IEEE 802.15.4 MAC 기술

조무호 | 김광식
경주대학교, 특허청

요 약

IEEE Std 802.15.4 표준기술은 저속 데이터 전송속도의 무선 통신 능력을 위한 표준을 정의 한다. 본고에서는 IEEE 802.15.4 MAC 기능을 요약해서 기술한다. 또한 보안기술 부분은 IEEE 802.15.4-2006 규격을 기준으로 해서 간략히 설명하고, 2003 버전과의 차이점에 대해서도 비교 설명한다.

I. 서 론

IEEE Std 802.15.4 표준기술은 무선 센서 네트워크 또는 무선 에드혹 네트워크에 적용될 수 있는 기술로서, 10m의 POS(Personal Operating Space)영역 동작에서 배터리가 없거나 아주 제한적인 소모가 요구되는 고정형, 휴대형 또는 이동형 디바이스의 저속 데이터 전송속도의 무선 통신 능력을 위한 물리 계층과 MAC 부계층을 정의 한다. IEEE 802.15.4 TG는 2000년 12월에 결성되었고, 2003년 5월 IEEE 802.15.4-2003 표준을 승인하여, 그해 10월에 출판하였다[1]. 이의 개정판인 IEEE Std 802.15.4-2006은 2006년 6월에 승인되었고, 9월에 출판되었다[2]. 2006년 개정의 목적은 2003 버전과의 상호 호환을 가지면서, 보완과 수정을 그 목적으로 한다. 이러한 내용에는 의미가 모호한 부분을 없애고 불필요하게 복잡한 부분을 감소시켰으며, 보안 키 사용에서의 유연성을 향상시키고, 새롭게 사용 가능한 주파수 할당에 대한 고려사항이 포함되었다.

본고의 제2장에서는 IEEE 802.15.4 MAC 기능의 핵심적인 부분만 간략히 기술하고자 한다[3]. 먼저, 무선 채널 접속을 위한 슈퍼프레임 구조와 CSMA-CA(Carrier Sense Multiple Access- Collision Avoidance) 메커니즘이 소개된다. 다음으로, 코디네이터와 디바이스간의 데이터 전송모델, PAN을 식별하기 위한 채널 스캔, PAN 코디네이터가 PAN을 시작하고 재정렬하는 PAN의 시작과 재정렬, 그리고 채널 스캔을 통해 PAN에 소속시키는 가입 절차와 가입된 디바이스가 PAN을 떠나는 탈퇴 절차가 소개된다. 마지막으로 비컨 프레임을 생성하는 코디네이터와 디바이스 간 동기를 맞추기 위한 절차인 동기화, 디바이스에 독점적으로 사용되는 채널을 할당하기 위한 GTS (Guaranteed Time Slot) 할당 및 관리 방법에 대해서 기술한다.

보안기술 부분은 상기의 MAC 기능 설명에 분리하여 별도의 장으로 소개한다. 보안 관점에서 보면, IEEE 802.15.4-2006 표준 기반의 무선 에드혹 네트워크는 타 무선 네트워크와 다르지 않다. 무선 에드혹 네트워크는 수동적인 도청(eavesdropping) 공격 및 잠재적인 능동적인 변경(tampering)에 취약한데, 그 이유는 전송 매체를 통해 브로드캐스팅 되는 무선 자체의 특성 때문이다 [4]. 무선 에드혹 네트워크에서 디바이스는 저비용이고, 컴퓨팅 파워, 가용 저장능력 및 전원 사용 능력에 극히 제한적이어서, 암호 알고리즘과 프로토콜의 선택에서 제한적일 수밖에 없고 보안 구조의 설계에 제약이 따른다. 따라서 대부분의 보안 기능들은 상위 계층에 구현될 수 있을 것이다. IEEE 802.15.4-2006 표준에서 암호 메커니즘은 대칭키 암호에 기반을 두며, 상위 계층 프로세서에 의해 제공되는 키를 사용한다. 이

키들의 설치와 유지는 본 표준의 범위 밖이다. 상기의 메커니즘은 암호학적 운용의 안전한 구현을 가정하고 키의 저장소가 안전하다고 가정한다. 본고의 제3장에서는 보안기술에 대해 IEEE 802.15.4-2006 규격을 기준으로 해서 간략히 설명하고, IEEE 2003 버전과의 차이점에 대해서도 비교한다. 마지막으로 제4장에서 결론을 맺도록 한다.

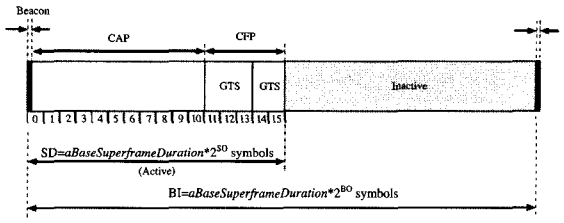
II. IEEE 802.15.4 MAC 기능적 설명

1. 슈퍼프레임 구조

PAN에 있는 코디네이터는 슈퍼프레임 구조를 사용하여 채널 시간을 선택적으로 제한할 수 있다. 슈퍼프레임은 네트워크 코디네이터가 전송하는 비컨에 의해 범위가 결정되며, 같은 사이즈를 갖는 16개의 슬롯으로 나눠진다. 비컨 프레임은 각 슈퍼프레임의 첫 번째 슬롯에서 전송되고, 만약 코디네이터가 슈퍼프레임의 사용을 원하지 않는다면 비컨은 전송되지 않는다. 비컨은 연결된 디바이스들을 동기화시키고, PAN을 식별하고, 슈퍼프레임 구조를 설명하기 위해 사용된다. 슈퍼프레임은 활동구간과 비활동구간을 가질 수 있다. 코디네이터는 비활동구간 동안에는 저전력 모드에 들어갈 수도 있다.

활동구간은 CAP(Contention Access Period)와 CFP (Contention Free Period)로 구성된다. CAP 동안에 통신을 원하는 디바이스들은 슬롯화된 CSMA-CA 방법을 이용한다. 반면에 CFP는 GTS들을 포함한다. GTS들은 CAP에 뒤이어서 활동구간의 마지막 부분에서 시작된다. PAN 코디네이터는 GTS를 7개까지 할당할 수 있으며, 하나의 GTS는 하나의 슬롯 이상의 기간을 점유할 수 있다.

슈퍼프레임의 구조는 macBeaconOrder와 macSuperframeOrder의 값에 의해 기술된다. macBeaconOrder는 코디네이터가 그의 비컨프레임의 어느 구간에 전송할 것인가를 나타낸다. macBeaconOrder의 값 BO와 비컨구간 BI는 다음과 같이 관련되어 있다: $0 \le BO \le 14$, BI= aBase SuperframeDuration*2^{BO}. 만약 BO=15이면, 코디네이터는 비컨 프레임을 전송하지 않으며, 특별히 비컨 요청 명령어 수신등과 같이 요청이 되는 경우에는 예외이다. 또한, 만약 BO=15이면 macSuperframeOrder의 값은 무시 된다.



(그림 1) 슈퍼프레임 구조의 한 예

macSuperframeOrder는 슈퍼프레임의 활동구간의 길이를 기술한다. macSuperframeOrder의 값 SO와 슈퍼프레임기간 SD는 다음과 같이 관련되어 있다: $0 \le SO \le BO \le 14$, SD=aBaseSuperframeDuration*2^{SO}. 만약 SO=15이면, 슈퍼프레임은 비컨 다음에 활동 구간이 남지 않는다.

2. CSMA-CA 메커니즘

CSMA-CA 메커니즘은 CAP 내에서 전송되는 데이터 전송 이전이나 MAC 명령어 프레임 전송에 사용되며, 그렇지 않은 프레임은 데이터요청 명령어의 ACK에 이어 즉시 전송된다. CSMA-CA 메커니즘은 비컨 사용 PAN에서는 비컨 프레임의 전송, ACK 프레임 또는 CFP에서 전송되는 데이터 프레임 전송을 위해서는 사용되지 않는다.

주기적인 비컨이 사용되면, MAC 부계층은 슈퍼프레임 CAP에서의 전송에 대해 CSMA-CA 메커니즘의 슬롯화 버전을 사용한다. 반대로 만약 PAN에서 주기적인 비컨이 사용되지 않거나 또는 비컨 사용 PAN에서 비컨이 위치 할 수 없다면, MAC 부계층은 CSMA-CA 메커니즘의 비슬롯화 버전을 사용하여 전송한다.

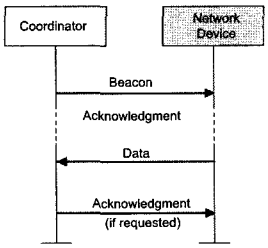
3. 데이터 전송 모델

데이터 전송 방식에는 3가지가 존재하는데, 그 중 첫 번째는 디바이스가 코디네이터에게 데이터를 전송하는 방식이고, 두 번째 방식은 디바이스가 코디네이터로부터 데이터를 수신하는 방식이다. 마지막으로 세 번째 방식은 데이터를 두 개의 동등 디바이스 사이에서 전송하는 방식이다. 스타 토폴러지는 데이터가 코디네이터와 디바이스 사이에서만 교환되기 때문에 오직 두 가지의 방식만 사용할 수 있지만,

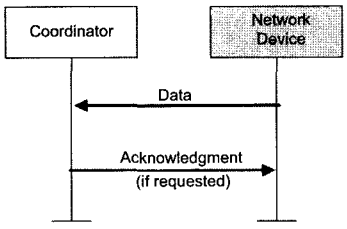
상호동일계층 토폴러지에서는 네트워크상의 어떠한 2개의 디바이스와도 데이터 교환이 가능하므로 세 가지 방식 모두를 사용할 수 있다.

네트워크상에서 비컨의 전송 가능 유무에 따라 각 전송방식의 메커니즘이 결정되는데, 비컨 사용 PAN은 동기화와 PC 주변장치와 같이 짧은 지연이 요구되는 디바이스의 네트워크에서 사용된다. 만약 네트워크가 동기화를 필요로 하지 않거나, 짧은 지연 디바이스를 지원하지 않는다면, 비컨을 사용하지 않을 것이다. 그러나 네트워크의 결합을 위해서 비컨이 필요하다. 비컨 사용 PAN에서 디바이스가 코디네이터로의 데이터 전송을 원할 때 우선 네트워크 비컨의 수신을 위해 대기해야 한다. 비컨이 수신될 때 디바이스는 슈퍼프레임 구조로 동기화하고 적절한 시점에 디바이스는 슬롯화 CSMA-CA를 사용하여 코디네이터로 데이터 프레임을 전송한다. 코디네이터는 ACK 프레임을 전송함으로써 데이터 수신이 성공되었음을 알린다. 비컨 비사용 PAN의 경우에는 단순히 비슬롯화 된 CSMA-CA를 사용하여 코디네이터로 데이터를 전송한다. 코디네이터는 ACK 프레임을 보내 데이터 수신이 성공하였음을 알린다.

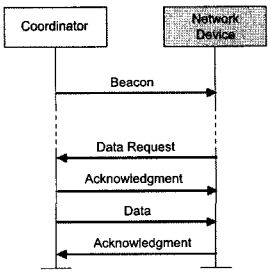
만약 비컨 사용 PAN에서 코디네이터가 디바이스에게 데이터를 전송을 원하면, 코디네이터는 비컨에 데이터가 대기중이라는 것을 표시한다. 디바이스는 주기적으로 비컨을 수신하여, 만약 데이터가 대기 중이면 슬롯화 된 CSMA-CA를 사용하여 데이터 요청 명령어를 보낸다. 코디네이터는 ACK를 보내어 데이터 요청 명령어 수신을 확인시키며, 대기 중이던 데이터는 슬롯화 된 CSMA-CA를 통해 보내지거나 혹은 가능하다면 ACK에 이어서 보내진다. 디바이스가 데이터 수신 ACK를 보내면 전체 트랜잭션이 종료된다.



(그림 2) 비컨 사용 PAN의 코디네이터로의 통신

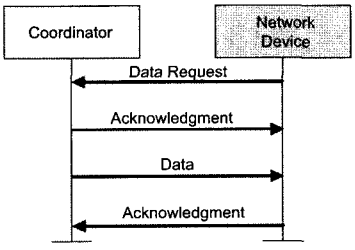


(그림 3) 비컨 비사용 PAN의 코디네이터로의 통신



(그림 4) 비컨 사용 PAN의 코디네이터로부터의 통신

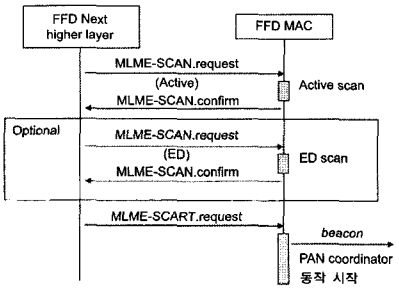
비컨 비사용 PAN에서 코디네이터는 디바이스에게 데이터 전송을 원할 때에는, 디바이스가 데이터 요구 메시지를 보낼 때까지 데이터를 보관하고 있다. 디바이스는 비슬롯화 된 CSMA-CA를 사용하여 데이터 요청 명령어를 주기적으로 코디네이터로 보내어 대기 중인 데이터가 있는가를 확인한다. 코디네이터는 ACK를 보내어 데이터 요청 명령어 수신을 확인시키며, 대기 중인 데이터가 있는 경우에는 비슬롯화 된 CSMA-CA를 사용하여 데이터 프레임을 전송한다. 만약 보낼 데이터가 없으면, ACK에 표시하거나 혹은 페이로드가 없는 데이터 프레임을 보내어 표시한다. 디바이스가 데이터 수신을 성공적으로 수행하였으면 ACK를 보내어 확인시킨다.



(그림 5) 비컨 비사용 PAN의 코디네이터로부터의 통신

4. 채널 스캔

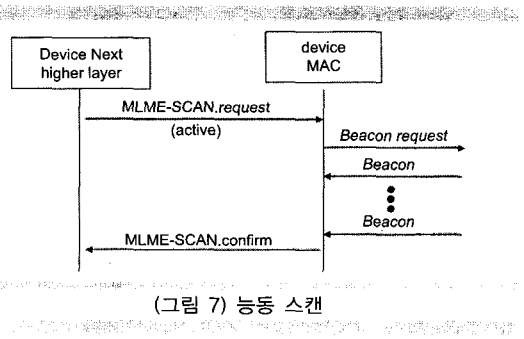
모든 디바이스들은 정해진 채널 목록에 대하여 수동 스캔(passive scan)과 orphan 스캔을 수행할 수 있다. 추가로 FFD(Full Function Device)는 ED(Energy Detection) 스캔과 능동 스캔(active scan)을 수행할 수 있다.



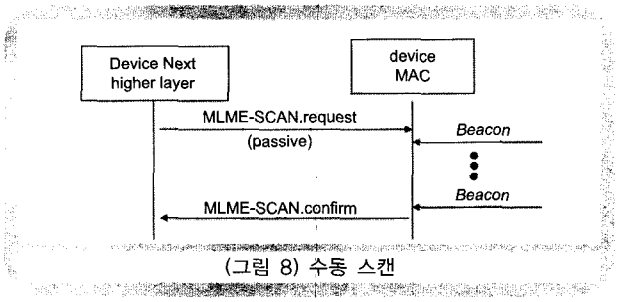
(그림 6) 능동 스캔과 ED 스캔

디바이스의 MLME(MAC sublayer management entity)는 채널 스캔 시작을 MLME-SCAN.request 프리미티브를 통해 지시받는다. 채널들은 낮은 채널 번호에서 높은 번호순으로 스캔 된다. 스캔 기간에, 디바이스는 비컨 전송을 일시 중지할 수 있으며, 스캔을 종료할 때, 디바이스는 다시 비컨을 전송할 수 있다. MLME-SCAN.confirm 프리미티브를 통해 스캔의 결과는 보고한다.

ED 스캔은 디바이스가 각 요청된 채널에서 최대 에너지 측정을 획득할 수 있게 한다. 이것은 미래의 PAN 코디네이터에 의해 새로운 PAN을 시작하기에 앞서서 이에 동작하는 채널을 선택하기 위해 사용될 수 있다. 능동 스캔은 디바이스가 그의 POS 내에서 비컨 프레임을 전송하는 임의의 코디네이터가 있는가를 찾을 수 있게 한다. 이것은 미래의 PAN 코디네이터에 의해 새로운 PAN을 시작하기에 앞서서 PAN 식별자를 선택하기 위해 사용되거나 또는 디바이스에 의해서 가입되기 전에 사용될 수 있다.

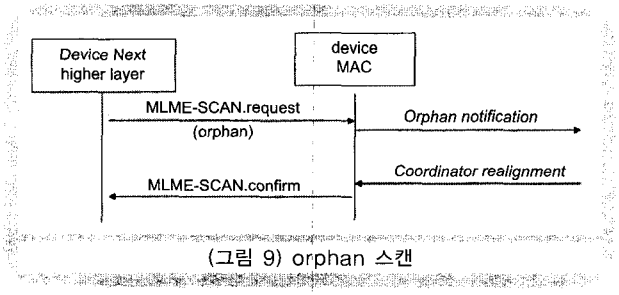


(그림 7) 능동 스캔



(그림 8) 수동 스캔

수동 스캔은 능동 스캔처럼 디바이스가 그의 POS 내에서 비컨 프레임을 전송하는 임의의 코디네이터를 찾을 수 있게 한다. 그러나 능동 스캔에서와 같은 비컨요청 명령어는 송출되지 않는다. 수동 스캔은 디바이스에 의해서 가입되기 전에 사용된다.

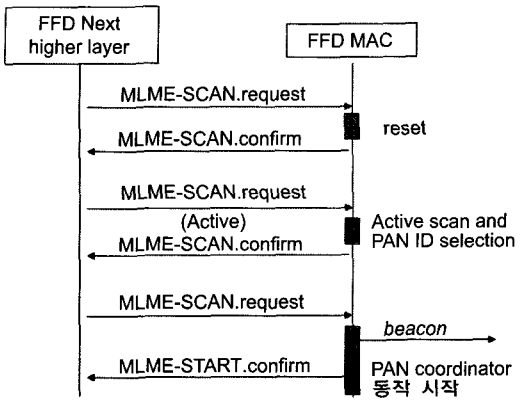


(그림 9) orphan 스캔

orphan 스캔은 디바이스가 동기화를 잃어버린 다음에 그의 코디네이터를 다시 찾을 수 있게 한다. orphan 스캔 동안 MAC 부계층은 코디네이터 재정렬 명령어 프레임이 아닌 PHY 데이터 서비스로 수신되는 모든 프레임을 폐기한다.

5. PAN의 시작과 재정렬

PAN은 MLME-RESET.request 프리미티브를 보내어 먼저 MAC 부계층 리셋을 수행하고, 능동채널 스캔과 적절한 PAN 식별자 선택 후에 FFD에 의해서만 시작된다. 능동채널 스캔 절차에서 주어지는 PAN 서술어들의 목록으로부터 적절한 PAN 식별자를 선택하는 알고리즘은 표준안의 범위에서 벗어난다.



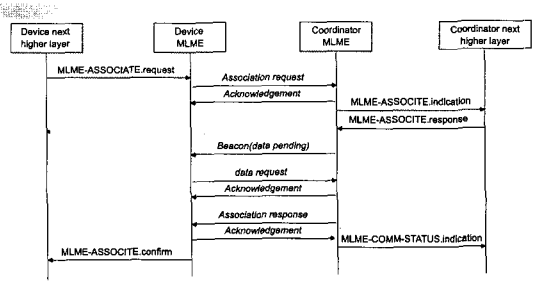
(그림 10) PAN의 시작

만약 코디네이터가 PAN 재정렬 파라미터가 설정된 MLME-START.request 프리미티브를 수신하면, 코디네이터는 코디네이터 재정렬 명령어 송출을 시도한다. 만약 코디네이터가 이미 비컨을 전송중일 때 프리미티브가 수신된 경우는, 계획된 비컨은 현재 채널에서 현재 채널의 슈퍼프레임구성을 사용하여 전송되며, 프레임제어필드의 프레임펜딩 서브필드는 1로 설정된다. 비컨 전송 바로 뒤에, 코디네이터 재정렬 명령어가 현재 채널에서 CSMA-CA를 사용하여 전송된다. 만약 코디네이터가 아직 비컨을 전송하지 않았을 때 프리미티브가 수신되면, 코디네이터 재정렬 명령어가 현재 채널에서 CSMA-CA를 사용하여 전송된다. 코디네이터 재정렬 명령어 전송이 성공하면, 새로운 슈퍼프레임구성과 채널파라미터들이, 만약 코디네이터가 이미 비컨을 전송하지 않았다면 즉시 동작하게 되고, 또는 전송 중이었으면 이어지는 계획된 비컨에서 동작하게 된다.

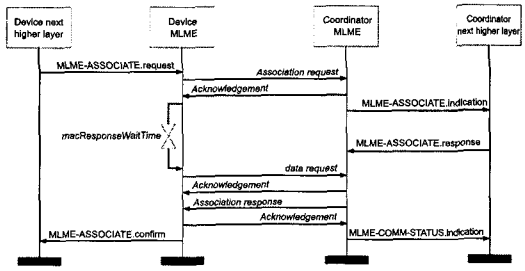
만약 디바이스가 가입되어 있는 코디네이터를 통해 코디네이터 재정렬 명령어를 받으면, 디바이스의 MLME는 MLME-SYNC-LOSS.indication 프리미티브를 차상위 계층으로 보낸다.

6. 가입(Association)

디바이스는 먼저 채널 스캔을 수행한 다음에만 가입을 시도할 수 있는데, 능동채널 스캔이나 혹은 수동채널 스캔을 수행한다. 채널 스캔의 결과는 적절한 PAN을 선택하는데 사용된다. 적절한 PAN을 선택하는 알고리즘은 채널 스캔 절차로부터 반환되는 PAN 서술어들의 목록과 관련 있는데 이는 표준안의 범위를 벗어난다. 가입할 PAN을 선택한 다음에 차상위 계층은 MLME-ASSOCIATE.request 프리미티브를 통해 가입에 필요한 정보들을 보낸다.



(그림 11) 비컨 사용 PAN에서의 가입



(그림 12) 비컨 비사용 PAN에서의 가입

코디네이터는 가입이 허용되는 것으로 설정된 경우에만 가입을 허용한다. 유사하게 디바이스는 스캔 절차의 결과에서 표시된 현재 가입을 허용하는 코디네이터를 통해서만 PAN에 가입하는 것을 시도한다. 만약 가입 허용이 불가로 설정된 코디네이터가 가입요청 명령어를 디바이스로부터 수신하면, 이 명령어는 무시 된다. 비컨 사용 PAN에서 가입 절차를 최적화하기 위해서, 디바이스는 사전에 가입하기를 원하는 코디네이터의 비컨을 추적하기 시작한다. 프리미티브를 통해서, PAN에 가입하기를 지시받은 디바이스는, 기존에 존재하는 PAN에 가입하는 것을 시도하며, 자신의 PAN을 시작하는 시도는 하지 않는다.

아직 가입되지 아니한 디바이스의 MAC 부계층은 PAN의 코디네이터로 가입요청 명령어를 보냄으로 가입 절차를 시작한다. 만약 가입요청 명령어가 채널 액세스 실패로 보낼 수 없다면, MAC 부계층은 차상위 계층에 통보한다. 가입요

청 명령어에 ACK 요청이 포함되어 있기 때문에, 코디네이터는 ACK 프레임을 보내어 명령어가 수신된 것을 확인시킨다.

가입요청 명령어에 대한 ACK는 그 디바이스가 가입되었다는 것을 의미하지 않는다. 코디네이터의 차상위 계층은 PAN에 있는 현재의 자원이 다른 디바이스에게 가입을 허용하기에 충분한가를 결정할 시간이 필요하다. 차상위 계층은 지정된 시간 내에 이 결정을 내려야 한다. 만약 코디네이터의 차상위 계층은 그 디바이스가 그의 PAN에 이전에 가입되었었던 것을 발견하면, 모든 이전에 획득했던 디바이스 특성 정보를 제거한다. 만약 충분한 자원이 가용하면 디바이스의 가입이 허용되며, 차상위 계층은 16-비트 단축주소를 그 디바이스에게 할당하며, MAC 부계층은 새로운 주소와 성공적인 가입을 나타내는 상태가 포함된 가입응답 명령어를 전송시킨다. 만약 충분한 자원이 가용하지 못하면, 코디네이터의 차상위 계층은 MAC 부계층에게 통보하며, 그리고 MLME는 실패를 나타내는 상태가 포함된 가입응답 명령어를 발생시킨다. 가입응답 명령어는 간접전송을 사용하여 가입을 요청한 디바이스에게 보내지는데, 즉, 가입응답 명령어 프레임이 코디네이터의 저장된 대기 목록에 추가되고, 이 데이터 프레임은 디바이스가 자유로울 때 추출된다.

만약 가입요청 명령어의 능력정보 필드 할당주소 서브필드가 1로 설정되면, 코디네이터의 차상위 계층은 16-비트 단축주소를 할당한다. 만약 가입요청 명령어의 할당주소 서브필드가 0으로 설정되면, 16-비트 단축주소는 0xfffe가 된다. 0xfffe인 단축주소는 디바이스가 가입되었지만, 코디네이터에 의해서 단축주소가 할당되지 않은 특별한 경우이다. 이 경우에 디바이스는 네트워크에서 동작하기 위해 64-비트 확장주소만 사용한다.

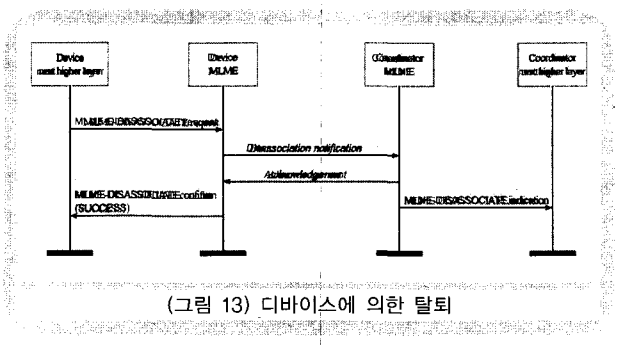
가입요청 명령어의 ACK를 수신하면, 디바이스는 지정된 시간 동안 코디네이터가 가입 결정을 내릴 때까지 대기한다. 비컨 사용 PAN에서 디바이스는 가입응답 명령어가 비컨 프레임에 표시되어 있을 때에 코디네이터로부터 이 명령어를 추출하기를 시도한다. 비컨 비사용 PAN에서 디바이스는 지정된 시간 뒤에 코디네이터로부터 가입응답 명령어를 추출하기를 시도한다.

만약 디바이스가 지정된 시간에 코디네이터로부터 가입응답 명령어 프레임을 추출하지 못했다면, MLME는 실패 상태를 가진 MLME-ASSOCIATE.confirm 프리미티브를 보내고, 가입 시도는 실패로 간주한다. 이 경우에 차상위 계층은 어떠한 비컨 추적도 종료한다.

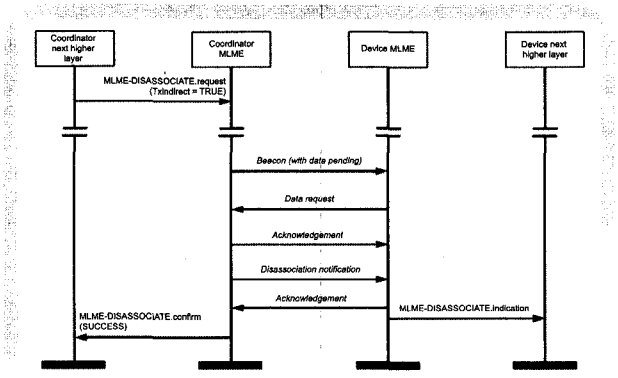
7. 탈퇴(Disassociation)

탈퇴 절차는 MLME-DISASSOCIATE.request를 차 상위 계층에서 MLME로 보냄에 의해서 시작된다. 코디네이터가 가입된 그의 디바이스들 중의 하나가 PAN에서 떠나기를 원한다면, 코디네이터의 차상위 계층은 MLME-DISASSOCIATE.request 프리미티브를 MLME로 보내고, MLME는 파라미터에 명시된 방법에 따라 탈퇴통보 명령어를 보낸다. 코디네이터의 MLME가 간접전송 방법으로 디바이스에게 탈퇴통보 명령어를 보내는 경우에는 탈퇴통보 명령어 프레임은 코디네이터의 저장된 대기 목록에 추가되고, 디바이스가 자유로울 때 추출된다. 탈퇴 명령어는 ACK 요청을 포함하고 있기 때문에, 수신 디바이스는 ACK 프레임을 보냄으로 수신을 확인한다. 만약 직접 혹은 간접 전송의 실패는, 코디네이터는 디바이스가 탈퇴 된 것으로 간주한다.

가입된 디바이스가 PAN을 떠나기를 원하면, 그 디바이스



(그림 13) 디바이스에 의한 탈퇴



(그림 14) 코디네이터에 의한 탈퇴

의 MLME는 탈퇴통보 명령어를 그의 코디네이터로 보낸다. 이 명령어가 채널 액세스 실패로 인해 보낼 수 없다면 MAC 부계층은 차상위 계층에 통보한다. 탈퇴 명령어는 ACK 요청을 포함하기 때문에, 코디네이터는 ACK 프레임을 보냄으로 수신을 확인시킨다. 여하튼 ACK가 수신되지 않아도, 디바이스는 스스로 탈퇴 된 것으로 간주한다.

8. 동기화(Synchronization)

비컨 사용 PAN에서 동기화는 비컨 프레임을 수신하고 디코딩시킴으로 수행된다. 비컨 비사용 PAN에서 동기화는 디바이스가 데이터를 수신을 위해 코디네이터를 폴링 하므로 수행된다.

비컨 사용 PAN에서 동작하는 모든 디바이스는 대기 중인 메시지를 검출하거나 혹은 비컨을 추적하기 위해 비컨 동기화를 획득할 수 있어야 한다. 디바이스들은 macPANId에 정의된 PAN 식별자를 포함한 비컨으로만 비컨 동기화 획득이 허용된다. 만약 macPANId가 브로드캐스트 PAN 식별자(0xffff)를 정의하면, 디바이스는 비컨 동기화 획득을 시도하지 않는다.

디바이스는 MLME-SYNC.request 프리미티브를 통해 비컨 획득에 대한 시도를 지시받는다. 만약 추적이 MLME-SYNC.request 프리미티브에 정의되면, 디바이스는 비컨 획득하기를 시도하며, 그의 수신기를 주기적인 시간적으로 활동시켜 비컨을 계속해서 추적한다. 만약 추적이 정의되어 있지 않으면, 디바이스는 단지 한번 비컨 획득을 시도하거나 또는 만약 추적이 그전의 요청에 의해 활성화되어 있다면 다음 비컨 뒤에 추적을 종료한다.

비컨 비사용 PAN에서 MLME-POLL.request 프리미티브를 수신하는 것으로 디바이스는 코디네이터로의 폴링을 지시받는다. 이 프리미티브를 수신하면, MLME는 코디네이터로부터 대기 중에 있는 데이터를 추출하는 절차를 따른다.

만약 차상위 계층이 그의 데이터 전송 요청에 대해 반복적인 통신 실패를 수신하면, orphan 되었다고 결론 내릴 수 있다. 단일 통신 실패는 디바이스의 트랜잭션이 코디네이터에 도달하는 것이 실패하면 일어나며, 즉, 데이터를 보냄에 있어서 지정된 재시도 후에도 ACK가 수신되지 않는 것이다. 차상위 계층이 orphan 되었다고 결론 내리면, MLME에 Orphan 디바이스 재정렬 절차나 혹은 MAC 부계층을 리셋 후에 가입 절차를 수행하도록 지시한다. 만약 Orphan 디바이스 재정렬 절차 수행을 차상위 계층에서 결정된다면, 파라미터가 orphan 스캔으로 설정되고 스캔 될 채널의 목록이 포함된 MLME-SCAN.request 프리미티브가 보내진다. 이 프리미티브를 수신하면, MAC 부계층은 orphan 스캔을 시작한다.

9. GTS 할당 및 관리

GTS는 디바이스에게 전적으로 전용되는 슈퍼프레임의 어느 한 구간에 있는 채널에서 그 디바이스가 동작하도록 허용한다. GTS는 PAN 코디네이터에 의해서만 할당되어야 하며, GTS는 PAN 코디네이터와 PAN과 가입된 디바이스 간의 통신에만 사용되어야 한다. 하나의 GTS는 하나 또는 그 이상의 슈퍼프레임 슬롯들까지 확장될 수 있다. 슈퍼프레임에서 충분한 용량이 있다면 PAN 코디네이터는 동시에 7개까지 GTS를 할당할 수 있다.

GTS 요청의 요구사항과 슈퍼프레임에서 현재 가용한 용량에 기초하여 GTS를 할당할 것인가를 PAN 코디네이터가 결정하는 것과 함께 GTS는 사용되기 전에 할당되어야 한다. GTS는 선입선처리(first-come-first-served) 근거로 할당되어야 하며, 모든 GTS는 슈퍼프레임의 끝에 그리고 CAP 후에 인접해서 놓여야 한다. 각 GTS는 더 이상 요구되지 않을 때 할당을 해제해야 하고, GTS는 PAN 코디네이터의 재량에 따라 언제든지 할당이 해제될 수 있으며, 또는 GTS를 처음 요구했던 디바이스에 의해서 할당이 해제될 수 있다. GTS를 할당 받은 디바이스는 CAP에서도 동작할 수 있다.

할당된 GTS에서 전송되는 데이터 프레임은 오직 단축주소만을 사용해야 한다.

GTS의 관리는 PAN 코디네이터에 의해서만 이루어져야 한다. GTS를 관리하기 위해서 PAN 코디네이터는 7개 GTS를 관리하는데 필요한 모드 정보를 저장할 수 있어야 한다. 각 GTS를 위해서 PAN 코디네이터는 자신의 시작 슬롯, 길이, 방향 및 가입된 디바이스 주소를 저장할 수 있어야 한다.

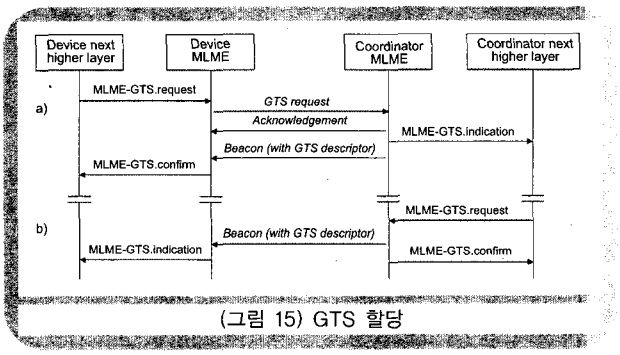
GTS 방향은 GTS를 소유하는 디바이스로부터 데이터 흐름에 관계되는 것으로서, 송신 또는 수신으로 규정된다. 그래서 디바이스 주소 및 방향은 각 GTS를 구분해서 식별해야 한다.

각 디바이스는 하나의 송신 GTS 및/또는 하나의 수신 GTS

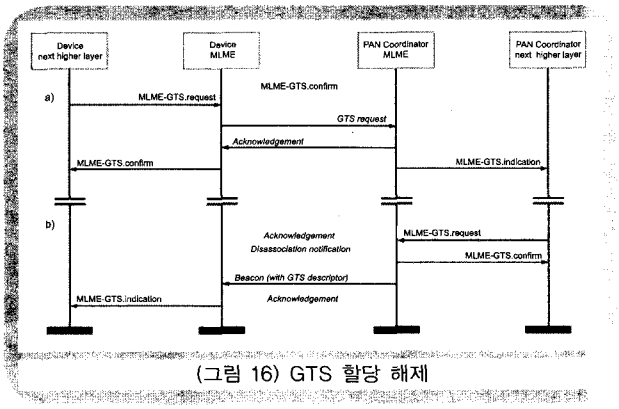
를 요구할 수 있다. 각 할당된 GTS를 위해 디바이스는 자신의 시작 슬롯, 길이 및 방향을 저장할 수 있어야 한다. 만일 디바이스가 수신 GTS를 할당 받게 되면 디바이스는 GTS의 전체를 위해 자신의 수신기를 활성화해야 한다. 동일한 방법으로 디바이스가 송신 GTS를 할당 받게 되면 GTS의 전체를 위해 PAN 코디네이터는 자신의 수신기를 활성화해야 한다. 만일 데이터 프레임이 수신 GTS 동안 수신되고 ACK가 요구된다면 디바이스는 보통 ACK 프레임을 송신해야 한다. 유사하게, 디바이스는 송신 GTS 동안 ACK 프레임을 수신할 수 있어야 한다.

디바이스는 현재 비컨을 추적하고 있는 경우에만 GTS를 할당하고 사용하도록 시도해야 한다. MLME는 비컨 추적이 설정된 MLME-SYNC.request 프리미티브를 보냄으로써 비컨들을 추적하도록 지시받는다. 만일 디바이스가 PAN 코디네이터와의 동기를 잃는다면 모든 자신의 GTS 할당은 손실되어야 한다. GTS의 사용은 선택 사양이다.

PAN 코디네이터는 최소 CAP 길이를 보존해야 하고 최소 CAP가 만족되지 않을 경우 사전 조치를 해야 한다. 그러나 GTS 유지관리를 수행하기 위해 필요한 비컨 프레임 길이에



(그림 15) GTS 할당

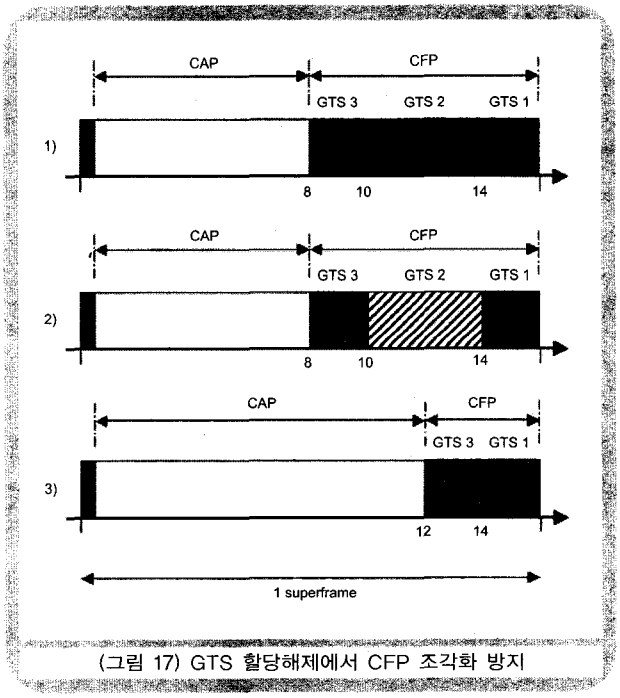


(그림 16) GTS 할당 해제

서의 임시적인 증가를 수용하는 예외가 허용된다.

디바이스들은 GTS 특성을 필요로 하는 응용의 요구사항에 따라 설정된 MLME-GTS.request 프리미티브를 통하여, 디바이스에 의해서(그림 15a) 또는 코디네이터에 의해서 (그림 15b)에 나타낸 바와 같이 새로운 GTS의 할당을 받는다.

디바이스는 MLME-GTS.request 프리미티브를 통하여 기존에 할당된 GTS의 할당해제를 지시받게 된다. 할당해제 되는 GTS는 더 이상 디바이스에 의해 사용되지 않아야 하고, 디바이스에 저장된 특성은 리셋 되어야 한다.



(그림 17) GTS 할당해제에서 CFP 조각화 방지

GTS의 할당해제는 결국 슈퍼프레임이 조각화(fragmented)될 수도 있다. 예를 들어, (그림 17)은 할당된 GTS들로 구성된 3단계 슈퍼프레임을 보여준다. 1단계에서, 3개 GTS가 할당되며 14, 10, 8 슬롯에서 각각 시작한다. 만일 GTS 2가 지금 할당해제가 되고(2단계), 어떤 조치가 일어나지 않으면 슈퍼프레임에 갭(gap)이 생길 것이다. 이것을 해결하기 위해 GTS 3은 그 갭을 채우기 위해 이동되어서 CAP의 크기를 증가시키도록 해야 할 것이다.(3단계)

PAN 코디네이터는 GTS의 할당해제에 기인하여 나타나게 되는 CFP에서 발생하는 어떠한 갭도 CAP의 길이를 최대화하기 위해 제거되는 것을 보장해야 한다.

III. IEEE 802.15.4 MAC 보안 기능

1. 보안서비스

암호 메커니즘은 아래의 보안서비스의 조합을 제공한다:

- 데이터 기밀성(Data confidentiality): 전송된 정보는 의도된 상대측에만 노출됨을 보증한다.
- 데이터 인증(Data authenticity): 전송된 정보의 소스를 보증한다.(그리고 이 정보는 경유지에서 수정되지 않는다.)
- 재연 방지(Replay protection): 복사된 정보가 탐지되는 것을 보증한다.

제공되는 프레임 보호는 실제로 프레임 단위로 달라지고, 데이터 인증의 가변 레벨이 허용되며(필요할 때 전송된 프레임에서 보안 오버헤드를 최소화하기 위해) 선택적으로는 데이터 기밀성이 허용된다. 중대한 보호가 요구될 때는 재연 방지 기술이 항상 제공된다.

암호학적 프레임 보호는 두 디바이스 간에 공유되는 하나의 키가 사용되거나 한 그룹의 디바이스 간 공유되는 하나의 키(그룹 키)가 사용될 수 있으며, 이에 따라 키 저장과 키 유지비용 대비 제공되는 암호학적 보호 수준 간의 유연성과 응용 별 특정키 사용 간의 트레이드오프를 허용한다. 만일 하나의 그룹 키가 일대일 통신에 사용되면 단지 외부 디바이스에 대해서만 보안이 제공되며, 키를 공유하는 그룹에 있는 잠재적인 악의적 디바이스에 대해서는 보안이 제공되지 않는다.

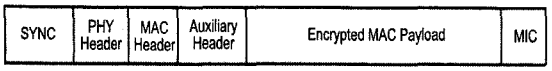
MAC 부계층에서는 모든 유입 및 유출 프레임에 대해서 프레임 보안에 기술된 메커니즘을 사용한다. 프레임 보안에 기술된 내용을 살펴보면, MAC 부계층은 상위 계층들에 의해 그렇게 하라고 요구되는 때에는 선택사양으로 특정 유입 및 유출 프레임들에 보안 서비스들을 제공하는 책임이 있다. 표준규격은 데이터 기밀성, 데이터 인증, 재연방지라는 보안 서비스를 제공하기 위해 7가지의 보안 관련 PIB attribute와 9가지 보안절차를 사용하고 있다.

2. 보안 관련 MAC PIB 속성 및 보안기능

디바이스는 옵션사항으로 보안을 구현하게 된다. 보안을 구현하지 않는 디바이스는 MAC 부계층이 유입 및 유출 프레임들에 어떠한 암호변형(cryptographic transformation)을 수행하는 메커니즘을 제공하지 않고 또한 보안과 관련된 어떠한 PIB 속성을 요구하지 않아야 한다. 보안을 구현하는 디바이스는 macSecurityEnabled 속성이 TRUE로 설정될 때, 보안과 관련되는 PIB 속성들에서의 정보를 사용하여 MAC 부계층이 유입 및 유출프레임들에 어떠한 암호변형을 수행하는 메커니즘을 제공해야 한다. 보안 관련 MAC PIB 속성들은 아래의 값을 포함한다.

- 키테이블 (macKeyTable, macKeyTableEntries)
- 디바이스테이블 (macDeviceTable, macDeviceTableEntries)
- 최소보안수준표 (macSecurityLevelTable, macSecurityLevelTableEntries)
- 프레임카운트 (macFrameCounter)
- 자동요청속성들 (macAutoRequestSecurityLevel, macAutoRequestKeyIdMode, macAutoRequestKeySource, macAutoRequestKeyIndex)
- 디폴트키소스 (macDefaultKeySource)
- PAN코디네이터주소 (macPANCoordExtendedAddress, macPANCoordShortAddress)

MAC 계층 프레임에 보안기능을 제공하기 위해 표준 규격에서는 MAC 계층 보안을 규정하고 있다. MAC 계층 보안은 MAC 계층 명령어, 비컨, 및 ACK 프레임들을 안전하게 하기 위해 사용된다. MAC 계층 데이터 프레임에 대한 보안은 단일 홉 상에 전송되는 메시지를 위한 보안을 제공하고, 멀티 홉에 대한 보안은 상위 계층에 의존한다. MAC 계층은 자신의 핵심 암호 알고리즘으로 AES (Advanced Encryption Standard)를 사용하며, AES 알고리즘을 사용하기 위한 다양한 보안 슈트들에 대해 기술하고 있다. MAC 계층은 보안 처리를 수행하지만 키를 설정하는 상위 계층에서 사용할 보안 레벨을 결정하게 된다. (그림 18)은 MAC 계층 보안을 제공하기 위해 사용되는 보안 필드와 함께 유출 프레임 구조를 보여준다. 그림에서 보듯이 MAC 계층은 보안 정보를 포함하기 위해 MAC 계층 헤드와 함께 보조 헤드를 추가한다. 메시지 무결성 코드 (MIC: message integrity code)는 0, 32, 64 or 128의 값을 가질 수 있으며, 데이터 무결성의 레벨을 결정하게 된다.



(그림 18) MAC 계층 보안기능이 포함된 프레임 구조

MAC 계층은 보안이 활성화된 프레임을 송신(수신)하는 경우에는, MAC 계층은 프레임의 목적지(발신)를 찾고, 목적지(발신)와 관련된 키를 추출하게 되며, 그 후에는 이 키를 사용하는 것으로 설계된 보안 슈트에 따라 프레임을 처리하게 된다. 각 키는 유일한 보안 슈트와 관련되며, MAC 계층 프레임 헤드는 프레임을 위한 보안이 활성 또는 비활성 되는지 여부를 규정하는 비트를 가진다. 보안 기능을 처리하기 위한 관련 MAC 보안 절차는 아래의 절차를 포함한다.

- 유출프레임보안절차(Outgoing frame security procedure)
- 유출프레임키 검색절차(Outgoing frame key retrieval procedure)
- 유입프레임보안절차(Incoming frame security procedure)
- 유입프레임 보안요소추출절차(Incoming frame security material retrieval procedure)
- KeyDescriptor 룩 업 절 차 (KeyDescriptor lookup procedure)
- 블랙리스트확인절차(Blacklist checking procedure)
- DeviceDescriptor 룩업절차(DeviceDescriptor lookup procedure)

〈표 1〉 IEEE 802.15.4-2003과 2006의 보안서비스 및 보안절차 차이점 비교

	2003	2006
보안 서비스	- Access control - Data encryption - Frame integrity - Sequential freshness	- Data confidentiality - Data authenticity - Replay protection
보안 절차	- ACL mode - