T-MAC환경에서 취약성 분석

홍진근*, 한군희*
*백석대학교 정보통신학부
e-mail:{jkhong, hankh}@bu.ac.kr

Vulnerability Analysis in T-MAC Environment

Jin-Keun Hong*, Kun-Hee Han*
*Div. of Information and Communication, Baekseok University

요 약

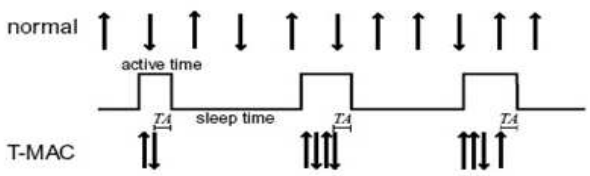
본 논문에서는 TMAC 환경에서 취약성 분석하였다. T-MAC의 보안 특성은 S-MAC 통신 프로토콜이 갖는 보안 취약성과 동일한 형태이다. T-MAC 통신은 TA가 도입된 것을 제외하면, S-MAC에서 강조하고 있는 동일한 보안 인증방안이 필요함을 확인할 수 있다.

1. 서 론

센서네트워크의 통신 프로토콜 및 보안에 대한 연구와 관련하여[1-5], Xiaoming Lu 등[1]은 Listen Sleep S-MAC 프로토콜 방식에서 동기 공격 및 방어에 관한 연구를 수행한 바 있고, Woonsik Lee 등[2]은 무선 센서 네트워크에서 글로벌 동기 알고리즘 분석에 관해 연구한 바 있다. W. Ye. J. Heidemann 등[3]은 무선 센서 네트워크에서 데이터 지연 문제를 해결하기 위해 적용적인 청취방안에 관하여 연구한 바 있으며, 이 논문에서는 기존의 S-MAC은 한 주기 동안 하나의 데이터가 전송되지만 제안된 기법에서는 제어 패킷의 NAV (Network allocation vector)를 사용하여 첫 데이터 전송이 끝나는 시간을 예측하고 해당 시간이 끝날 때 NAV가 설정된 모든 노드들이 활성 상태(on)로 전환하여 다시 전송에 참여하도록 한다. 그러나 이 방안은 근본적인 지연 문제를 해결하지 못하고 있다. 동적 듀티 사이클을 기반으로 하는 MAC에 대한 연구로 P. Lin 등이 제안한 바 있다[4]. 이 방안은 S-MAC이나 listen/sleep의 주기를 갖는 프로토콜들에서 사용되는 듀티 사이클 비율을 사전에 정하고, 전송되는 데이터 트래픽 양을 고려하여 동적으로 듀티 사이클을 가변시켜 지연 요소를 감소하는 방안이다. 대부분의 센서 네트워크 관련 연구는 에너지 효율성 측면에 집중되어 있으며, 실제 T-MAC 통신을 기반으로 발생할 수 있는 타협된 노드로부터의 서비스 거부 공격에 대한 연구가 요구되고 있다. 본 논문에서는 T-MAC 통신을 기반으로 통신 동기가 이루어질 때 발생 가능한 서비스 거부 공격 사례를 분석하고 이를 기반으로 전력 효율성 측면에서 영향을 분석하고자 한다. 본 논문의 구성은 2장에서 T-MAC 통신 프로토콜의 특성을 살펴보고 3장에서 T-MAC 통신 프로토콜의 보안 취약성을 분석하였으며 4장에서 결론을 맺었다.

2. T-MAC 통신 프로토콜 특성

T-MAC이 갖는 기본적인 통신 방식을 다음 그림1에서 제시하였다. T-MAC에서는 자신의 프레임 시작 시점에 한번에 메시지를 전송한다. RTS는 고정된 경쟁을 위한 주기를 거치고 난 다음, waiting/listening 이후 전송된다. 경쟁 시간은 충돌이 발생하지 않더라도 항상 사용된다. 송신을 원하는 노드가 TA 인터벌 동안 응답을 받지 않을 경우 sleep 모드로 돌아가고, 이때 수신 노드가 깨어 있을 때 2번까지 재전송하고 난 다음 sleep 모드로 들어간다.



