한국산학기술학회논문지
Vol. 10, No. 2, pp. 345-350, 2009

센서네트워크에서 S-MAC 공격에 따른 전력 효율성 분석

홍진근[1*]

Analysis of Power Efficiency in according to S-MAC attack in the Sensor Network

Jin-Keun Hong[1*]

요 약 본 논문에서는 센서 네트워크 S-MAC 통신 프로토콜에서 보안 취약성을 살펴보고 서비스 거부 공격의 취약성에 따른 영향을 통신절차 단계별로 소비되는 전력 효율성 측면에서 분석하였다. 따라서 연구 결과로부터 정상적인 S-MAC 통신을 위해 신뢰성, 효율성 및 보안을 고려한 인증방안의 필요성을 도출할 수 있다.

Abstract In this paper, it is reviewed vulnerability of security in S-MAC communication protocol of sensor network, and analyzed in the respect of power efficiency, which is consumed at each stage of communication procedure in according to vulnerability of denial of service. Therefore, from research results, it can be induced the need of authentication scheme, which is considered reliability, efficiency and security of normal S-MAC communication.

Key Words : Sensor, MAC

1. 서론

오늘날같이 급변하는 환경에 유비쿼터스 센서네트워크를 기반으로 하는 어플리케이션이 세계 각국에서 생활과 산업전반에서 나타나고 있다. 이러한 센서 네트워크는 우리 생활에 각종 분야에서 발견 가능한 센서와 연결되어 물리량을 측정하거나 기계장치를 제어하는 무선 신호처리 부분과 데이터를 수신하고 제어 신호를 송신하며 미들웨어로 데이터를 전송하는 디바이스, 그리고 네트워크의 구성, 동작 상태, 데이터 관리, 리포트 생성 기능을 담당하는 시스템으로 구성된다[1-2].

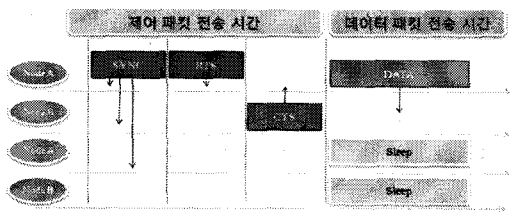
그런데 실제 무선 환경에서는 RF부, 임베디드 하드웨어 및 소프트웨어 등을 갖는 노드에서 보다 적합한 무선 통신 프로토콜, 알고리즘에 대한 개발, 구현 및 시험평가가 이루어진다. 시험 평가 가운데 가장 중요한 항목 가운데 하나가 보안성 항목이며, 보안 서비스는 네트워크를 정상적으로 운영하기 위해 반드시 요구된다. 센서네트워크의 통신 프로토콜 및 보안에 대한 연구와 관련하여 [3-8], Xiaoming Lu 등[3]은 Listen Sleep S-MAC 프로토콜 방식에서 동기 공격 및 방어에 관한 연구를 수행한 바 있고, Woonsik Lee 등[4]은 무선 센서 네트워크에서 글로벌 동기 알고리즘 분석에 관해 연구한 바 있다. W. Ye. J. Heidemann 등[5]은 무선 센서 네트워크에서 데이터 지연 문제를 해결하기 위해 적응적인 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[6]. 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 S-MAC 통신을 기반으로 발생할 수 있는 타협된 노드로부터의 서비스 거부 공격에 대한 연구가 요구되고 있다.

[1]백석대학교 정보통신학부
*교신저자: 홍진근(jkhong@bu.ac.kr)
접수일 08년 12월 15일 수정일 09년 02월 3일 게재확정일 09년 02월 18일

본 논문에서는 S-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 S-MAC 통신 프로토콜의 특성을 살펴보고 3장에서 S-MAC 통신 프로토콜의 보안 취약성을 분석하였으며 4장에서 결론을 맺었다.

2. S-MAC 통신 프로토콜 특성

S-MAC 프로토콜 기반은 단일 주파수를 사용하는 경쟁기반의 프로토콜을 지원하며, 주기적인 Sleep 시간을 갖는다. 센서노드는 가상 클러스터를 구성하여 노드가 깨어나는 시간을 동기화하고 일정시간(duty cycle)동안 Active 상태로 데이터를 주고받는다. CTS (Clear to send) /RTS (Request to send) 신호교환으로 통신 노드가 결정되면 곧바로 Sleep상태로 전환되고 재활성 상태가 되기까지 트랜시버의 전원을 차단한다. S-MAC에서 송신측과 수신측은 RTS/CTS/DATA/ACK 순서로 신호가 교환되고, Active 시점에 상호 SYNC 신호를 교환하고 CSMA (Carrier sense multiple access) 기반으로 일정 여유시간 이후 RTS를 전송한다. SYNC 신호는 이웃 노드와 Active 시간을 조정하며 RTS 신호보다 작은 프레임 형식으로 비주기적으로 상호교환이 일어난다. 센서 노드의 RTS/CTS 신호 청취과정에서 특정 노드가 통신 연결이 이루어지는 것이 판단될 때 다른 노드들은 Sleep 상태로 전환된다. S-MAC은 단일 주파수를 사용하는 경쟁기반의 프로토콜로서 시간을 Active 구간과 Sleep 구간으로 프레임을 구성한다. Sleep 구간에서는 데이터를 송수신 하지 않고 전원 오프 상태를 유지하며, Active 구간에 이웃 노드와 통신하게 되므로 소비되는 에너지를 절감 할 수 있다. 그림 1에서 S-MAC의 주기는 제어 패킷 시간('Listen period')과 데이터 전송 또는 Sleep을 위한 'Sleep period'로 구성된다.



[그림 1] S-MAC 프로토콜 통신 과정

Node A에서 Node B 방향으로 통신을 요구할 경우 먼저 Node A는 그룹 내 SYNC 신호를 전송하여 Sleep 상태에 있던 노드들을 깨운다.

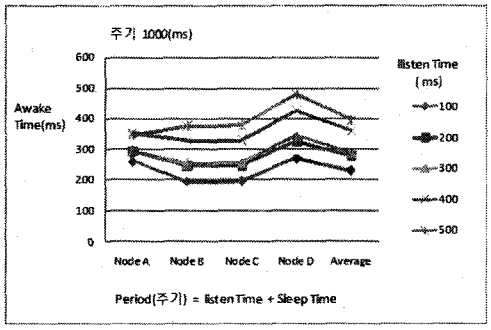
[표 1] S-MAC 통신 환경

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
패킷 주기	1,000 사이클
패킷 Listen 인터벌	10 사이클(동기주기)

이때, Node A 그룹 내에 소속된 통신가능한 모든 노드들(Node B, C, D)이 동기신호를 수신한다. 그러나 Node A가 보내는 RTS 신호는 Node B에서 응답으로 CTS를 송신한다. 또한, 두 노드가 데이터를 전송할 때 Node C와 D는 Sleep 모드로 전환한다.

주기 1000msec 환경에서 10%의 듀티 사이클로 가정할 경우, Listen 시간 100msec~500msec으로 설정한 상태에서 Awake 시간 분포를 그림2에서 나타내었다. 또한 한 주기 사이클은 listen 시간과 sleep 시간의 합으로 나타낼 수 있으며 이 시간은 동기시간, CTS, RTS, guard 및 sleep 시간의 합으로 나타낼 수 있다.

$$T_p = T_{listen} + T_{sleep} = T_{synch} + T_{RTS} + T_{CTS} + T_{guard} + T_{sleep} \quad (1)$$

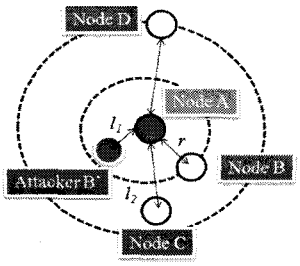


[그림 2] P(주기)가 1000msec 환경에서 Awake 시간 비교

여기서 T_p는 주기 사이클을 나타내고, T_{listen}는 listen 소요시간, T_{sleep}은 sleep 소요시간, T_{synch}는 동기시간, T_{RTS}는 RTS 시간, T_{CTS}는 CTS시간을, T_{guard}는 가드시간을 나타낸다.

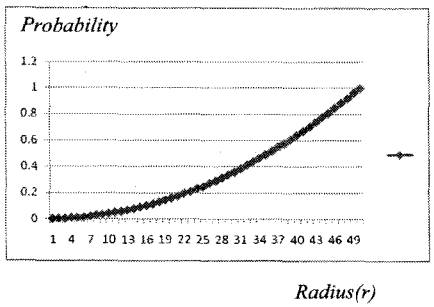
3. S-MAC 통신 프로토콜의 보안 취약성 분석

S-MAC 프로토콜 기반은 단일 주파수를 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. 만일 Node A에 대한 응답으로 정상적인 통신 대상이 Node B일 경우, Node B보다 근접한 공격자 B'가 Node B를 가장하고 응답하는 경우가 발생할 경우 이에 대한 대책은 없다. 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.



[그림 3] S-MAC 통신에서 DoS 공격 예

주기를 갖는 MAC프로토콜들은 한 번 Sleep할 경우 다음 Listen주기 동안 Sleep상태를 유지하기 때문에 전송 지연 문제가 발생한다. 센서 네트워크에서 효율적 에너지 소모를 중요하게 고려하더라도 데이터 전송 지연 역시 무시할 수 없는 주요 요인이다. l_1은 Node A로부터 공격자 B'까지의 거리를 나타내고, r_2는 정상적인 통신 대상인 Node B까지의 거리를 나타낸다. 또한 l_2 는 그룹 내의 다른 노드인 Node C까지의 거리를 나타낸다.



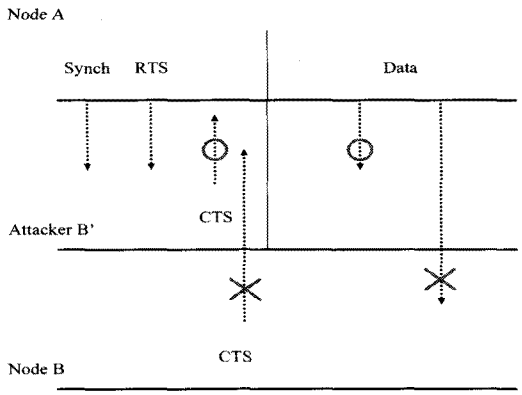
[그림 4] 반경r 기준하여 공격자 노드가 나타날 확률

πl_1^2은 반경 r이내에 존재하는 유한점의 영역으로 나타낼 수 있다.

3.1 Node A와 B간 인증방안이 미적용의 경우

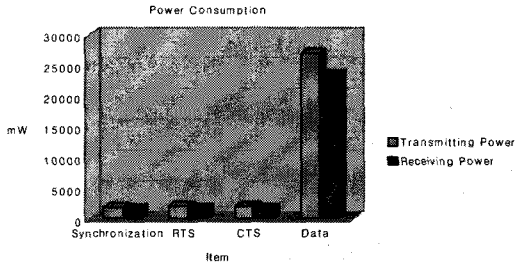
a) RTS 신호와 CTS 신호에 인증방안 미적용시

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 않을 경우, 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. 그림5에서 Node A는 Attacker B'로 Data 패킷을 전송한다. 이 과정에서 Node A와 Attacker B'간 데이터 교환을 위한 정상적인 인증과정이 적용하고 인증이 이루어지면 Node B입장에서는 자동적으로 서비스 거부가 발생한다.



[그림 5] 공격자 Attacker B'의 하이재킹에 따른 Node B 서비스 방해 예

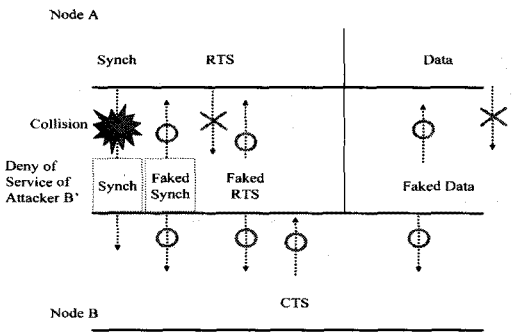
그러나 Node A와 Attacker B'간 데이터 교환을 위한 인증과정이 없을 경우 동일한 정보를 Node B가 수신할 수 있다. 송수신 전송에 따른 에너지 소모량을 그림6에서 제시하였다.



[그림 6] 전송 항목에 따른 에너지 소비량

b) Node A의 동기신호와 충돌에 따른 서비스 방해

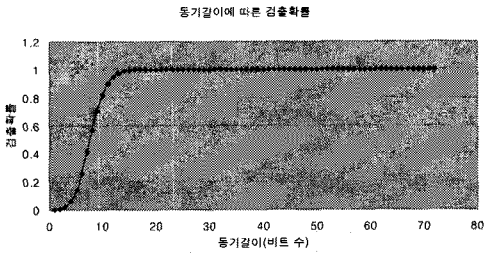
Attacker B'가 의도적으로 Node A와 동시에 거짓 동기 신호를 전송함으로써 동기신호의 충돌을 유도하고, 공격자가 고의적으로 Node A의 패킷 전송을 방해할 목적으로 거짓 동기를 전송하며 이로 인해 Node A의 RTS 신호나 Data 패킷 전송은 방해받게 된다. 즉 정상적인 시간에 통신이 요구되고, 통신 방해로 인해 Node A는 Sleep 모드로 전환할 수 도 없으며 지속적인 전력 소비가 발생된다. 또한 공격자의 의도적인 서비스 방해로 인해 Node B 또는 다른 그룹 내의 노드들도 Sleep 노드로 전환되는 것을 방해할 수 도 있다.



[그림 7] Faked Synch 신호에 따른 서비스 방해 예

$$P_c = 1 - P_{nt} - P_t \qquad (2)$$

P_c는 충돌이 발생할 확률이며 P_{nt}는 그룹 내에서 전송이 없을 경우 확률, P_t는 공격자가 없는 환경에서 그룹 내 임의의 노드에서 전송할 확률이다. 동기 길이에 따른 동기 검출확률을 그림8에서 제시하였다.



[그림 8] 동기 길이 대비 검출확률

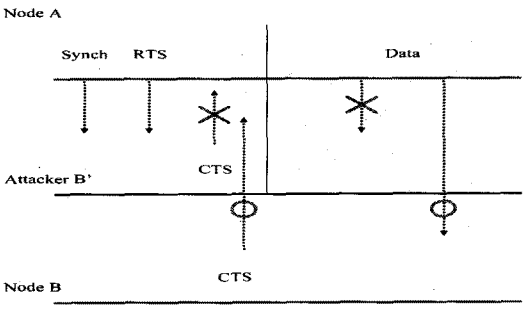
Node A에서 통신절차에 따른 소비전력을 표2에서 제시하였다.

[표 2] 통신 절차에 따른 소비전력 예(Node A)

프로세스 항목	송신소비 전력(mW)	수신소비 전력(mW)	Sleep소비 전력(mW)
동기충돌	1,900	-	1.9
Fake 동기	-	1,663	-
RTS 전송	2,112	-	-
Fake RTS	-	1,848	-
동기 전송	1,900	-	-
RTS 전송	2,112	-	-
CTS 전송	-	1,848	-
Fake Data	-	23,654	-
Data 전송	27,033	-	2.1

3.2 Node A와 Node B간 인증방안 적용시

a) RTS 신호와 CTS신호의 인증방안 적용시



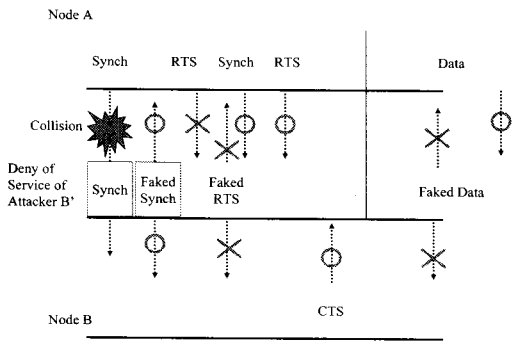
[그림 9] RTS/CTS 신호의 인증방안 적용 예

RTS/CTS 신호에 인증방안이 적용될 경우 Atacker B'가 의도적으로 Node A와 거짓 CTS신호를 전송하여 통신을 요청하나 인증 확인으로 인해 통신이 차단되고 Node B의 통신요청에 Node A가 응답함으로써 정상적인 통신이 이루어진다. Node A의 통신절차에 따른 소비전력을 표 3에서 제시하였다.

[표 3] 통신 절차에 따른 소비전력 예(Node A)

프로세스 항목	송신소비 전력(mW)	수신소비 전력(mW)	Sleep소비 전력(mW)
동기 전송	1,900	-	-
RTS 전송	2,112	-	-
CTS 전송	-	1,848	-
Fake CTS	-	1,848	-
Data 전송	27,033	-	2.1

b) 인증방안 적용에 따른 거부공격 차단



[그림 10] 인증방안 적용으로 정상적인 통신 예

Attacker B'가 공격으로 Node A와 동기 신호충돌이나 거짓 동기를 전송으로 인해 방해를 받을 수 있으나, RTS 단계에서 인증이 적용되어 통신이 차단되며 인증방안이 적용됨으로써 정상적인 Node A의 동기에 대해 Node B의 응답이 이루어질 수 있다. Node A의 인증 및 데이터 전송 완료과정에서 소비전력을 표 4에서 제시하였다.

[표 4] 인증절차에 따른 소비전력 예(Node A)

프로세스 항목	송신소비 전력(mW)	수신소비 전력(mW)	Sleep소비 전력(mW)
동기충돌	1,900	-	1.9
Fake 동기	-	1,663	-
RTS 전송	2,112	-	-
Fake RTS	-	840	-
동기 전송	1,900	-	-
RTS 전송	2,112	-	-
CTS 전송	-	1,848	-
Fake Data	-	11,600	-
Data 전송	27,033	-	2.1

상기 실험들로부터 살펴볼 때 Sleep 상태에서 일부 차이를 보이며, 수신 소비전력에서 차이가 존재함을 볼 수 있다. 또한 RTS와 CTS 인증방안을 적용할 경우 송신 및 수신 소비전력이 상대적으로 낮게 소비됨을 알 수 있다.

4. 결 론

본 논문에서는 센서 네트워크 S-MAC 통신환경에서 통신동기가 이루어질 때 발생 가능한 서비스 공격 유형에 따른 전력 효율성 측면에서 영향을 분석하였다. 분석된 내용은 S-MAC 통신이 갖는 보안 취약성을 기반으로 분석하였으며 인증방안을 적용할 경우와 비교 분석하였다. 연구된 내용은 센서 네트워크 보안통신을 위한 대책 마련에 기여할 것으로 사료된다.

참고문헌

[1] 대덕특구지원단, "U-센서네트워크," 2008 대덕특구 산업시장정보 보고서, 2008.12.

[2] 허재두, 최은창, 김동균, "센서네트워크 응용기술 동향," IITA 주간기술동향 통권 1457호, 2008. 7. 30.

[3] 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.

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

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

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

[7] T. V. Dam and K. Langendoen, "An Adaptive Energy-Efficient MAC Protocol for Wireless Sensor Networks," Proceedings of ACM Sensys2003, Nov. 2003.

[8] Wang, Hongfa, "A Robust Mechanism for Wireless Sensor Network Security," Proceedings of WiCOM2008, Oct. 2008.

홍 진 근(Jin-Keun Hong) **[정회원]**

- 2008년 8월 ~ 현재 : 백석대학교 정보통신학부 교수

<관심분야>
전술통신, 센서넷, RFID, 무선랜 보안