Journal of the Korea Academia-Industrial Cooperation Society
Vol. 12, No. 10 pp. 4606-4611, 2011

http://dx.doi.org/10.5762/KAIS.2011.12.10.4606

DS-MAC 공격에 따른 보안 영향 분석

홍진근[1*]
[1]백석대학교 정보통신학부

Analysis of Security Effectiveness in according to DS-MAC attack

Jin-Keun Hong[1*]
[1]**Division of Information Communication, Baekseok University**

요 약 본 논문에서는 센서 네트워크 DS-MAC 통신 프로토콜에서 보안 취약성을 살펴보고 서비스 거부 공격과 변조공격의 취약성에 따른 영향을 통신절차 단계별로 보안영향을 분석하였다. 본 논문에서는 센서노드간 인증방안 미적용의 경우와 인증방안 적용의 경우, 송신 및 수신 보안영향 측면에서 살펴보았다.

Abstract In this paper, it is reviewed vulnerability of security in DS-MAC communication protocol of sensor network, and analyzed in the respect of security effectiveness, which is consumed at each stage of communication procedure in according to vulnerability of denial of service and modification attack. In this paper, we present about the respect of security effectiveness of transmission and reception in case of operation mode with or without authentication scheme between sensor node.

Key Words : Sensor, MAC, Security

1 서론

최근 의학·생명공학을 포함한 IT융합분야에서, 센서 네트워크에 대한 MAC 통신 프로토콜에 대한 연구가 지속적으로 이루어지고 있다. 특히 센서 네트워크의 연구 테마 가운데 주 관심이 효율적인 에너지 소모에 대한 관심이 모아지고 있다. [1-7]. 본 연구에서는 센서 네트워크에서 보편적으로 사용되는 S-MAC과 동적인 S-MAC 통신 프로토콜이 서비스 거부 공격이라는 보안 이슈와 연결 지어 분석하고자 한다.

먼저 선행연구로, 센서네트워크의 통신 프로토콜 및 보안에 대한 연구와 관련하여 살펴보면 다음과 같다. Monir Hossen 등은 지연에 민감한 대규모 센서 망을 위한 최적화된 지연에 안전한 MAC 프로토콜을 제안한 바 있다[3].

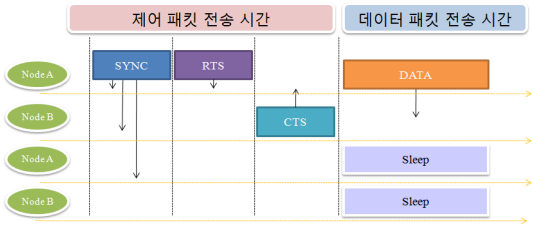
이 연구에서는 센서 네트워크에 적용되는 여러 유형의 MAC 오퍼레이션을 살펴보고, 저자가 제안하고 있는 LS-MAC 프로토콜과 비교하여 지연성 측면에서 분석하고 있다. 또한 지연성을 에너지 소모와 연결성을 가지고 분석하여 성능을 평가하고 있다. 또한 Xiaoming Lu 등[4]은 Listen Sleep S-MAC 프로토콜 연구에서 동기 공격 및 방어에 대한 연구를 한 바 있다. Woonsik Lee 등[5]은 무선 센서 네트워크에서 글로벌 동기 알고리즘을 분석하였으며, W. Ye. J. Heidemann 등[6]은 무선 센서 네트워크에서 데이터 지연 문제를 해결하기 위해 적응적인 청취방안을 연구하였다. 이 주제는 S-MAC이 한 주기 동안 한 개의 데이터가 전송되지만, 제어 패킷의 NAV (Network allocation vector)를 사용하여 첫 데이터 전송이 끝나는 시간을 예측하고, 해당 예측 시간이 종료시점에 NAV가 설정된 모든 노드들이 활성 상태(active on)로 전환하여 다시 전송에 참여하도록 하는 메커니즘에 관한 것이었다. 이 연구의 경우 근본적인 지연 문제는 해결하지 못한다는 지적을 받고 있다. 동적 듀티 사이클을 기반으로 하는 MAC에 대한 연구 주제는 P. Lin 등이 제안한 바 있다[7]. 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 방

*교신저자 : 홍진근(jkhong@bu.ac.kr)
접수일 11년 08월 25일 수정일 (1차 11년 09월 09일, 2차 11년 09월 15일, 3차 11년 09월 29일) 게재확정일 11년 10월 06일

