Journal of The Korea Institute of Information Security & Cryptology(JKIISC) ISSN 1598-3986(Print)
VOL.23, NO.3, June 2013 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2013.23.3.459

멀티 홉 UWSN 환경에서의 μTESLA 운영에 관한 고찰*

최 진 춘,[1†] 강 전 일,[1] 양 대 헌,[1] 이 경 희[2‡]
[1]인하대학교, [2]수원대학교

Study of Operating μTESLA in Multi-hop Unattended WSN*

JinChun Choi,[1†] Jeonil Kang,[1] DaeHun Nyang,[1] KyungHee Lee[2‡]
[1]INHA University, [2]The University of Suwon

요 약

μTESLA는 WSN(Wireless Sensor Network)에서 대표적인 에너지 효율적 브로드캐스트 인증 방법이다. 지금까지 μTESLA의 문제점을 파악하고 이를 해결한 많은 연구들이 존재하지만, 그들 대부분은 자신들의 성능 입증을 위해 현실과는 거리가 먼 실험 환경에서 검증되었다. 우리는 현실에서 실제 WSN을 사용할 법한 실험 환경을 가정하고 이 바탕 위에서 μTESLA가 가진 실체적인 성능에 대해서 고찰해볼 필요가 있다고 생각하였다. 이 논문에서는 BS가 네트워크에 상주하지 않는 UWSN(Unattended WSN) 환경에서 동면과 활동을 반복하는 센서 노드들이 멀티 홉으로 통신을 수행하는 경우를 가정하였다. 이러한 환경에서 우리는 다양한 모의실험을 통하여 μTESLA의 성능을 새로이 검증 및 분석하였다.

ABSTRACT

μTESLA is well known as the most representative energy-efficient broadcast authentication method. Until now, there are many researches that figure out the problems or limitation of μTESLA and mitigate or solve them, but most researches have been verified in the environment far from the real world. We consider the necessity of verifying what the real efficiency of μTESLA is. In this paper, we assume that sensors that continuously repeat hibernation and activity perform communication under the UWSN(Unattended WSN), which BS does not stay in the network. In this environment, we newly inspect the performance of μTESLA by performing various simulations.

Keywords: Unattended Wireless Sensor Network, broadcast message authentication, μTESLA, NS-2

I. 서 론

WSN(Wireless Sensor Network)은 작은 크기의 무선 센서 노드들로 구성된 네트워크로 각각의 센서 노드는 무선 통신이 가능한 통신 모듈과 작은 크기의 메모리, 저 전력으로 운영되는 마이크로 컨트롤러를 가지고 있다. 또한 주변의 데이터를 수집할 센서 모듈을 장착하고 있다. WSN에서 중요한 문제 중 하나는 센서 노드의 수명이다. 효율적으로 WSN을 구성하고 운영하기 위해서는 필연적으로 센서 노드의 수명을 최대한 오래 유지하면서 성능의 저하는 피하는 기법을 개발해야 한다.

WSN에서 배치된 센서 노드들이 수집한 데이터를 수집하는 과정에서 브로드캐스트 메시지가 발생하게 된다. 이러한 브로드캐스트 메시지는 무결성이 요구되는데 이는 암호화 되거나 인증되지 않은 메시지를 네트워크 내의 센서 노드들에게 전송하는 악의적인 사용자가 있을 수 있기 때문이다[1]. 따라서 브로드캐스트 메시지의 무결성을 유지하기 위한 여러 가지 방법들

접수일(2013년 2월 18일), 수정일(2013년 4월 8일), 게재확정일(2013년 4월 18일)
* 이 논문은 인하대학교의 지원에 의하여 연구되었음.
† 주저자, noodlejin@isrl.kr
‡ 교신저자, khlee@suwon.ac.kr(Corresponding author)

중 하나로 비 대칭키 암호 방식을 구현함으로써 메시지의 무결성을 제공할 수 있다.

브로드캐스트 메시지 인증의 한 방법으로 TESLA[2]를 이용할 수 있다. 하지만 일반적으로 사용되는 TESLA의 경우는 WSN환경을 고려하지 않기 때문에 저 전력으로 운영되는 센서 노드에서는 사용하기에 적합하지 않다. 따라서 WSN 에서는 센서 노드를 위해 구현된 μTESLA[3]를 이용한다.

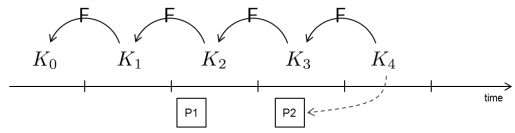
μTESLA는 기본적으로 BS와 센서 노드가 전부 1홉으로 연결되어 있는 네트워크 상황을 고려하여 작성된 방식이다. 그들의 논문에서 멀티 홉 또한 동작할 수 있다고 하였지만, 그 효율성 및 성능은 검증된 적이 없었다. 또한 μTESLA는 기본적으로 BS(Base Station)가 항상 네트워크에 존재하여 짧은 슬롯을 가지고 키를 노출시키는 것을 가정하기 때문에, UWSN(Unattended Wireless Sensor Network)[4]와 같이 네트워크에서 BS가 존재하지 않고 일정 주기마다 네트워크를 방문하여 센서 노드들이 수집한 데이터를 취합해 가는 방식에서는 효율적인 동작을 보장할 수 없을지도 모른다.

본 논문의 구성은 다음과 같다. 2장에서는 브로드캐스트 메시지 인증 기법, WSN에서 사용되는 라우팅 프로토콜에 관련된 연구들에 대해 알아본다. 3장에서는 멀티 홉 μTESLA 환경과 응용 가능한 시나리오에 대해 설명한다. 4장에서는 모의실험에 이용한 센서 모델과 환경 구성에 대해 알아본다. 5장에서는 시뮬레이션 수행 결과로 μTESLA의 운영에 있어 다양한 환경 변수의 변화에 따라 소비되는 전력량과 가용율을 분석한다. 6장에서는 시뮬레이션 수행 결과로 알 수 있는 예측 운용 가능 시간과 적정 노드 분포 수에 대한 토의를 한다. 마지막으로 7장에서는 결론을 맺는다.

II. 관련 연구

2.1 μTESLA

μTESLA는 센서 노드와 BS사이에 브로드캐스트 메시지를 인증하기 위한 비 대칭키 기반의 인증 기법이다. 기존의 TESLA가 전자 서명 기반으로 동작했던 것과 달리 μTESLA에서는 [그림 1]처럼 해시 함수로 생성되는 키 체인을 이용하여 상호간에 시간이 동기화된 노드들의 대칭키의 노출을 지연시키는 방법을 통해 비 대칭키 암호를 구현하였다. 이렇게 구현된



[그림 1] 키 체인을 이용한 μTESLA의 구현

μTESLA는 주변의 센서 노드들에게 메시지를 보낼 때 메시지와 함께 키 체인에서 생성된 키를 이용하여 MAC(Message Authentication Code)을 붙여서 전송하게 된다. 이러한 방법을 적용할 때, 브로드캐스트 메시지와 해당 브로드캐스트 메시지를 인증할 수 있는 키를 보내는 시간 간격인 키 슬롯의 길이와 메시지를 인증하는 시간과의 트레이드 오프 관계가 생기게 된다. 즉 키 슬롯을 짧게 만들면 키를 검증하는데 걸리는 시간이 오래 걸리게 되며 많은 키를 소모하게 된다. 하지만 메시지 검증을 하는 시간은 빨라진다. 반대로 키 슬롯을 길게 만든다면 키를 검증 하는 시간은 짧아지지만 메시지 검증시간이 느려져서 네트워크의 반응성이 느려진다고 볼 수 있다. 따라서 네트워크의 반응성과 네트워크의 수명을 고려하여 그에 맞는 적절한 길이의 키 슬롯을 설정하는 것이 중요하다.