[그림1] T-MAC 통신의 기본 구성

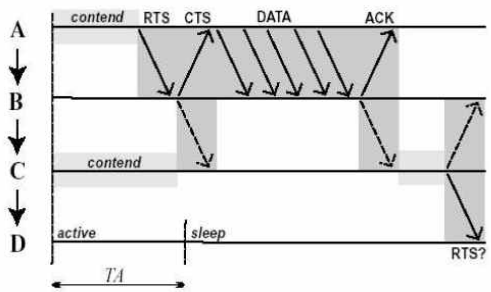
노드는 이웃노드가 통신을 하고 있다면, sleep 모드로 들어갈 수 없다. 이웃 노드로부터의 RTS/CTS를 수신하는 시간은 TA 시간보다 충분히 작아야 하고, 노드가 통신 제약 거리 범위 밖에 있다면, RTS를 수신할 수 없으므로, TA 인터벌이 적어도 CTS 시작 시간보다 충분히 길어야 한다. 다음은 TA 인터벌의 최소 길이를 나타낸 것이다.

$$TA > C + R + T \quad (1)$$

여기서 C는 Contention interval(경쟁 인터벌)을 말하고, R은 RTS 패킷의 길이를 나타낸다. 또한 T는 왕복시간(RTS가 끝나는 시간과 CTS의 시작 시간의 인터벌)이다.

그런데 고정된 duty cycle을 가진 S-MAC은 에너지 소비에 있어서 비효율적인 반면, T-MAC[19]은 S-MAC의 sleep 주기에서 발생할 수 있는 에너지 소모를 줄였다는 점에서 장점을 지닌다. S-MAC은 listen 주기에서 RTS, CTS를 교환한 노드들이 전체 sleep 주기 동안에 지속적으로 깨어 있다. 그러나 두 노드의 데이터 전송이 끝났음에도 불구하고, 계속해서 wake 상태를 유지하는 것이 에너지측면에서 비효율적이라는 사실은 알려져 있는 일이다. T-MAC에서는 TA 시간 동안 데이터의 전송이 없을 경우, 바로 sleep 함으로써 불필요한 에너지 소모 문제를 해결하였다.

T-MAC은 S-MAC의 active 시간 동안의 Idle listening에 소비되는 에너지를 감소시킨다. T-MAC은 일정 정보를 교환하기 위해서 전송 시도가 없는 경우에도 매우 큰 active시간을 보장할 수 있다. 그러나 이웃 노드에게 전송할 데이터가 있음에도 불구하고 이웃노드가 일찍 sleeping 모드로 전환됨에 따라 데이터를 전송할 수 없는 문제가 초래된다.



[그림2] 초기 sleeping 문제

노드 C의 경우, 노드 D와 통신을 개시할 때, C는 경쟁에 들어간다. 만일 A와 B가 RTS/CTS 교환을 통해 데이터 전송이 이루어지고 있다면, 노드 C는 TA 기간 동안에 전송을 할 수가 없으므로, A, B의 전송이 끝날 때 까지 기다린 후, B는 C와 통신을 하고, 다시 C는 D와 통신을 시작할 수가 있다. 이 시간동안 노드 D는 sleep 상태를 유지해야만 한다. 처리율 측면에서, 노드 C는 50%의 전송 성공률을 가지며, 노드 D는 25%의 전송 성공률을 가진다. 이와 같은 문제를 초기 sleeping 문제라 하며, S-MAC 보다 50% 낮은 처리율을 갖는다.

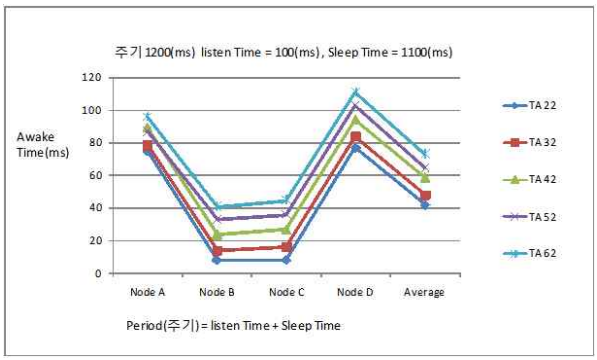
3. T-MAC 통신 프로토콜의 보안취약성

T-MAC의 통신 환경을 다음 표1에서 제시하였다.

[표 1] T-MAC 통신 환경

파라미터	값
듀티사이클	10%
Listen 시간	150msec
Sleep 시간	1,500msec
Sync 패킷 크기	9 Bytes
RTS/CTS/ACK	10 Bytes
Transmitting I(mA)	8mA(avg.)
Receiving I(mA)	7mA(avg.)
deep sleep I(clock only)	8uA
Data 패킷 크기	128 Bytes
TA 주기	가변(22~62msec)
패킷 주기	1,000 사이클
패킷 Listen 인터벌	10 사이클(동기주기)

T-MAC 시뮬레이션에서 에너지 효율이 우수한 주기 1200(ms)에 listen time 100(ms) sleep time 1100(ms)를 기준으로 TA 주기를 22(ms)에서부터 62(ms)까지 가변 할 수 있다.