안이다. 대부분의 논문은 실제 S-MAC을 비롯한 주요 MAC 통신 프로토콜을 기반으로 하며, 발생할 수 있는 타협된 노드로부터의 서비스 거부 공격, 듀티 정보 변조에 대한 위험성을 고려되지 않고 있다. 본 논문은 DS-MAC의 서비스 거부 공격, 변조 공격을 중심으로 보안영향을 살펴보고자 한다. 본 논문에서는 S-MAC과 DS-MAC 통신을 기반으로 통신 동기가 이루어질 때 발생 가능한 서비스 거부 공격, 변조공격 사례를 중심으로 보안영향을 분석하고자 한다. 본 논문의 구성은 2장에서 DS-MAC 통신 프로토콜의 특성을 살펴보고 3장에서 DS-MAC 통신 프로토콜의 보안 영향을 분석하였으며 4장에서 결론을 맺고자 한다.

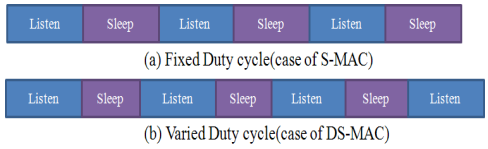
2. DS-MAC 통신 프로토콜 특성

S-MAC 프로토콜은 하나의 주파수를 사용하는 경쟁기반의 프로토콜 기반으로 주기적으로 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) 신호 교환으로 통신 노드가 결정되면 즉시 Sleep 상태로 전환되고 재활성 상태(Re active)가 되기까지 트랜시버의 전원을 차단한다. S-MAC에서 송신측과 수신측은 RTS/ CTS/DATA/ACK 순서로 신호 교환이 이루어지며, 활성(Active) 시점에 상호 동기정보(SYNC)를 교환한다. CSMA(Carrier sense multiple access) 기반에 일정한 여유시간이 지나고 RTS를 전송한다. SYNC 신호는 이웃 노드와 Active 시간을 조정하는데 RTS 신호보다 작은 프레임 형식으로 비주기적으로 상호 교환이 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. 그림1에서 S-MAC의 주기는 제어 패킷 시간('Listen period')과 데이터 전송 또는 Sleep을 위한 'Sleep period'로 구성된다.



[그림 1] S-MAC 프로토콜 통신절차
[Fig. 1] Communication Procedure of S-MAC Protocol

그림2에서처럼 S-MAC 통신은 Sleep time이 고정인 반면, DS-MAC 통신에서 Sleep time은 전송되어야 할 통신량에 따라 가변적이다. DS-MAC은 고정된 듀티 사이클(duty cycle)을 제공하는 S-MAC과 달리, 전송되는 정보의 부하 정도에 따라 자동으로 듀티 사이클을 가변한다. 이렇게 함으로써 전력 소비에 영향을 크게 미치지 않으면서, 지연에 민감한 어플리케이션에 대해서는 지연을 감소시킬 수 있는 이점이 있다.



[그림 2] S-MAC(a) 및 DS-MAC(b)의 듀티 사이클
[Fig. 2] Duty Cycle of S-MAC(a) & DS-MAC(b)

모든 노드가 데이터 전송 시점에 공통된 기본 서비스 듀티 사이클을 정한다. DS-MAC의 듀티 사이클은 전송 정보가 많을 때, 즉 지연이 증가할 때, sleep time을 감소시킨다(듀티 사이클은 증가한다). DS-MAC 프로토콜 절차는 다음과 같다. 우선 이웃 노드로부터 데이터를 수신한다. 수신된 데이터에서 지연정보를 추출하여 평균 지연시간을 계산한다. 해당 이웃 노드의 평균 지연시간이 크면 이 새로운 듀티 사이클 정보가 업데이트 된다. 이 업데이트된 정보는 이웃 노드에 SYNC 정보를 통해 전달된다. 이웃 노드들은 이 새로운 듀티 사이클 정보를 업데이트 하게 된다. DS-MAC 통신 프로토콜 방식은 임의의 노드에서 전송하는 정보가 특정 노드로 전송하는 것이 대부분일 경우에도, 이웃하는 인접 노드의 경우 동일하게 듀티 사이클을 증가시켜야 하므로 idle listening을 통해 에너지 소모가 일어난다. 이 듀티 사이클 정보는 SYNC 패킷 내에서 제공되며, 노드는 동기 정보에 덧붙여 SYNC 패킷을 통해 현재 듀티 사이클 정보를 브로드캐스트 하게 된다. SYNC 패킷을 듣고 있던 이웃하는 노드들이 이 패킷 내의 듀티 사이클 정보를 확인하고, 만일 이