2.2 GAF, GPSR

이 논문에서 구현한 시나리오에 사용된 라우팅 기법은 다음과 같다. 먼저 GAF(Geographical Adaptive Fidelity)[5]는 기본적으로 노드들의 전력 소모를 최소화 하기위해 정사각형으로 그리드(grid)를 구성한다. 각 센서 노드들은 각각 센서 노드들이 배치된 가상의 그리드 공간에서 액티브(active) 노드를 선정하고, 수집한 데이터를 액티브 노드에게 전송하며 액티브 노드는 센서 노드들의 데이터를 취합한다. 이때 그리드 간에 안정적인 통신이 이루어지기 위해서는 노드의 통신 반경을 R 이라 하면, 그리드의 한 변의 길이는 $R/\sqrt{5}$ 이하가 되어야 한다. 이것은 서로 다른 그리드 안의 액티브 노드와 통신이 안정적으로 이루어지기 위한 조건이다. 하지만 본 논문에서 구현한 것은 기존의 GAF가 아니라 시나리오에 맞게 변형된 GAF라고 볼 수 있다. 원래 GAF에서처럼 하나의 그리드 안에 하나의 액티브 노드가 존재하며 항상 운영되는 것이 아니라, 노드들 간에 주변 탐색 과정을 통해 CH(Cluster Header)를 선정하고 CH가 취합한 데이터를 BS에게 보낼 때에는 GPSR(Greedy Perimeter Stateless Routing)[6]을 이용하여

BS까지 전달하는 것이다. GPSR은 시작 노드로부터 BS에 가장 가까운 센서 노드로 데이터를 전달하는 방식이다. 센서 노드는 자신의 위치와, 주변 탐색 과정을 통해 주변 센서 노드의 식별자와 물리적 위치를 알고 있다고 가정한 상태에서 사용되는 프로토콜이다. 이 라우팅 프로토콜은 메시지를 전달함에 있어 Greedy Forwarding과 Perimeter Forwarding 규칙을 따른다. Greedy Forwarding은 메시지를 보내는 노드가 자신의 주변 노드 중에서 목적지 노드와 가장 가까운 노드에게 메시지를 전달한다는 규칙이고, Perimeter Forwarding은 만약 메시지를 보내는 센서 노드 자신이 해당 목적지 센서 노드와 가장 가깝지만 자신의 주변 노드에 해당 목적지 센서 노드가 없는 경우에는, 무조건 자신과 목적지 센서 노드를 기준으로 왼쪽에서 가장 멀리 있는 센서 노드에게 전달하는 규칙이다. GPSR은 이 두 가지의 규칙 중에서 Greedy Forwarding을 먼저 수행하고 만약 이것이 실패한다면 Perimeter Forwarding을 수행하는 과정을 반복하면서 메시지를 목적지 센서 노드까지 전달한다. 만약 센서 노드의 밀도가 충분히 촘촘하게 네트워크에 분포되어 있다면 거의 Greedy Forwarding으로 메시지 전달이 가능할 것이며, 이것은 일직선에 가까운 최적의 경로이다. 그러나 물리적으로 센서 노드가 충분히 배치되지 않은 경우에는 Perimeter Forwarding을 통해 메시지를 전달하게 된다.

III. 멀티 홉 UWSN 환경에서의 μTESLA

3.1. 멀티 홉 UWSN 환경

실제 환경에서 사용되는 WSN을 보면 데이터를 수집하기 위해 센서 노드들을 배치하고, 수집된 데이터를 취합하여 사용하기 위해 BS를 배치하는 경우가 많다. 이와 달리 UWSN의 경우는 센서 노드들을 배치하여 데이터를 수집하는 것은 같지만 BS가 네트워크 내에 센서 노드들과 계속 같이 있는 것이 아니라, 일정 주기마다 센서 노드들이 배치된 네트워크를 방문하여 센서 노드들이 수집한 데이터를 수거한 뒤 네트워크를 떠나가는 방식으로 동작한다[7]. 이와 같은 UWSN에서 BS와 여러 홉 떨어진 거리에 노드들이 배치되어 있는 경우, 센서 노드들은 수집한 데이터들을 곧바로 BS에게 전송할 수가 없다. 이를 해결하기 위해서는 여러 가지 방법이 있을 수 있지만 이 논문에서는 GAF를 이용하여 센서 노드들을 그리드로 나눠서 배치된 노드들 중 그리드마다 CH를 선정하고, GPSR을 이용하여 CH가 수집한 데이터를 BS까지 정상적으로 전달하게끔 하였다.

3.2. 센서 노드의 동면

많은 WSN의 응용환경에서 센서 노드들은 에너지 소비를 줄이고 더 오랫동안 활동할 수 있도록 동면(hibernation)과 활동(activity) 상태를 오간다고 가정하는 경우가 많다. 이는 센서가 항상 무언가를 감지할 필요가 없는 경우 좋은 에너지 관리 전략이라고 볼 수 있을 것이다. 그러나 이러한 에너지 관리 전략은 많은 프로토콜과 운용 기법 등에서 무시되는 경향이 있다. 그것은 센서 노드의 동면 때문에 해당 프로토콜의 동작이 보장받지 못하는 경우가 많기 때문이다.

μTESLA의 경우 또한 센서 노드의 동면은 여러 가지 추가적인 이슈를 불러일으킬 수 있다. 예를 들어, 키의 업데이트가 센서 노드의 동면으로 인하여 되지 않았을 경우, 새로운 키를 검증하기 위해 소모되는 시간이 다른 센서 노드보다 더 오래 걸릴 수 있다. 키를 검증하는 데 걸리는 시간 동안 센서 노드는 다른 어떠한 일도 할 수 없으므로, 키 슬롯의 길이는 이러한 키 검증 시간을 고려하여 결정되어야 한다.

3.3. 실제 응용 가능 시나리오들

실제 환경에서 센서 노드의 동면을 가정한 멀티 홉 UWSN을 활용할 수 있는 시나리오는 다음과 같다.