[그림 3] TA에 따른 Awake Time

T-MAC 프로토콜은 S-MAC에서와 같이 단일 주

파수를 사용하는 경쟁기반이다. Node A가 그룹 내 다른 Node 에 통신을 위해 Sync 동기를 전송하고 RTS 패킷을 보내게 될 때, 해당 Node는 CTS 신호를 보내 응답하게 된다. 다만 S-MAC과 차이점이 있다면, TA개념을 도입한 것이다. 만일 Node A에 대한 응답으로 정상적인 통신 대상이 Node B일 경우, Node B보다 근접한 공격자 B′가 Node B를 가장하고 응답하는 경우가 발생할 경우 TA에 대한 효율성은 무너지게 된다. 현재 물리적인 접속 방안에서는 별도의 replay attack 방지를 위한 방안이 없으며 또한 Node B인지에 대한 정상적인 인증과정이 없다. 따라서 공격자는 Node B를 가장하고 응답 신호인 CTS를 주변에 보낼 수 있다. 이와 같은 유형의 공격은 정상적인 서비스를 방해하는 요소로 작용하게 된다.

또한 Node A에서 동기신호를 그룹 내의 센서노드에 전송하고 RTS 신호를 보낸 이후, CTS 신호를 수신하는 과정에서, Node A와 Node B사이에 RTS 신호와 CTS 신호에 대한 인증방안이 적용되지 않는다면, Node A와 Node B 거리보다 가까운 지점의 Attacker B′가 존재할 때, Node A에서 전송한 RTS 신호에 대해 Attacker B′가 CTS 신호를 전송할 수 있으며, Node B에서 전송한 CTS 신호는 거부될 수 있다. 이것은 S-MAC 갖는 기본적인 통신 특성이다. 그런데 문제는 통신 제약 거리 범위 내에 위치한 이웃한 Node C나 Node D에 대해, 악의적인 노드가 고의적으로 RTS를 전송할 수 있다는 점이며, 이는 곧 Node C, D가 정상적으로 sleep 할 수 없는 이유가 된다.

Attacker B′가 의도적으로 Node A나 기타 공격하고자 하는 대상에 대해, 동시에 거짓 동기신호를 전송함으로써, 동기신호의 충돌을 유도하고, 공격자가 고의적으로 Node A의 패킷 전송을 방해할 목적으로 거짓 동기를 전송하며, 이로 인해 Node A의 RTS 신호나 Data 패킷 전송은 방해받게 된다. 즉 정상적인 시간에 통신이 요구되고, 통신 방해로 인해 Node A는 Sleep 모드로 전환할 수 도 없으며 지속적인 전력 소비가 발생된다. 또한 공격자의 의도적인 서비스 방해로 인해 Node B 또는 다른 그룹 내의 노드들도 Sleep 노드로 전환되는 것을 방해할 수 도 있다는 점 등은 S-MAC이 갖는 보안 취약성 문제도 동일하게 T-MAC에서도 노출되고 있다는 점이다.

4. 결 론

본 논문은 T-MAC의 통신 프로토콜의 보안 취약성이 S-MAC 통신 프로토콜 특성에서 노출되는 보안 취약성과 동일함을 언급하면서 보안 인증의 필요성을 언급하였다.

참고문헌

[1] W. Xiaoming Lu, Matt Spear, Karl Levitt, Norman S. Matloff, S. Felix Wu, "A Synchronization Attack and Defense in Energy Efficient Listen-Sleep Slotted MAC Protocols," Proceedings of ICESIST2008. 2008. 8.

[2] Woonsik Lee, Hwang Soo Lee, "Analysis of a global synchronization algorithm in wireless sensor networks," Proceedings of MFI2008, 2008. 8.

[3] W. Ye, J. Heidemann and D. Estrin, "An Energy Efficient MAC Protocol for Wireless Sensor Networks," Proceedings of IEEE INFOCOM2002, June 2002.

[4] Lin P., Qiao C., Wang X., "Medium access control with a dynamic duty cycle for sensor networks," Proceedings of WCNC2004, March 2004.