IEEE 802.15.4 네트워크에서 효율적이고 안전한 미디어 액세스 메커니즘

허 준, 홍충선
경희대학교 컴퓨터공학과
e-mail: heojoon@khu.ac.kr, cshong@khu.ac.kr

Efficient and Secured Media Access Mechanism in IEEE 802.15.4 Networks

Joon Heo, Choong Seon Hong
Dept. of Computer Engineering, Kyung Hee Univ.

요 약

IEEE 802.15.4 표준을 기반으로 하는 무선 액세스 기술은 진화된 컴퓨팅 시스템을 구축하는 데 있어 광범위하게 사용될 수 있을 것이다. 이러한 기술의 활용은 보안성과 공정성이 보장되어야 하지만, 무선 환경에서 악의적인 디바이스는 불공정한 방법을 사용하여 채널 대역폭을 차지할 수 있다. 본 논문에서는 이러한 공격에 대응할 수 있도록 코디네이터의 결정에 의해 정상적인 디바이스가 채널에 우선적으로 액세스 할 수 있는 메커니즘을 제안하고, 이를 위해 기존의 IEEE 802.15.4 표준을 활용할 수 있는 방안을 제시한다. 시뮬레이션 결과는 본 논문에서 제안하는 메커니즘이 MAC 레이어에서의 공격을 효과적으로 방지할 수 있음을 보여준다.

1. 서론

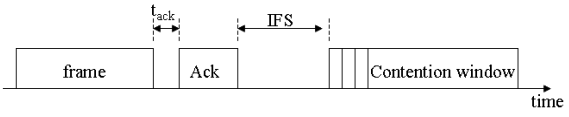
IEEE 802.15.4, IEEE 802.11과 같은 무선 프로토콜은 채널 공유를 위해 분산 경쟁 메커니즘을 사용하고 있다. 경쟁기반 메커니즘은 상호 협약적인 메커니즘 (예를 들면, 전송 전에 랜덤 백오프 시간을 가짐)을 기반으로 하고 있으며, 이러한 방법을 사용함으로써 네트워크에 포함되어 있는 디바이스들이 공정하게 채널을 공유할 수 있게 된다. 그러나, 무선 환경의 특성상 악의적인 디바이스는 채널을 불공정한 방법으로 획득함으로써 네트워크의 성능을 저하시키고 정당한 디바이스들이 채널을 사용하지 못하도록 할 수 있다. 악의적인 디바이스들이 채널을 획득하기 위해 사용하는 공격방법으로 아래와 같은 예를 들 수 있다 [2][4].

- 각 디바이스들이 서로 다른 범위를 가지고 있는 *CW* (Contention Window) 사이즈를 작게 함. 다시 말해 [0, *CW*] 범위를 사용하는 대신 [0, *CW*/3]의 범위 내에서 백오프 시간을 선택.
- 충돌이 발생했을 경우 *CW*값을 두 배로 증가시키지 않고 적은 범위 내에서 재전송을 시도.

위와 같은 공격이 이루어 질 경우 정당한 디바이스들의 성능은 심각하게 감소될 수 있음이 그 동안의 연구를 통해 증명되었다[3][4]. 본 논문에서는 이러한 공격을 방지하기 위해 채널 우선순위에 대한 새로운 메커니즘을 제안하고, 기존 표준 프로토콜에 이러한 기능을 적용할 수 있는 방안을 제시한다.

2. IEEE 802.15.4에서의 채널 액세스

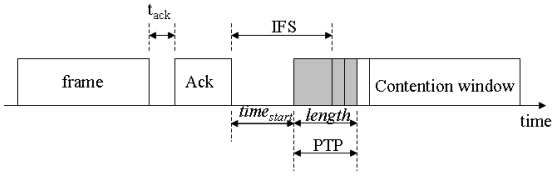
본 절에서는 채널 액세스를 위해 IEEE 802.15.4 표준에서 정의하고 있는 몇 가지 특징에 관하여 설명한다[1]. 이 표준에서 복수의 디바이스들은 채널에 액세스하기 위하여 기본적으로 CSMA-CA 메커니즘을 사용한다. 송신 데이터를 가지고 있는 디바이스는 먼저 [0, 2^{BE}-1] 범위에서 백오프 값을 랜덤하게 선택한다. *BE*는 백오프를 위한 지수 값이며, 이 값은 백오프 선택을 위한 범위를 나타낸다. 각 디바이스는 CAP (Contention Access Period) 동안에 프레임을 전송하기를 원할 경우 먼저 랜덤하게 선택된 백오프 슬롯만큼 대기한다. 만약 채널이 사용(busy) 상태라면 디바이스는 또 다른 랜덤 백오프 값을 선택하여 그 시간동안 기다리게 된다. 만약 채널이 미사용(idle) 상태라면 전송을 원하는 디바이스는 다음번 백오프 슬롯 경계에서 전송할 수 있다. 그러나, 확인(Acknowledgment) 프레임은 CSMA-CA 메커니즘을 따르지 않고 전송될 수 있다. 또한, MAC 서브 레이어는 물리계층에서 데이터가 수신될 수 있는 동안의 특정 시간을 정의하고 있다. 만약 수신된 프레임이 확인 프레임을 요구한다면 디바이스는 이러한 물리적인 시간이 지난 후 확인 프레임(ack)을 전송할 수 있으며 그에 이어 프레임 간격(IFS)가 위치하게 된다. 이 개념은 그림 1에서 설명하고 있다[1].



(그림 1) IFS(Interframe Space)

3. Priority Time Period를 사용한 채널 액세스

제안된 메커니즘은 기존의 IEEE 802.15.4 MAC 레이어 표준의 수정을 최소화하는데 초점을 맞추었다. 위에서 언급한 것처럼 악의적인 디바이스는 표준에서 정의된 범위보다 더 작은 백오프 값을 선택함으로써 (예를 들면, [0, 2^{BE}-1] 범위에서 백오프 값을 선택하는 것이 아니라 [0, (2^{BE}-1)/3] 범위에서 선택) 불공정하게 채널을 획득할 수 있다. 제안된 메커니즘은 코디네이터 (coordinator)에 의해 결정되는 *PTP*(Priority Time Period)를 정의하고 정당한 디바이스들이 경우에 따라 이 범위를 사용함으로써 악의적인 공격으로 발생할 수 있는 성능저하를 방지할 수 있는 메커니즘을 제안한다. 만약 정당한 디바이스가 반복적으로 채널 획득에 실패할 경우 디바이스는 *PTP*를 사용할 수 있으며, *PTP*사용을 위한 정보는 암호화된 값을 코디네이터로부터 전송받는다. *PTP*에서 시작시간은 그림 2와 같이 IFS안에 위치한다.



(그림 2) *PTP* (Priority Time Period)의 정의

그림 2에서 $time_{start}$ 는 확인 프레임 전송 후에 *PTP*를 사용할 수 있는 시작 시간을 의미하며, *length* 는 *PTP* 지속시간을 의미한다. $time_{start}$와 *length*는 모두 코디네이터에 의하여 결정된다. 코디네이터는 이 값을 결정한 후 암호화하여 정당한 디바이스에게 전달한다. 코디네이터와 디바이스간의 키 교환은 상위레이에서 정의하며, 본 논문에서는 언급하지 않는다.

IEEE 802.15.4에서 정당한 디바이스는 채널을 획득하기 위해 CSMA-CA 알고리즘을 사용한다. 제안된 메커니즘에서 만약 *NB* 값이 3이상이 될 경우 (NB>3) 디바이스는 *PTP*를 사용할 수 있다. *NB*값은 현재의 전송까지 시도한 백오프 회수를 의미하며 IEEE 802.15.4 표준의 경우 *NB*의 최대 값을 6으로 정의하고 있다. 새로운 프레임을 전송할 경우 이 값은 0부터 시작된다.

Beacon frame format

Octets: 2	1	4/40	2	variable	variable	variable	2
Frame control	Sequence number	Addressing fields	Superframe specification	GTS field	Pending address	Beacon payload	FCS

Bits: 0-3	4-7	8-11	12	13	14	15
Beacon order	Superframe order	Final CAP slot	Battery life extension	Priority Time Period	PAN coordinator	Association permit

Superframe specification field

(그림 3) *PTP*를 위한 비콘 프레임 형식

우선적으로 코디네이터는 현재의 네트워크에 *PTP*를 적용할 것인지를 결정하고 그림 3과 같은 비콘 프레임 안에 그 사항을 표시하게 된다. 그림 3에 표시된 1비트의 값이 이러한 용도로 사용된다. 만약 *PTP*를 사용할 경우 이 비트는 1 값을 가지며 그렇지 않을 경우 0값을 가진다.

또한, 그림 4와 같이 *PTP*를 사용하기 위한 실제적인 정보들은 코디네이터와 정당한 디바이스 간에 공유되는 비밀 키로 암호화되어 비콘 프레임의 페이로드 부분을 사용해 전송된다. 악의적인 디바이스는 비밀 키로 암호화되어 전송되는 이 정보를 알 수 없다.

- 암호화된 비콘 페이로드: $E_{key}\{time_{start}, length\}$

Encrypted beacon payload

Octets: 1	1
$time_{start}$	*length*

(그림 4) *PTP*를 사용하기 위한 암호화된 정보

또한, 제안된 메커니즘은 *PTP*를 사용하여 프레임을 전송하는 디바이스가 정당한 것임을 증명하기 위해 해쉬(hash) 값을 포함하여 전송하도록 정의하며, 그림 5는 해쉬 함수의 입력 값($time_{start}$)과 이 값이 프레임 안에 포함되는 부분을 설명하고 있다.

Format of the frame control field

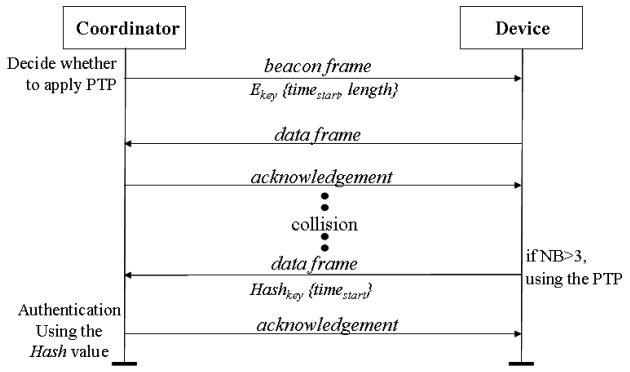
Bits: 0-2	3	4	5	6	7-9	10-11	12-13	14-15
Frame type	Security enable	Frame pending	Ack. request	Intra-PAN	Reserved	Dest. Addressing mode	Reserved	Source Addressing mode

$Hash_{key}\{time_{start}\}$

(그림 5) 인증을 위한 해쉬(hash)값 정의

코디네이터는 이 해쉬 값을 사용해 프레임을 전송한 디바이스의 정당성 유무를 판단할 수 있다. 만약 인증에 실패하여 악의적인 디바이스로 판명될 경우, 코디네이터는 네트워크 정책에 따라 해당 디바이스와의 연결을 끊는 등의 조치를 취할 수 있다.

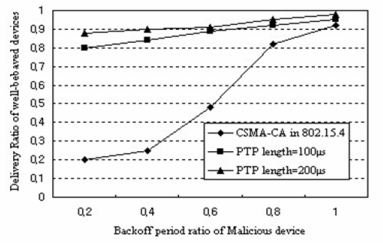
그림 6은 앞서 제안한 메커니즘을 사용할 경우를 전체적인 시퀀스 형식으로 설명하고 있다. 이 그림에서 각 통신 방법 및 메시지는 IEEE 802.15.4 표준을 따른다.



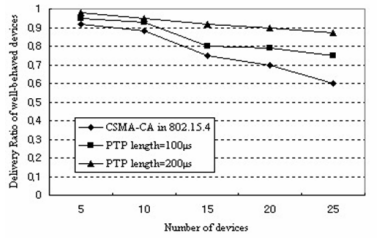
(그림 6) *PTP*를 사용한 채널 획득

4. 성능 평가

성능평가를 위한 값은 "정당한 디바이스의 데이터 프레임 전송률(Delivery Ratio of data frames of well-behaved devices)"을 선택하였으며, 이 값은 디바이스의 전송률을 통한 디바이스의 프레임 전송 효율을 나타낸다. 시뮬레이션은 NS-2 모듈을 수정하여 사용하였다. 트래픽은 20바이트의 패킷 사이즈를 갖는 CBR 트래픽을 사용하였다. 그림 7(a)는 악의적인 디바이스의 백오프 범위에 따른 결과를 보여주고 있다. (예를 들어, 만약 악의적인 디바이스가 [0, $(2^{BE}-1)/4$] 범위에서 랜덤한 백오프 값을 선택하였다면 그 값은 0.25이다. 그림 7(b)는 디바이스의 수에 따른 전송률을 나타내고 있다. 시뮬레이션 결과에서 알 수 있듯이 제안된 메커니즘을 사용하는 경우 MAC 레이어 공격에서도 성능을 유지할 수 있음을 알 수 있다.



(a) Delivery ratio vs. backoff period ratio of malicious device



(b) Delivery ratio vs. number of devices

(그림 7) *PTP*를 사용할 경우 공격에 대한 성능유지

5. 결론 및 향후 과제

MAC 레이어서의 공격에 대한 방어는 정당한 디바이스가 채널을 공유함에 있어서 디바이스의 성능을 유지하기 위해 무엇보다 중요한 기술이라고 말할 수 있다. 이를 위해, 본 논문에서는 *PTP* 메커니즘을 정의하고 이를 IEEE 802.15.4에 적용할 수 있는 방안을 새롭게 정의하였으며, 예약된 비트 값을 사용함으로써 기존의 표준에 새로운 요구사항을 추가하지 않도록 하였다. 또한 시뮬레이션 결과를 통해 제안된 메커니즘이 MAC에 효율적으로 대처할 수 있음을 보였다. 향후 과제로서 제안된 메커니즘을 구체화하고 좀 더 다양한 공격에 대한 대비책을 마련해야 할 것이다.

참 고 문 헌

[1] IEEE Standard for Wireless Medium Access Control and Physical Layer Specification for Low-Rate Wireless Personal Area Networks, P802.15.4, 2003.

[2] Pradeep Kyasanur, Nitin H. Vaidya, "Detection and handling of MAC layer misbehavior in wireless networks", Dependable Systems and Networks 2003, pp.173 182, June 2003.

[3] N. Sastry, D. Wagner, "Security Consideration for IEEE 802.15.4 Networks", WiSe'04 Proceeding, pp.32-42, 2004.

[4] Hao Yang, Haiyun Luo, Fan Ye, Songwu Lu, Lixia Zhang, "Security in Mobile Ad Hoc Networks: Challenges and solutions", Wireless Communications, Volume 11,Issue: 1,pp 38-47, Feb 2004.