- 터널 안전성 검사: 터널 내에 센서 노드들을 배치하여 터널의 안전성을 체크할 수 있는 각종 데이터들을 수집하여 저장하고, BS는 주기적으로 이 터널을 지나가면서 센서 노드들이 저장하고 있는 데이터들을 취합하여 안전성 분석에 사용할 수 있다.
- 다리 안전성 검사: 각종 교통수단이나 사람이 왕복하는 다리에 미리 센서 노드들을 배치한 후, 다리의 진동 세기나 다리 주변의 습도, 온도 등의 데이터를 수집하여 다리에 미치는 영향을 분석할 수 있다. 이렇게 센서 노드들이 수집한 데이터를 BS가 수거하여 다리 안전성 검사에 사용할 수 있다.
- 도로 상태 검사: 평소 차량의 통행량이 많아 유지보수가 필요한 도로에 미리 센서 노드를 설치해 둔 뒤에 센서 노드를 이용하여 차량 통행량,

도로에 전해지는 진동 세기 측정, 도로에 영향을 주는 온도, 습도 등의 데이터를 측정할 수 있다. 주기적으로 BS를 도로에 보내서 센서 노드들이 수집한 데이터를 취합하여 나중에 도로 건설에 참고할 데이터로 사용하거나, 현재 사용 중인 도로의 유지보수 등에 사용할 수 있다.

이러한 센서 노드들이 수집한 데이터들을 BS가 안전하게 수집하기 위해서는 WSN에 맞는 안전성과 센서 노드의 수명을 고려한 브로드캐스트 메시지 인증 기법이 필요하다.

3.4 안전하지 않은 μTESLA의 운용

멀티 홉 UWSN 환경에서 μTESLA를 운용하는 경우 다음과 같은 문제점이 있다. BS가 브로드캐스트 해 주는 메시지를 센서 노드가 인증하여 신뢰하기 이전에 받은 메시지를 플러딩 하는 방식으로 구현하는 경우, BS가 브로드캐스트 메시지에 대한 TESLA 키를 보내주기 이전에는 BS가 올바른 메시지를 전송한 것인지 신뢰할 수 없는 메시지를 다른 센서 노드들에게 브로드캐스트 해줘야 한다는 문제점이 있다. 만약 센서 노드가 BS로부터 받은 브로드캐스트 메시지를 바로 플러딩 하지 않고 TESLA 키를 받아서 메시지를 인증한 이후에 플러딩 한다면 다른 센서 노드들에게 보내는 메시지는 신뢰할 수 있는 메시지가 아니라 이미 공개된 TESLA 키를 이용해 만든 메시지이기 때문에 악의적인 사용자가 임의로 생성해 낸 메시지일 수도 있다. 따라서 TESLA 키가 공개된 이후에는 해당 키로 생성한 메시지는 신뢰할 수 없게 된다.

IV. 모의실험

4.1 실험 환경

이 논문에서는 NS-2(버전 2.29)를 이용하여 실험을 수행하였고, 실험 환경의 구체적인 설정과 방법은 다음과 같다.

4.1.1 센서 모델

실험에 적용한 센서 모델은 MICAz[8]로 가정하고, MICAz의 성능을 시뮬레이션에 적용하였다. MICAz는 크게 마이크로 컨트롤러인 ATmega 128L[9]과 통신 모듈인 CC2420[10]으로 구성되어 있다. ATmega128L의 상태는 센서 노드가 수행하는 일에 따라 동면 모드(hibernation mode), 휴식 모드(idle mode), 활동 모드(active mode)로 변하게 된다. 동면 모드는 센서 노드가 외부의 신호로는 반응하지 못하고, 내부 명령이나 스케줄에 따라서 휴식 모드 로 변할 수 있다. 휴식 모드는 수면 모드(sleep mode)의 한 종류로 동면 모드와는 다르게 외부 신호나 내부 인터럽트로 상태를 바꿀 수 있다. 휴식 모드에서는 동면 모드나 활동 모드로 상태를 바꿀 수 있다. 휴식 모드에서는 4.125mA 의 전류를 사용한다. 활동 모드는 센서 노드에서 해시 함수 수행 등의 동작을 할 때 사용하는 상태이다. 활동 모드에서는 8.3 mA 의 전류를 사용한다. 이는 Krämer 등의 실험에서[11][12] ATmega128L의 실제 측정된 값을 고려할 때 적절하다고 볼 수 있다.

CC2420은 일반적으로 수신 모드(receive mode)와 전송 모드(transmit mode)로 동작하는데, 수신 모드 에서는 19.7mA 의 전류를 사용하고, 전송 모드에서는 전파 반경에 따라 소모하는 전류가 다르다.

4.1.2 시뮬레이션 환경 구성

이 논문에서는 NS-2를 이용하여 시뮬레이션을 구현하였다. 시뮬레이션 동작 과정에서 센서 노드가 취합한 데이터를 전송할 때, 일정 크기 이상의 데이터는 정상적으로 전송되지 못하는 것을 발견하고 이를 해결하기 위해 데이터 분할을 구현하였다. 또한, 유니캐스트 메시지 전송 후에 메시지가 정상적으로 도착하였을 경우에 수신한 센서 노드에서 ACK 메시지를 전송하도록 구현하였다. 그리고 GAF에서 필요한 그리드의 크기는 10m로 구성하였고, 하나의 그리드 당 4개의 노드가 포함될 수 있도록 노드의 수를 설정하였다. 그리고 이 실험에서는 센서 노드의 통신 반경을 15m로 설정하였는데, 이 통신 반경에 맞는 dBm을 구하기 위해 자유 공간 신호 감쇠 모델(Free Space Propagation Loss Model)을 사용하여 계산하였다. d가 거리(=15m), f가 주파수(=2.4×10^9 Hz), c가 빛의 속도(=2.99792485×10^8m/s)일 때, 자유 공간 신호 감쇠 $FSPL$은

$$FSPL=\left(\frac{4\pi df}{c}\right)^2=\frac{P_t}{P_r}=2277106 \quad (1)$$

와 같다. 여기서 P_t는 송신 전력 세기, P_r은 수신 전

〔표 1〕 WSN에서 해시 함수의 수행시간을 계산하기 위한 α와 β값 및 블록 사이즈

해시 알고리즘	α	β	block size(bits)
MD5	203656	86298	512
SHA-1	60980	458660	512

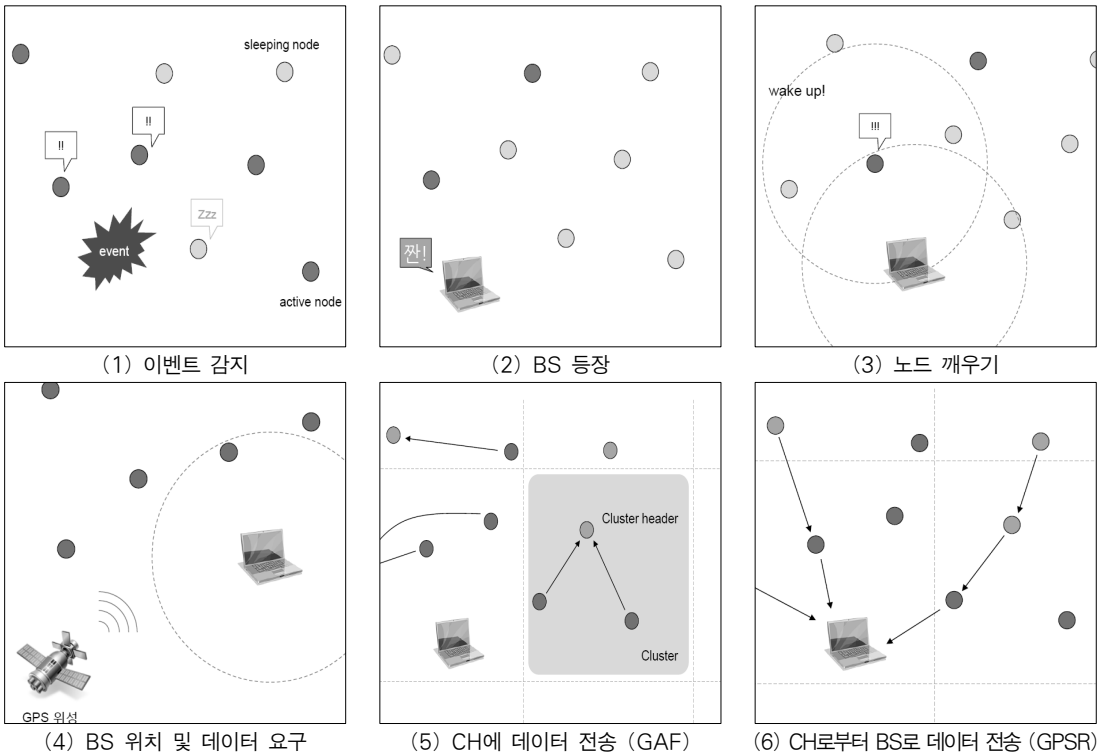
력 세기와 같다. CC2420의 수신 가능 전력 세기 P_r은 -95dBm($=3.1623\times10^{-13}$W)이상이어야 하므로 P_t는 -31.43dBm($=7.2008\times10^{-7}$W)이상이면 된다. CC2420 규격 문서를 보면 최소 -25dBm로 전파를 송출할 수 있는데, 이 때, 소모되는 전력은 15.3 mW($=8.5$mA$\times1.8$V)이다.[1)]

통신 반경을 30m, 45m로 하였을 때에도 위의 공식을 이용하여 계산하면 각각 -25.41dBm과 -21.88 dBm으로 구할 수 있다. 이때, 송신 전력 세기는 공히 17.82mW($=9.9$mA$\times1.8$V)로 하였다.[2)]

또한, μTESLA에서 BS가 보낸 TESLA 키를 인증할 때 HMAC을 사용하는데, WSN에서 해시 함수의 수행시간을 계산하기 위해서는 다음과 같은 공식을 이용한다〔13〕.

$$t_{exec} = \frac{a+\beta\times[tlen/bsize]}{procFreq\times bus\,Width} \quad (2)$$

여기서, $tlen$은 입력의 텍스트의 길이이며, $bsize$는 해당 함수의 블록 사이즈, $procFreq$는 프로세서의 클록 수, $bus\,Witdh$는 프로세서의 버스 크기이다. 〔표 1〕의 상수값 α,β와 block size 값을 대입하고, ATmega128L 의 스펙을 입력하면 다음과 같은 결과를 얻을 수 있다. SHA-1의 경우 0.008119초, MD5의 경우 0.004531초를 각각 얻을 수 있다.



(1) 이벤트 감지 (2) BS 등장 (3) 노드 깨우기

(4) BS 위치 및 데이터 요구 (5) CH에 데이터 전송 (GAF) (6) CH로부터 BS로 데이터 전송 (GPSR)

〔그림 2〕 모의실험을 위한 시나리오 주요 구성

1) CC2420은 마이크로프로세서와의 통신에는 3V를 이용하지만 그 외의 동작에는 1.8V를 사용한다.
2) CC2420의 송출 전력 세기를 8 단계로 조절할 수 있는데, -15dBm 다음은 -25dBm이어서 이 둘을 구별하도록 전력을 조절할 수는 없다.

4.2 최선의 시나리오 구성

이 논문에서는 멀티 홉 UWSN 환경에서 μTESLA를 이용하여 BS가 일정 주기마다 네트워크에 방문하여 데이터를 취합해 가는 상황을 모델링하여 〔그림 2〕와 같은 시나리오를 설정하였다.

이러한 시나리오에 기반 하여 구현한 시뮬레이션의 동작은 다음과 같다.

- 센서 노드들은 일정한 공간에 배치되어 있고, 각각의 센서 노드들은 주변 센서 노드를 탐색하는 메시지를 브로드캐스트 하여 1홉 이내에 있는 센서 노드들의 리스트를 저장, 관리한다.
- 주변 센서 노드 탐색이 끝난 센서 노드들은 각자 정해진 스케줄에 따라 휴식 상태와 동면 상태를 반복하게 된다. 동면 모드를 유지하는 시간은 키 슬롯보다 작게 설정하여 노드가 Wake up 메시지를 놓치지 않고 전송 받도록 설정한다.
- 특정 시간에 데이터를 수집해 가기 위해 BS가 네트워크에 등장하고 노드들의 상태를 휴식 모드로 바꾸기 위해 Wake up 메시지를 브로드캐스트 하게 된다. 이 메시지를 받은 센서 노드들은 플러딩을 통해 주변 노드들에게 전파하게 된다. 센서 노드는 이 메시지를 받은 후 바로 동면을 중단하는 것은 아니며 이후 지정된 키 슬롯이 지난 후에 μTESLA 키를 받은 뒤 활동 모드로 상태를 전환하고 이전에 받은 Wake up 메시지를 인증한다. 이러한 과정을 성공적으로 마친 센서 노드는 휴식 모드로 전환하여 대기하게 된다.
- BS는 키 슬롯 시간만큼 TESLA 키를 보내고, 센서 노드들이 휴식 모드로 바뀐 후에는 센서 노드가 수집한 데이터를 BS로 전송할 것을 요청하는 메시지를 브로드캐스트로 보낸다. 센서 노드들은 BS에게서 받은 브로드캐스트 메시지를 다른 주변 센서 노드들에게 전파하고 BS는 키 슬롯만큼의 시간이 지난 후 브로드캐스트한 메시지에 대한 TESLA 키를 보낸다. 센서 노드들은 TESLA 키를 받아서 플러딩 해준 뒤 메시지를 인증한다.
- 데이터 전송 메시지를 정상적으로 수신하고 BS로부터 TESLA 키를 받아 메시지를 인증한 후에 센서 노드들은 각 센서 노드별로 그리드를 구성하고, CH를 결정하여 수집한 데이터를 CH에게 전달한다. CH는 그리드 내의 센서 노드들이 보내준 데이터를 취합하여 GPSR을 이용하여 최단거리로 BS에게 전송한다.
- BS에서 데이터 취합이 끝난 후에는 센서 노드들에게 Bye 메시지를 브로드캐스트 하여 휴식 모드였던 센서 노드들을 동면 모드로 전환시킨다. 이 역시 Bye 메시지를 받은 센서 노드들은 바로 동면 모드로 전환되지 않고 일단 주변 센서 노드들에게 플러딩을 해준다. 키 슬롯 시간이 지난 후에 BS는 이전에 보낸 Bye 메시지에

〔표 2〕 성능 분석을 위해 설정한 환경 변수 값

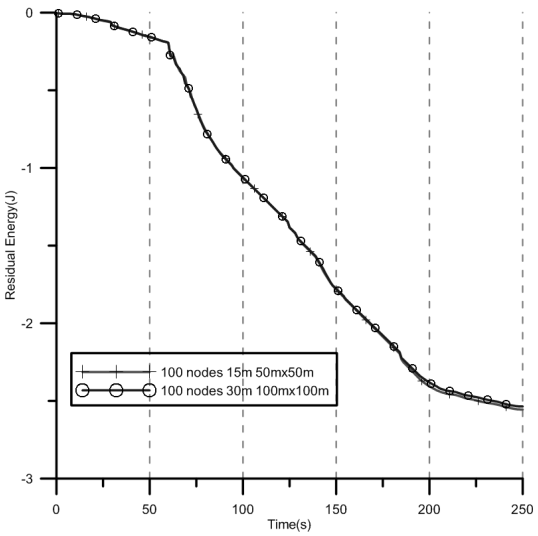
환경 변수	설명	값
통신 반경	노드와 노드, BS와 노드간의 최대 통신 거리	15m, 30m, 45m
해시 함수	HMAC 또는 μTESLA 키 검증에 사용하는 암호학적 해시 함수	SHA-1, MD5
센서 노드의 수	전체 네트워크 내의 센서 노드 수	100개, 400개, 900개
키 슬롯 길이	μTESLA의 슬롯 길이	30초
그리드 크기	GAF 적용을 위한 면적 크기	10m x 10m, 20m x 20m, 30m x 30m
클러스터 헤더 선정 방법	그리드 안에서의 클러스터 헤더 선정 방법	BS 근접 우선, (무작위, 에너지 우선)
노드 분포	네트워크 내에 노드 분포 방법	무작위,(격자)
네트워크 크기	노드가 분포하는 영역의 크기	50m x 50m, 100m x 100m, 150m x 150m
동면/활동 주기	노드가 동면과 활동 상태를 전환하는 주기	동면 : 15~20초, 활동 : 5초
센서 노드의 밀도	네트워크를 구성하는 각각의 그리드 내의 노드 수(센서 노드의 수와 그리드 크기에 대한 종속 변수)	1개, 2개, 2.5개, 3개, 4개 / 그리드

대한 TESLA 키를 보내주고 이것을 받은 센서 노드는 주변 센서 노드들에게 플러딩을 해준 뒤 이전에 받은 Bye 메시지를 인증한다. 인증이 성공하여 정상적인 메시지로 확인된 후에는 센서 노드들은 정해진 스케줄에 따라 동면 상태와 휴식 상태를 반복하게 된다.

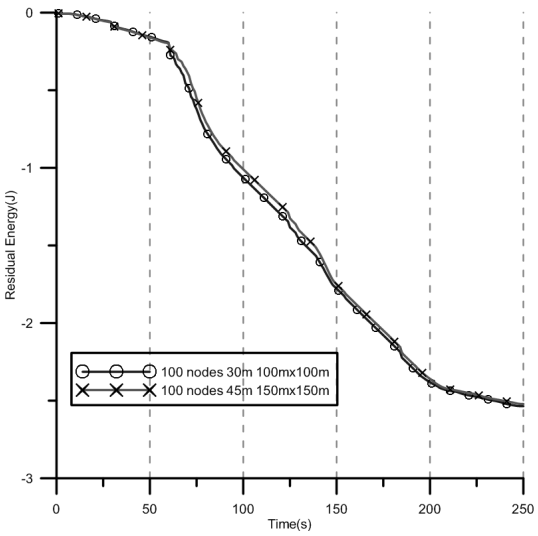
불행하게도 이러한 시나리오는 앞서 설명한 것과 같이 어쩔 수 없는 메시지 플러딩 때문에 BS인척 무작위로 메시지를 보내는 공격자에게 안전하지 못하다. 그러나 이 이외에 멀티 홉에서 μTESLA를 작동시킬 수 있는 방법은 존재하지 않는다.

V. 실험 수행 및 그 결과

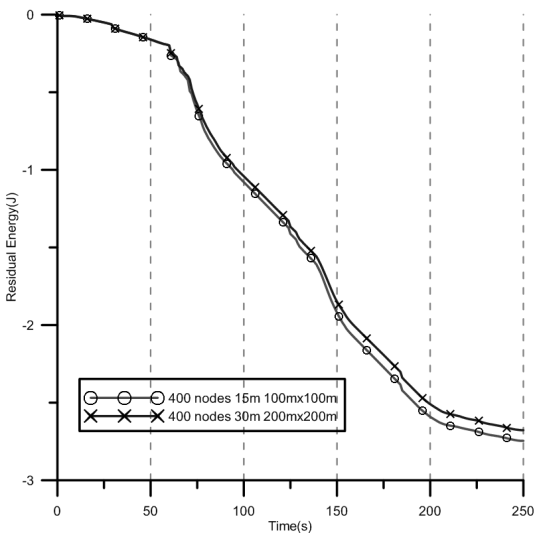
μTESLA의 성능을 평가하기 위해서는 먼저 〔표 2〕와 같은 환경 변수에 대한 정의가 필요하다. 이 논문에서 구현한 시뮬레이션에 적용한 환경 변수는 다음과 같다. 먼저 통신 반경을 15m, 30m, 45m 로 변경



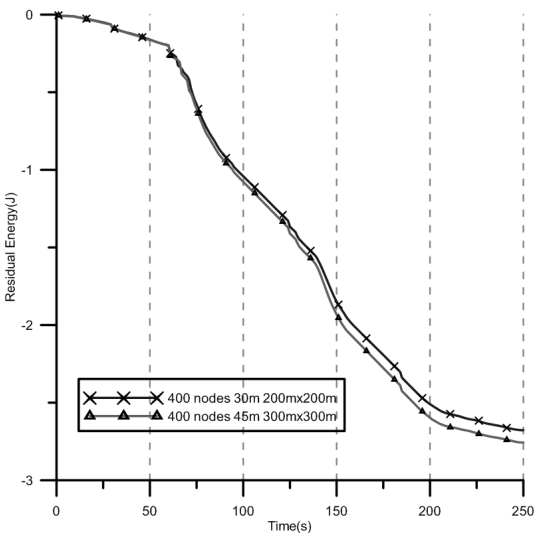
〔그림 3〕 100개의 센서 노드에서 통신 반경을 15m, 30m 으로 하였을 경우



〔그림 4〕 100개의 센서 노드에서 통신 반경을 30m, 45m 으로 하였을 경우



〔그림 5〕 400개의 센서 노드에서 통신 반경을 15m, 30m 으로 하였을 경우

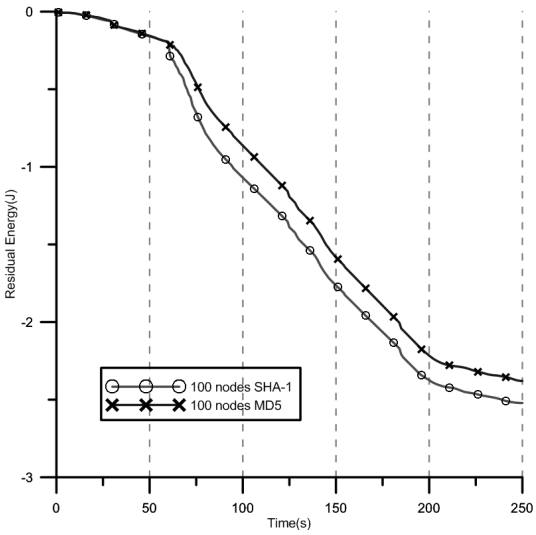


〔그림 6〕 400개의 센서 노드에서 통신 반경을 30m, 45m 으로 하였을 경우

하면서 그에 따라 네트워크의 토폴로지 크기와, 그리드의 크기도 맞게 변경해 주었다. 그리고 μTESLA에서 사용하는 해시 함수의 종류에 따라 달라지는 잔류 에너지양을 측정하였다. 또한 센서 노드의 개수를 각각 100개, 400개, 900개로 다르게 하면서 네트워크 크기를 그에 맞게 변경한 후 측정된 결과를 볼 수 있다. 마지막으로 같은 네트워크 크기에서 하나의 그리드 안에 포함되는 센서 노드의 개수, 즉 네트워크 내의 센서 노드의 밀도를 각각 그리드 1개 안에 센서 노드가 1개, 2개, 2.5개, 3개, 4개 포함될 때에 따라 변하는 센서 노드의 가용율과 잔류 에너지양을 보였다. 가용율(Availability)은 센서 노드의 밀도가 달라질 때 네트워크 내의 센서 노드가 Wake up 되는 비율을 말한다. 또한 측정된 잔류 에너지양은 실험에 참여한 모든 센서 노드들의 평균값을 계산하였다.

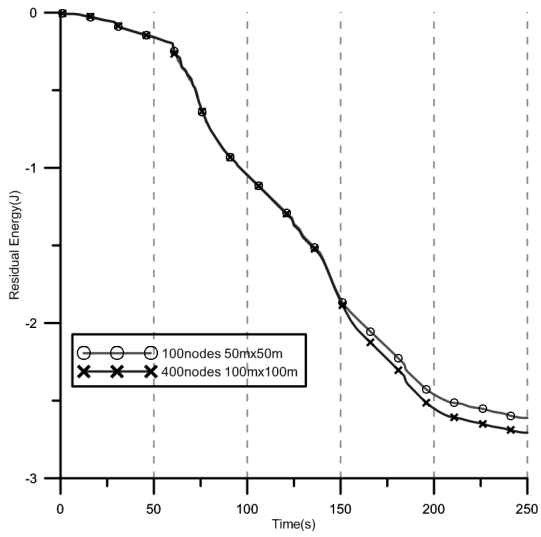
5.1 통신 반경의 차이

센서 노드의 수는 100개로 유지하면서 센서 노드의 통신 반경을 15m, 30m로 하고, 늘어난 통신 반경만큼 토폴로지 크기와 그리드 크기 역시 늘려서 실험을 하였을 때 〔그림 3〕와 같은 결과를 볼 수 있었다. 통신 반경을 15m, 30m으로 하였을 때에는 거의 차이점을 보여주지 않았고, 통신 반경을 30m, 45m로 설정하고 실험 하였을 때에는 〔그림 4〕와 같은 결과를 볼 수 있다.

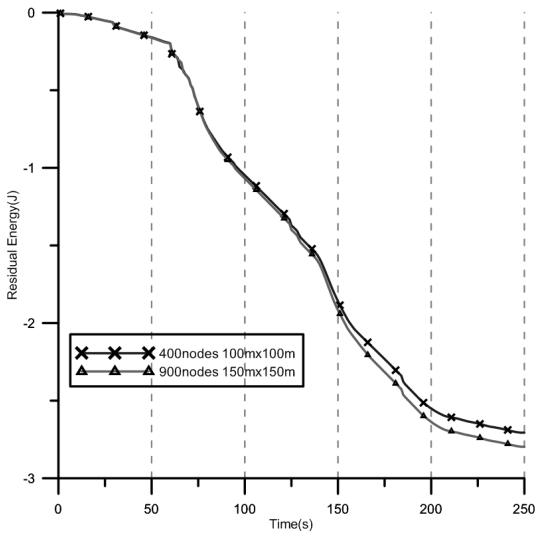


〔그림 7〕 사용되는 해시 함수를 SHA-1과 MD5 로 하였을 경우

다음으로 노드의 수를 100개에서 400개로 늘린 뒤 통신 반경을 15m, 30m로 설정한 실험 결과는 〔그림 5〕와 같다. 역시 센서 노드를 400개로 한 상태에서 통신 반경을 30m, 45m로 설정한 경우는 〔그림 6〕과 같다. 이는 통신 반경에 따라 네트워크의 크기와 그리드 크기 역시 늘려주었기 때문에 통신반경의 변경이 센서 노드의 잔류 에너지양에는 큰 영향을 주지 않은 것으로 볼 수 있다.



〔그림 8〕 센서 노드의 수를 각각 100개, 400개로 하였을 경우



〔그림 9〕 센서 노드의 수를 각각 400개, 900개로 하였을 경우

5.2 해시 함수의 차이

센서 노드가 BS로부터 받은 TESLA 키를 인증할 때 HMAC에서 사용하는 해시 함수를 SHA-1과 MD5로 사용했을 때 생기는 차이점은 〔그림 7〕과 같다. MD5를 사용하였을 때 SHA-1 보다 소비되는 전력이 더 많음을 볼 수 있는데 이는 시뮬레이션 환경 구성에서 설명한 바와 같이 ATmega128L에서 해시 함수 수행 시 걸리는 시간이 차이가 나기 때문이다.

5.3 노드 개수의 차이

서로 다른 크기의 네트워크 내의 센서 노드 수를 각각 100, 400개로 했을 때, 즉 네트워크 내의 센서 노드의 밀도는 같고 센서 노드의 수를 다르게 하였을 때 생기는 차이점은 〔그림 8〕과 같다. 각각 실험의 결과로 나온 가용율은 센서 노드가 100개인 경우 98.9989%이고, 400개인 경우는 97.2431%임을 알 수 있다. 같은 밀도의 센서 노드가 존재하는 네트워크의 경우 노드의 수가 많을 때 소모되는 에너지양이 좀 더 많음을 볼 수 있다.

이번에는 다른 조건은 이전 실험과 같고 센서 노드의 수만 400개, 900개로 하였을 때 나온 결과는 〔그림 9〕와 같다. 900개의 경우 가용율은 92.9293%이었다. 센서 노드의 수가 많아짐에 따라 전송되는 데이터의 양이나 센서 노드간의 통신량이 늘어나기 때문에 에너지 소모량이 더 많음을 볼 수 있다.

5.4 노드 밀도의 차이

네트워크의 센서 노드 밀도를 그리드 당 1개, 2개로 했을 때 볼 수 있는 차이점은 〔그림 10〕와 같다. 이 그래프에서 표현된 가용율은 그리드 당 센서 노드가 1개일 때 18.1818%, 2개일 때 76.8844%으로 나타났다. 이는 낮은 가용율을 보이는 네트워크에서는 BS로부터 Wake up 메시지를 받지 못하여 깨어나지 못한 센서 노드가 많음을 뜻한다. 따라서 다른 노드 밀도를 가진 실험과 비교할 때 더 적은 에너지를 소모하는 것을 알 수 있다.