듀티 사이클 값이 정해진 일정보다 높으면 자신의 듀티 사이클을 2배로 설정하고, 낮으면 수신자는 간단하게 일정 테이블을 간단하게 업데이트 한다. 현재의 전력 소비 레벨이 정해진 값 이하 일 때, 2배의 듀티 사이클이 허용된다. 즉 전송 양이 적을 경우 sleep time을 2배로 증가시켜 에너지 소모를 감소시킨다. RTS를 수신한 노드가 듀티 사이클 변경에 대한 요구를 받아들일 것인지를 결정하고, 결정된 값이 CTS 메시지를 통해 송신자에게 전달된다. Node A에서 Node B 방향으로 통신을 요구할 경우 먼저 Node A는 그룹 내 SYNC 신호(듀티 정보 포함)를 전송하여 Sleep 상태에 있던 노드들을 깨운다. 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. 메시지 전달 형식은 다음 그림3과 같다.

Length	Type	ToAddr	FromAddr	Duration (NAV)	CRC

[그림 3] RTS/CTS의 전달 메시지 형식
[Fig. 3] Transmission Message Format of RTS/CTS

DS-MAC 프로토콜에서 통신특성은 표1에서와 같다.

[표 1] DS-MAC 통신 특성
[Table 1] DS-MAC Communication Characteristics

파라미터	값
듀티사이클	가변 10/20/40%
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)

3. DS-MAC 통신 프로토콜의 보안 영향

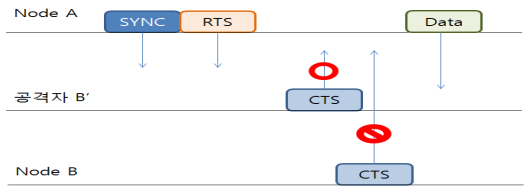
DS-MAC 프로토콜은 S-MAC 프로토콜의 단일 주파수를 사용하는 경쟁기반이다. Node A가 그룹 내 다른 Node 에 통신을 위해 Sync 동기를 전송하고 RTS 패킷을 보내게 될 때, 해당 Node는 CTS 신호를 보내 응답하게 된다. 만일 Node A에 대한 응답으로 정상적인 통신 대상이 Node B일 경우, Node B보다 근접한 공격자 B'가 Node B를 가장하고 응답하는 경우가 발생할 경우 이에 대한 대책은 없다. 현재 물리적인 접속 방안에서는 별도의 replay attack 방지를 위한 방안이 없으며 또한 Node 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 동작하게 된다. DS-MAC 프로토콜은 여전히 보안공격 요소가 존재한다. DS-MAC은 프레임 무결성 검사를 위해 CRC를 제공하나, 이 CRC 값 역시 변조 가능성이 존재한다. DS-MAC 프로토콜에서 주요 보안 이슈는 별도의 MIC(Message Integrity Code) 인증을 통해, Duration 값(듀티 사이클)에 대한 무결성 보장이 이루어져야 한다. 먼저 DS-MAC 프로토콜에서 일어날 수 있는 인증방안 미적용 문제를 살펴본다.

3.1 노드간 인증방안이 미적용 문제

a) RTS 신호와 CTS 신호에 인증방안 미적용

Node A에서 동기신호(SYNC)를 그룹 내의 센서노드에 전송한다. 이 정보에는 기본 듀티 사이클 값(듀티 길이)이 포함된다. 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 지점에 공격자 B'가 존재할 때, Node A에서 전송한 RTS신호에 대해 공격자 B'가 CTS 신호를 전송할 수 있으며, 정상적인 Node B에서 전송한 CTS 신호는 거부될 수 있다.

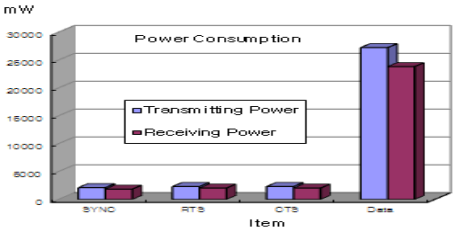
그림3에서 Node A는 공격자 B'로 Data 패킷을 전송한다. 이 과정에서 Node A와 공격자 B'간 데이터 교환을 위한 정상적인 인증과정이 적용하고 인증이 이루어지면 Node B는 자동적으로 서비스 거부가 일어난다.



[그림 3] 공격자 B'의 가로채기
[Fig. 3] Interception of Attacker B'

그러나 Node A와 공격자 B'간 데이터 교환을 위한 인증과정이 없을 경우 동일한 정보를 Node B가 수신하여

가로채기 할 수 있다. 송수신 전송에 따른 에너지 소모량을 그림4에서 제시하였다.



