이스가 연합에 성공하기 까지 걸리는 평균 시간을 나타낸 그래프이다. 그래프를



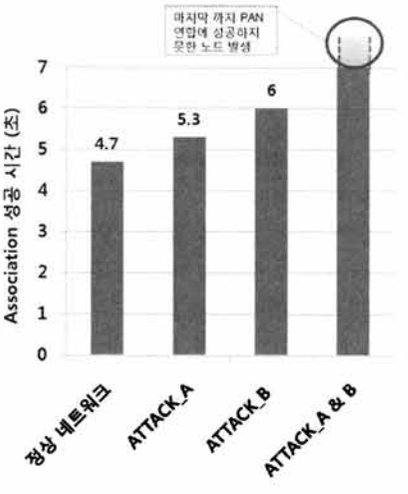
(그림 10) 공격 후 Beacon Request 전송 메시지 수



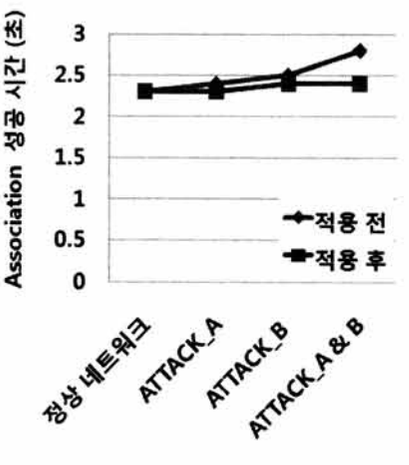
(그림 11) 디바이스의 Association 성공시간

살펴보면 정상 네트워크 내에서 디바이스들이 PAN에 연합하는 평균 시간보다 ATTACK_A, ATTACK_B와 ATTACK_A&B 슬립거부 공격이 가해졌을 때 디바이스가 PAN에 연합하는 평균 시간이 증가하는 것을 볼 수 있다. 또한 (그림 12)를 통해 각 공격이 수행되었을 경우, 디바이스가 PAN에 모두 연합을 완료하는 시간을 분석해 보면 정상 네트워크의 경우보다 ATTACK_A와 ATTACK_B의 경우 연합을 하는데 훨씬 긴 시간이 소요 되는 것을 볼 수 있다. ATTACK_A&B의 경우에는 마지막까지 PAN에 가입하지 못하고 누락되는 노드가 발생하여 정상적인 네트워크 형성이 이루어지지 못하였다.

다음으로는 3.3절에서 제안한 탐지 메커니즘을 적용하여 성능을 비교하였다. (그림 13)은 정상 네트워크와 슬립거부 공격이 발생하는 네트워크에 대해 탐지 메커니즘을 적용한 경우와 그렇지 않은 경우의 PAN 연합 평균 시간을 비교하여 분석하였다. 탐지 메커니즘을 적용한 경우에는 공격 노드 탐지 시, 그 노드를 리셋시켜 공격을 중지하도록 하였다.



(그림 12) 모든 노드 Association 완료 시간



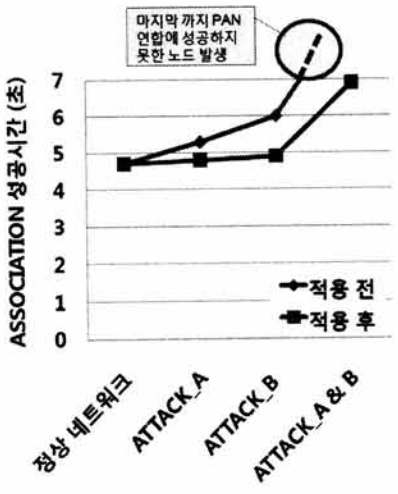
(그림 13) 탐지 메커니즘 적용 후, 노드의 Association 평균 시간 비교

실제 네트워크에서는 리프로그래밍 메커니즘[20]에 의해 정상적인 수행 코드를 원격으로 전송하여 다시 로딩하게 할 수 있다. 이를 통해서 탐지 메커니즘이 적용된 경우 정상 네트워크의 연합 평균 성공 시간과 크게 차이가 나지 않는 것을 볼 수 있다.

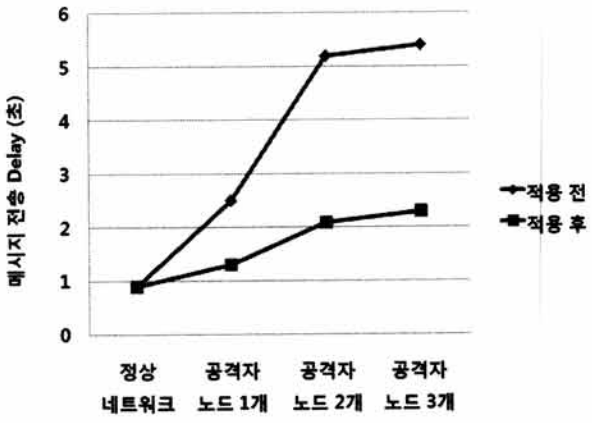
(그림 14) 역시 탐지 메커니즘을 적용하지 않은 경우와 적용 한 경우의 전체 노드의 연합 성공시간을 보여준다. 이 분석을 통해 제안한 메커니즘이 적용될 경우 공격이 발생하더라도 메커니즘 적용 전보다 더 효율적인 네트워크 운영이 가능한 것을 볼 수 있다. 메커니즘을 적용하기 전에는 ATTACK_A와 ATTACK_B를 동시에 실행하여 공격을 진행한 경우에는 아예 PAN에 가입하지 못하는 노드가 발생하였지만 메커니즘을 적용 후에는 ATTACK_A&B의 공격에도 모든 노드가 PAN에 연합하여 네트워크를 형성하고 운용된다.

정상 네트워크에서의 노드들의 센싱 값 전달은 슬립거부 공격이 시행되면 그 효율은 저하 될 수 있다. 시뮬레이션을 통하여 정상 네트워크에서의 메시지 지연 시간과 공격이 발생 했을 때의 메시지 평균 전송 지연 시간을 살펴보았다. 센싱 전달 값은 모든 노드에서 1초 주기로 센싱값을 전달하는 것으로 설정하였고, 메시지 전달의 평균 전송 지연시간을 측정하였다. 실험 결과 (그림 15)에서처럼 Association Reguest메시지에 의한 공격에 있어서 공격자 노드가 증가함에 따라 탐지 메커니즘을 적용하였을 때 그 영향이 상당이 감소되는 것을 볼 수 있다.

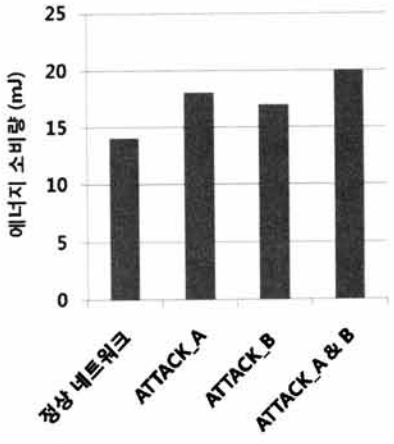
슬립거부 공격은 각 노드가 Sleep 상태로 들어가지 못하게 되므로 에너지 소모가 일반적인 네트워크 상황보다 크고 이로 인해 서비스가 제대로 작동하지 못하는 경우 또한 발생 가능하다. 팬 코디네이터의 에너지 소모량을 비교해 보면 (그림 16)에서처럼 ATTACK_A와 ATTACK_B가 수행된 경우 정상 네트워크 보다 팬 코디네이터에서 많은 에너지 소모를 하게 되고, 특히 ATTACK_A&B의 경우 가장 많은 에너지 소모가 발생한다. 지금 결과의 시뮬레이션에서는 짧은 시간 실험을 하였지만 실제 네트워크에서는 더 긴 시간 공격이 수행될 수 있으므로 이에 의한 에너지 소모는 더 클 수 있다



(그림 14) 탐지 메커니즘 적용 후 모든 노드의 Association 성공 시간



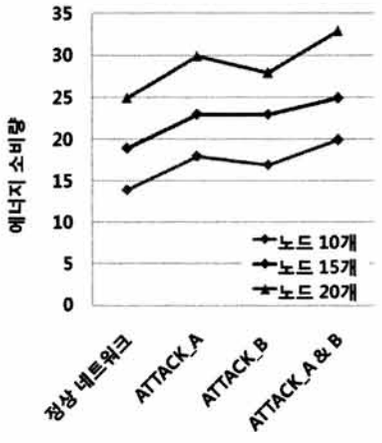
(그림 15) 공격자 노드 수 증가에 따른 센싱 지연 값



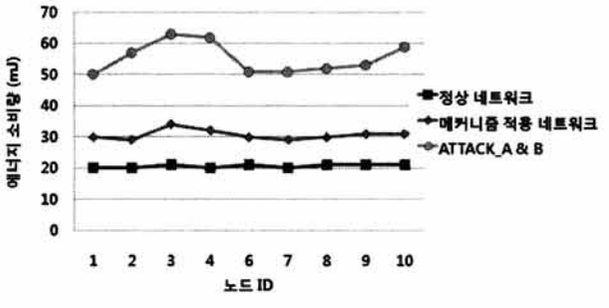
(그림 16) 코디네이터의 에너지소모량

이를 디바이스 노드 수를 증가시키며 시뮬레이션을 진행한 결과 (그림 17)과 같은 그래프가 도출되었다. 이를 통해 공격 노드가 많을수록 에너지 소비가 많아지는 것을 알 수 있고 공격으로 인한 에너지 소비의 피해도 커지는 것을 볼 수 있다. 실제 현실에서는 훨씬 많은 양의 센서 노드의 개수가 공격에 활용될 수 있으므로 실제 생활에서의 슬립거부 공격의 위험성의 심각도를 유추해 볼 수 있다.

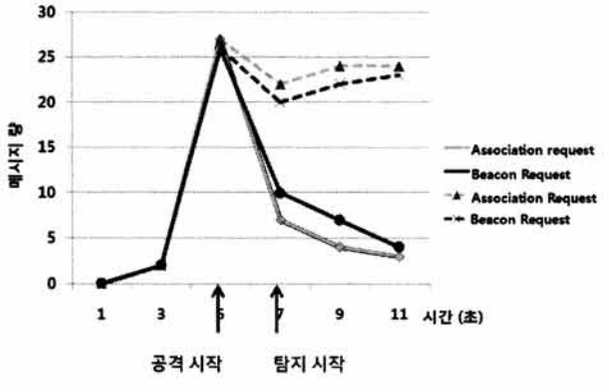
(그림 18)에서는 디바이스 노드의 에너지 소비량을 분석하였다. 정상 네트워크의 경우, 디바이스 노드의 에너지 소비량에 비하여 ATTACK_A&B의 에너지 소비량은 2배가 훨씬 넘어 각 노드의 에너지는 물론 네트워크의 전반적인 파워손실로 인한 네트워크 오류 등이 예상된다. 이에 제안한 메커니즘을 적용하면 정상 네트워크 에너지 소모량만큼 적은 에너지를 소비하지는 않지만 ATTACK_A&B공격이 시행되었을 경우보다 큰 폭으로 에너지 소비량이 감소하게 된다.



(그림 17) 노드량에 따른 코디네이터 에너지소모량



(그림 18) 노드별 에너지 소비량



(그림 19) 공격과 탐지 메커니즘에 따른 메시지 변화량

마지막으로 탐지 메커니즘을 적용한 후 공격자 노드를 탐지하고 이 공격자 노드에 대한 리셋으로 대응하는 경우, request 메시지 변화량을 살펴보았다. (그림 19)와 같이 공격이 시작되면 바로 메커니즘에 의해 공격에 의한 메시지량이 감소하는 모습을 볼 수 있다.

5. 결 론

본 논문에서는 많은 상용 센서에서 채택하고 있는 IEEE 802.15.4 표준을 분석해 보고 센서 네트워크 환경에서 가능한 슬립거부 공격에 대해 살펴보았다. 다양한 슬립거부 공격 중에서도 표준에서 제공하는 보안 서비스와 무관하게 수행 가능한 슬립거부 공격을 모델링 하여 이를 탐지할 수 있는 메커니즘을 제안하였다.

보안 서비스에 무관하게 언제든지 발생할 수 있는 슬립거부 공격 중, Association Request 메시지에 의한 연합 동작 내의 공격과 Beacon Request 메시지에 의한 능동 스캔 동작 내의 공격을 모델링하고, 이러한 공격자가 있을 경우의 노드의 소비 에너지와 네트워크의 영향에 대한 시뮬레이션을 QualNet 시뮬레이션 툴을 이용하여 수행하였다. 실험 결과를 통하여 슬립거부 공격이 이루어질 경우 네트워크 형성에 오류가 발생할 수 있고, 팬 코디네이터와 에너지 낭비는 물론 디바이스 노드조차 에너지 소모량이 증가하는 것을 알게 되었다. 또한 제안한 탐지 메커니즘을 통해 효율적인 공격 탐지가 수행 되면서 노드의 에너지의 고갈을 방지할 수 있고 네트워크의 운용에도 오류 없이 진행되는 것을 확인할 수 있었다.

참 고 문 헌

[1] IEEE Std 802.15.4, "Part 15.4:Wireless Medium Access Control(MAC) and Physical Layer(PHY) Specifications for Low-Rate Wireless Personal Area Networks(WPANs)," September, 2006.

[2] 김태연, "무선 센서 네트워크를 위한 새로운 키 사전 분배 구조", 정보처리학회논문지C, Vol.16-C, No.02, pp.0173-0188, 2009년 4월.

[3] 서재원, 김미희, 채기준, "의료 센서 네트워크에서의 효율적인 전송 구조 및 Key Provisioning을 사용한 키 관리 기법 연구", 정보처리학회논문지C, Vol.16-C, No.03, pp.0285-0298, 2009년 6월.

[4] 조관태, 김용호, 이동훈, "센서 네트워크 내의 위조된 데이터 삽입 공격 방지를 위한 인증 방법", 정보처리학회논문지C, Vol.14-C, No.05, pp.0389-0394, 2007년 8월.

[5] David Raymond, Randy Marchany, Michael Brownfield, Scott Midkiff., "Effects of Denial of Sleep Attacks on Wireless Sensor Network MAC Protocols," Proc. 7th Ann. IEEE Systems, Man, and Cybernetics (SMC) Information Assurance Workshop (IAW), IEEE Press, pp.297-304, 2006.

[6] "QualNet 4.5 Product Tour," http://www.scalable-networks.com, Dec., 2006.

[7] Wenyuan Xu, Ke Ma, Wade Trappe, Yanyong Zhang, "Jamming sensor networks: attack and defense strategies," Network, IEEE, Vol.20, No.3, pp.41-47, 2006.

[8] Wenyuan Xu, Wade Trappe, Yanyong Zhang, Timothy Wood, "The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks,"Proc. 11th Ann. Int'l Conf. Mobile Computing and Networking, ACM Press, pp.46-57, 2005.

[9] Wenyuan Xu, Timothy Wood, Wade Trappe, Yanyong Zhang, "Channel surfing and spatial retreats: defenses against wireless denial of service," 3rd ACM workshop on Wireless security, pp.80-89, 2004.

[10] W. Ye, J. Heidemann, D. Estrin, "Medium Access Control with Coordinated Adaptive Sleeping for Wireless Sensor Networks,"IEEE/ACM Trans. Networking, Vol.12, No.3, pp.493-506, 2004.

[11] J. Polastre, J. Hill, D. Culler, "Versatile Low Power Media Access for Wireless Sensor Networks," 2nd ACM Int'l Conf. Embedded Networked Sensor Systems, ACM Press, pp.95-107, 2004.

[12] T. VanDam, K. Langendoen, "An Adaptive Energy-Efficient MAC Protocol for Wireless Sensor Networks," 1st ACM Int'l Conf. Embedded Networked Sensor Systems, ACM Press, pp.171-180, 2003.

[13] David R. Raymond, Scott F. Midkiff, "Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses," IEEE Pervasive Computing, Vol.7, No.1, pp.74-81, 2008.

[14] John Paul Walters, Zhengqiang Liang, Weisong Shi, Vipin Chaudhary "Wireless Sensor Network Security: A Survey," Security in Distributed, Grid, and Pervasive Computing, Auerbach Publications, CRC Press, 2006.

[15] Misic, V.B., Fang, J., Misic, J., "MAC layer security of 802.15.4-compliant networks," Proc. of IEEE International Conference on Mobile Adhoc and Sensor Systems Conference, 2005.

[16] Neal Patwari, Alfred O. HeroIII, Matt Perkins, Neiyer S. Correal and Robert J.O'Dea, "Relative Location Estimation in Wireless Sensor Networks," IEEE TRANSACTIONS ON SIGNAL PROCESSING 2002.

[17] Neal Patwari, Alfred O. Hero III, "Demonstration Distributed Signal Strength Location Estimation," ACM SenSys 2006.

[18] L. Sang and A. Arora, "Spatial signatures for lightweight security in wireless sensor networks," IEEE INFOCOM, pp.2137-2145, April, 2008.

[19] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-telepathy: extracting a secret key from an unauthenticated wireless channel," ACM MobiCom, pp.128-139, 2008.

[20] P. J. Marron, M. Gauger, A. Lachenmann, D. Minder, O.Saukh, and K. Rothermel, "Flexcup: A flexible and efficient code update mechanism for sensor networks," European Workshop on Wireless Sensor Networks (EWSN), 2006.

김 아 름

e-mail : reumreum@ewhain.net
2006년 중앙대학교 정보시스템학과(학사)
2009년 이화여자대학교 컴퓨터공학과 석사
관심분야 : 센서네트워크 보안, 침입탐지 및 대응기술

김 미 희

e-mail : iceblueee@gmail.com
1997년 이화여자대학교 전자계산학과(학사)
1999년 이화여자대학교 컴퓨터학과(석사)
1999년~2003년 한국전자통신연구원 연구원
2007년 이화여자대학교 컴퓨터공학과(박사)
2007년~2009년 이화여자대학교 컴퓨터공학과 전임강사
2009년~현 재 미국 North Carolina State University Postdoc Researcher
관심분야 : 무선 네트워크(센서네트워크, 유비쿼터스네트워크, 메쉬네트워크) 보안, 물리계층 보안

채 기 준

e-mail : kjchae@ewha.ac.kr
1982년 연세대학교 수학과(학사)
1984년 미국Syracuse University 컴퓨터학과(석사)
1990년 미국 North Carolina State University 컴퓨터공학과(박사)
1990년~1992년 미국 해군사관학교 컴퓨터학과 조교수
1992년~현 재 이화여자대학교 컴퓨터공학과 교수
관심분야 : 네트워크 보안, 인터넷/무선통신망/고속통신망/센서네트워크 (보안)프로토콜 설계 및 성능분석