다음으로 센서 노드의 밀도를 그리드 당 2.5개, 3개로 하였을 때에는 〔그림 11〕과 같은 모습을 보였다. 센서 노드의 가용율은 그리드 당 센서 노드의 수가 2.5개일 때 83.1325%, 3개일 때 85.9532%임을 알 수 있다. 추가적으로 센서 노드 밀도가 그리드 당 3개일 때와 4개일 때의 차이점은 〔그림 12〕와 같다. 이때의 센서 노드의 가용율은 센서 노드가 그리드 당 3개인 경우 85.9532%, 4개인 경우 97.2431%로 측정되었다.

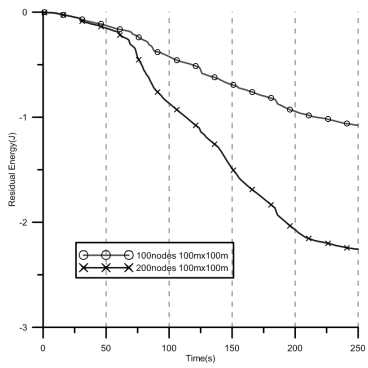
VI. 토의

6.1 예측 운용 가능 시간 (배터리 교체 시기)

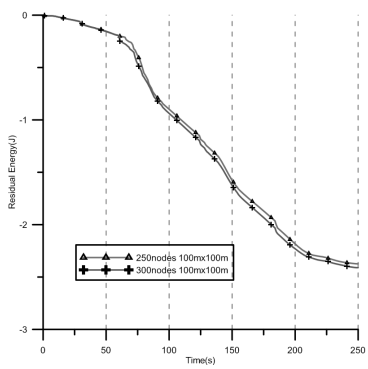
시뮬레이션에서 가정한 센서인 MICAz는 2개의 AA 배터리를 이용한다. 따라서 다음과 같은 계산으로 2개의 배터리의 전류량을 알 수 있다.

$$2 \times 1.5\,V \times 2\,Ah \times 3600 s/h = 21600\,J$$

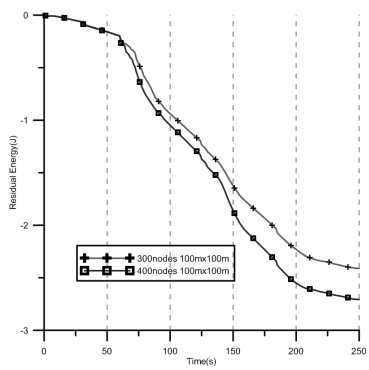
가장 기본적인 상황으로 센서 노드의 수는 100개, 통신 반경은 15m, 그리드 당 센서 노드의 수는 4개가



〔그림 10〕 센서 노드 밀도를 그리드 당 1개, 2개로 설정한 경우



〔그림 11〕 센서 노드 밀도를 그리드 당 2.5개, 3개로 설정한 경우



〔그림 12〕 센서 노드 밀도를 그리드 당 3개, 4개로 설정한 경우

배치되게끔 설정하고 12시간 마다 1회 BS가 방문하여 데이터 취합을 하는 시나리오를 가정하였을 때, 한 번 검증한 후 다음 BS의 방문까지 센서 노드 하나가 소모하는 에너지의 양은 120.6163J 이므로, 하루에 소모되는 에너지는 241.2326J 으로 예상할 수 있다. 이것을 배터리의 전류량에 맞춰 계산하면 2개의 AA 배터리를 이용했을 때 가능한 운용 가능 시간은 89.54일로 예상할 수 있다. 이러한 계산은 센서 노드가 데이터 센싱에 필요한 에너지 및 배터리의 자연 방전으로 없어지는 에너지를 고려하지 않았기 때문에 실제로는 이보다 더 짧은 시간을 운용할 것으로 예측된다.

6.2. 적정 노드 분포

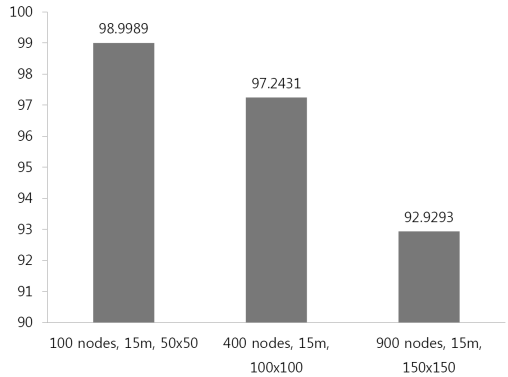
〔그림 13〕과 〔그림 14〕는 노드의 개수와 밀도에 따른 가용율 변화를 보여준다. 〔그림 13〕의 경우 한 그리드 안에 4개의 센서 노드가 동일한 밀도로 분포된 경우, 전체 토폴로지의 홉 수가 늘어났을 때의 분포를 의미한다. 홉 수가 늘어날수록 가용율은 점차 감소함을 알 수 있다. 〔그림 14〕의 경우 15m의 통신 반경을 가진 노드들이 100m×100m 환경에 분포할 때, 노드의 개수가 늘어남으로써, 노드의 밀도가 늘어날수록 가용율이 증가함을 알 수 있다. 응용 환경마다 다르겠지만, 정상적으로 네트워크가 동작하기 위해서는 최소한 80%이상의 가용율을 가져야 한다고 가정하였을 때, 노드의 밀도는 한 그리드에 2.5개 정도가 분포해야 적당하다는 것을 알 수 있다.

VII. 결 론

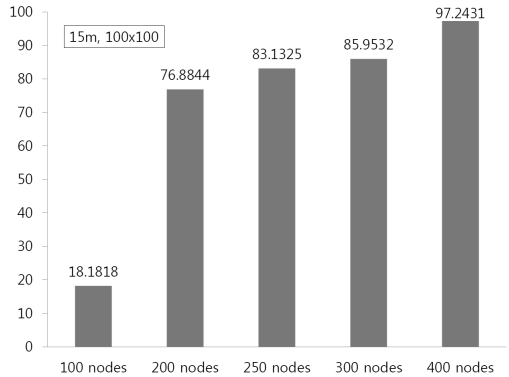
이 논문에서는 멀티 홉 UWSN환경에서 μTESLA가 갖는 성능을 NS-2 시뮬레이터를 이용하여 측정해 보았다. 현실 세계를 반영하여 μTESLA를 동작시키기 위해 최선이라고 생각하는 시나리오를 작성하였으며, 그에 따른 문제점을 일차적으로 발견할 수 있었다. 외부 공격자의 서비스 거부 공격에 대한 위험성에도 불구하고 μTESLA의 문제점은 받은 메시지를 인증하기 이전에 플러딩을 해줘야 한다는 것이다. 또 다른 문제점은 키 슬롯의 크기를 결정하는 문제이다. 만약 키 슬롯이 크다면 BS가 데이터를 가져가는데 걸리는 시간이 매우 길어질 수 있다. 그러나 키 슬롯이 작다면 오랜만에 등장한 BS로부터 받은 키를 검증하기 위해서 소모해야하는 키 검증 시간이 길어진다. 당연하게도 키 슬롯의 크기는 키 검증 시간보다 작아야 한다. 또한 동면을 반복하는 노드를 고려한다면, 키 슬롯은 동면 주기보다 길어야 하는데, 이 논문에서 키 슬롯은 동면 주기인 30초에 맞추어져야만 했다. 이들은 μTESLA에서는 전혀 고려하지 못했던 문제점이다.

이 논문에서 통해서 수행한 시뮬레이션에서 얻어낸 결론에 따르면 우리가 가정한 멀티 홉 UWSN 환경에서 BS가 데이터를 수집하기 위해서 걸리는 시간은 180초 가까이 되면, 한 번에 소모되는 배터리 양은 3J에 약간 못 미치며 잠정적으로 90일 정도 배터리의 교환 없이 해당 시나리오를 운용할 수 있을 것이다. 또한 우리는 한 노드의 통신 반경을 기준으로 설정되는 그리드에서 약 2.5개의 노드가 분포하였을 때, 가용율이 80%이상이 됨을 알아낼 수 있었다.

우리는 이 논문의 실험을 근거로 μTESLA의 사용이 멀티 홉 UWSN 환경에서 좋은 선택이 아님을 알 수 있었다. μTESLA 대신 멀티레벨 μTESLA와 같은 다른 브로드캐스트 인증 기법을 사용할 수 있겠지



〔그림 13〕 노드의 개수에 따른 가용율 변화



〔그림 14〕 노드 밀도에 따른 가용율 변화

만, 원천적으로 남아 있는 서비스 거부 공격에 취약점은 극복하기 힘들다. 따라서 μTESLA와 같이 지연 인증에 기반을 둔 대칭키 방식의 브로드캐스트 인증 방식대신 공개키 서명과 같은 방식이 바람직할 수 있겠으나, 에너지 소비 측면에서 또 다른 결과가 예상되는 만큼, 이는 앞으로의 연구 과제로 남겨둔다.

참고문헌

〔1〕 Bojkovic, Zoran S., Bojan M. Bakmaz, and Miodrag R. Bakmaz. "Security issues in wireless sensor networks." International Journal of Communications 2.1 pp. 106-115. 2008.

〔2〕 A. Perrig, R. Canetti, J.D. Tygar and D. Song, "The TESLA broadcast authentication protocol," Proceedings of RSA CryptoBytes'02, 2002.

〔3〕 Perrig, A., Szewczyk, R., Wen, V., Culler, D., and Tygar, J. D. "SPINS: Security protocols for sensor networks." Proceedings of the 7th annual international conference on Mobile computing and networking. ACM, 2001.

〔4〕 Di Pietro, R., Mancini, L. V., Soriente, C., Spognardi, A., and Tsudik, G, "Data security in unattended wireless sensor networks." Computers, IEEE Transactions on 58.11 pp. 1500-1511. 2009.

〔5〕 S. Roychowdhury and C. Patra, "Geographic Adaptive Fidelity and Geographic Energy Aware Routing in Ad Hoc Routing," Special Issue of IJCCT Vol.1 Issue 2, 3, 4; 2010 for International Conference [ACCTA-2010], pp. 3-5, Aug. 2010.

〔6〕 B. Karp and H.T. Kung, "GPSR: greedy perimeter stateless routing for wireless networks," MobiCOM 00, pp. 243-254, Aug. 2000.

〔7〕 Di Pietro, R., Mancini, L. V., Soriente, C., Spognardi, A., and Tsudik, G, "Catch me (if you can): Data survival in unattended sensor networks." Pervasive Computing and Communications, 2008. PerCom 2008. Sixth Annual IEEE International Conference on. IEEE, pp. 185-194, Mar. 2008.

〔8〕 Crossbow, MICAz Data Sheet, 6020-0060-04 Rev A, http://www.openautomation.net/uploadsproductos/micaz_datasheet.pdf

〔9〕 Atmel AVR., ATmega128L Data Sheet, Rev. 2467O-AVR-10/06, http://www.atmel.com/Images/doc2467.pdf

〔10〕 Texas Instruments, CC2420 Data Sheet, SWRS041c, http://www.ti.com/lit/ds/symlink/cc2420.pdf

〔11〕 Krämer, Marc, and Alexander Geraldy. "Energy measurements for micaz node." 5. GI/ITG KuVS Fachgespräch ,Drahtlose Sensornetze 2006.

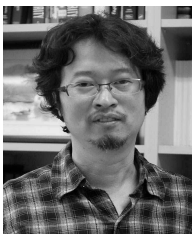
〔12〕 Fan, Zhang, and Li Wenfeng. "Energy efficiency testbed for wireless sensor networks." Systems Man and Cybernetics (SMC), 2010 IEEE International Conference on. IEEE, pp. 3807-3812, Oct. 2010.

〔13〕 Ganesan, P., Venugopalan, R., Peddabachagari, P., Dean, A., Mueller, F., & Sichitiu, M. "Analyzing and Modeling Encryption Overhead for Sensor Network Nodes," WSNA '03: Proc. 2nd ACM Int'l. Conf. Wireless Sensor Networks and Applications, New York: ACM Press, pp. 151 - 159. Sep. 2003.

〈저 자 소 개〉

최 진 춘 (JinChun Choi) 학생회원
2011년 2월: 인하대학교 컴퓨터 정보공학과 졸업
2011년 3월~현재: 인하대학교 컴퓨터 정보공학과 석사 과정
〈관심분야〉 네트워크 보안, 무선 센서 네트워크 보안

강 전 일 (Jeonil Kang) 학생회원
2003년 2월: 인하대학교 컴퓨터 공학과 졸업
2006년 2월: 인하대학교 정보통신대학원 석사
2006년 3월~현재: 인하대학교 정보공학과 박사 과정
〈관심분야〉 RFID 보안, 생체 인식 보안, 무선 센서 네트워크 보안, 무선 인터넷 보안, 웹 인증 보안



양 대 헌 (DaeHun Nyang) 정회원
1994년 2월: 한국과학기술원 과학기술 대학 전기 및 전자 공학과 졸업
1996년 2월: 연세대학교 컴퓨터 과학과 석사
2000년 8월: 연세대학교 컴퓨터 과학과 박사
2000년 9월~2003년 2월: 한국전자통신연구원 정보보호연구본부 선임연구원
2003년 2월~현재: 인하대학교 컴퓨터 정보 공학부 부교수
〈관심분야〉 암호 이론, 암호 프로토콜, 인증 프로토콜, 무선 인터넷 보안

이 경 희 (Kyunghee Lee) 정회원
1993년 2월: 연세대학교 컴퓨터과학과 학사
1998년 8월: 연세대학교 컴퓨터과학과 석사
2004년 2월: 연세대학교 컴퓨터과학과 박사
1993년 1월~1996년 5월: LG소프트(주) 연구원
2000년 12월~2005년 2월: 한국전자통신연구원 선임연구원
2005년 3월~현재: 수원대학교 전기공학과 조교수
〈관심분야〉 바이오인식, 정보보호, 컴퓨터비전, 패턴인식