[그림 4] 전송 데이터에 따른 에너지 소비량
[Fig. 4] Energy Consumption Quantity according to Transmission Data

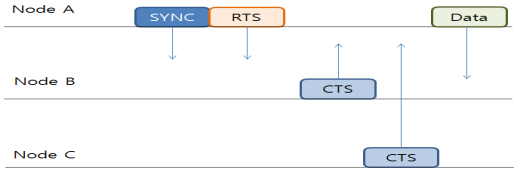
표2는 노드간 인증방안이 적용되지 않을 경우, S-MAC에서 일어날 수 있는 동기충돌과 Fake 동기에 따른 영향을 나타낸 것이다.

[표 2] 통신 절차에 따른 소비전력(Node A)
[Table 2] Energy Consumption according to communication procedure(Node A)

통신절차	송신소비 전력(mW)	수신소비 전력(mW)
동기충돌	1,900	-
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	-

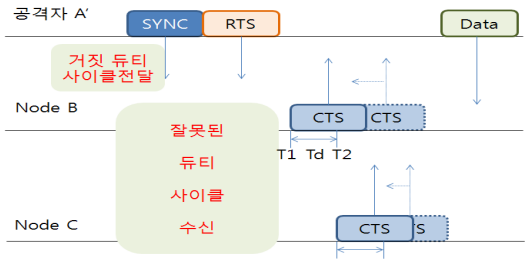
b) 듀티 사이클 변조에 따른 전력 소모공격

먼저 SYNC 정보(듀티 사이클)를 방송한다. 이 과정에서 공격자가 의도적으로 거짓 SYNC 값 즉 변조된 듀티 사이클(듀티 길이 정보) 값을 전달하여 노드들로 추가 전력을 소모하게 할 수 있다. 이것은 변조된 SYNC 정보(듀티 사이클) 방송에서부터 시작하여, 변조된 RTS, CTS 전달 과정에서 일어날 수 있다.



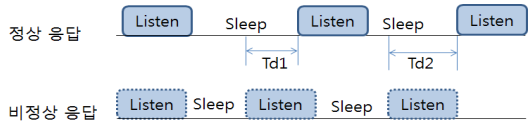
[그림 5] 정상적인 SYNC/RTS/CTS신호전달 과정
[Fig. 5] Transmission Procedure of normal SYNC/RTS/CTS Signal

그림6에서처럼 정상적인 경우 T2 시점에 Awakening 하게 되지만, 거짓 듀티 값으로 인해, T1 시점에 Awakening이 일어난다. Td는 듀티 사이클 변조 공격에 따라 Sleep 상태에서 Transition이 일어난 짧아진 시간을 나타낸다.



[그림 6] 듀티 사이클 변조 공격에 따라 단축된 sleep 시간 (Td)
[Fig. 6] Reduced Sleep Time(Td) according to modification attack of duty cycle

그림7에서는 듀티 사이클 변조가 일어나지 않은 정상 응답에 비해, 듀티 사이클 변조가 일어날 경우인 비정상 응답으로 빠른 Awakening은 제한된 전력 소비 환경에서 추가적인 전력 소비가 요구된다. 그러므로 Td1, Td2만큼 빠른 시간에 awakening 함으로써 전력 소비가 일어나는 센서 노드의 수명이 단축된다. 공격자 노드를 중심으로 주변 노드가 모두 이와 같은 공격 영향을 받게 됨으로써, 주변 노드의 전력 소비는 동시에 수명 단축이 일어난다.



[그림 7] 듀티 환경에서 단축된 Sleep 시간
[Fig. 7] Reduced Sleep Time in duty environment

$$Qs = T_L \times P_L = Tc \times Pc \;/\; (Tl \times Pl + Ts \times Ps + T\alpha \times P\alpha) \quad \text{(식 1)}$$

T_L은 센서 노드의 수명시간이고, Tc는 배터리 수명시간이다. Tl은 센서 노드 *listen* 시간(송신, 수신)이고, Ts는 *sleep* 시간이다. Tα는 *sleep* 천이 시간이다. P값은 각 파라미터별로 소비전력을 나타낸다. 동일한 데이터 송신 및 수신환경에서 듀티 변화에 따른 Node B, C에서 일어날 소비전력을 표3에서 제시하였다.

[표 3] 듀티에 따른 전력소비
[Table 3] Energy Consumption according to duty

통신절차		각 상태에서 듀티 변조기반 소비전력(mW)		
		듀티10%	듀티20%	듀티40%
Idle 시간	Node B	2,112	4,224	8,448
	Node C	2,112	4,224	8,448

거짓 듀티 공격에 따라 듀티 사이클이 증가할수록 Awakening 상태가 지속되므로 idle 시간의 소비전력이 증가함을 알 수 있다.

3.2 노드간 보안방안 적용

a) 인증방안 적용

RTS/CTS 신호에 인증방안이 적용될 경우 공격자는 의도적으로 거짓 듀티를 제공할 수 없다. 만일 거짓 듀티를 제공한다고 할 경우, 듀티 정보 변조유무를 확인함으로써 의도적인 공격에 대비할 수 있다.

[표 4] 정상적인 인증에 따른 전력소비
[Table 4] Energy Consumption according to normal authentication

통신절차		각 상태에서 듀티 변조기반 소비전력(mW)		
		듀티10%	듀티20%	듀티40%
SYNC 전송		1,900	1,900	1,900
RTS 전송		2,112	2,112	2,112
CTS 전송	Node B	2,112	2,112	2,112
	Node C	2,112	2,112	2,112
Idle 시간	Node B	2,112	4,224	8,448
	Node C	2,112	4,224	8,448
Data 전송	Node B	27,033	27,033	27,033
	Node C	27,033	27,033	27,033
소비전력 합계 (1 사이클 기준)		66,526	70,750	79,198

b) 인증방안 적용과 변조 방지 방안 적용

노드간 인증방안 적용과 듀티 사이클 변조 방안이 적용될 경우, 소비전력을 표5에서 제시하였다.

상기 실험들로부터 살펴볼 때, 인증방안이 적용되나 변조방지 방안이 적용되지 않을 경우, 서비스듀티사이클 변조 공격에 따라 소비전력이 영향을 받고 있음을 알 수 있다. 만일 듀티 사이클 40%로 변조가 일어날 경우, 변조방안이 적용된 경우 소비전력을 악 이용한 공격에 대처할 수 있다.

[표 5] 인증절차/변조방지 방안이 적용된 경우 전력소비
[Table 5] Energy Consumption with authentication Procedure/Modification Protect

통신절차		각 상태에서 소비전력(mW)
SYNC 전송		2,376
RTS 전송		2,587
CTS 전송	Node B	2,587
	Node C	2,587
Idle 시간	Node B	2,587
	Node C	2,587
Data 전송	Node B	27,508
	Node C	27,508
소비전력 합계 (1 사이클 기준)		70,327

4. 결 론

본 논문에서는 센서 네트워크 DS-MAC 통신환경에서 발생 가능한 서비스거부 공격, 거짓 듀티에 따른 공격 유형을 보안영향 측면에서 그 영향을 분석하였다. 분석된 내용은 DS-MAC 통신 프로토콜을 기반으로 하는 주요 보안 영향 측면에서 분석하였으며 인증방안, 변조방안 적용 유무와 비교 분석하였다. 연구된 내용은 센서 네트워크 보안통신을 위한 대책 마련에 기여할 것으로 판단된다.

References

[1] IDTechEX, “Wireless Sensor Networks 2011-2021,” 2011 IDTechEX Report, 2011.6.

[2] Wang, “Technology trend for election of secure cluster head in Sensor Network,” IITA ITFinds No1478, 2010. 12. 29.

[3] Mnoir Hossen, Ki-Doo Kim and Youngil Park, “Optimized Latency Secured(LS) MAC Protocols for Delay Sensitive Large Sensor Networks,” Internal Journal of Wireless Communication and Information Systems (IJWCIS), Vol.1 No.1, 2011. 4, pp.18-24.

[4] 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.

[5] Woonsik Lee, Hwang Soo Lee, "Analysis of a global synchronization algorithm in wireless sensor networks,"

Proceedings of MFI2008, 2008. 8.
[6] W. Ye, J. Heidemann and D. Estrin, "An Energy Efficient MAC Protocol for Wireless Sensor Networks," Proceedings of IEEE INFOCOM2002, June 2002.
[7] Lin P., Qiao C., Wang X., "Medium access control with a dynamic duty cycle for sensor networks," Proceedings of WCNC2004, March 2004.

홍 진 근(Jin-Keun Hong) **[정회원]**

- 2008년 12월 ~ 현재 : 백석대학교 정보통신학부 교수

<관심분야>
전술통신, 센서넷, RFID, 무선랜 보안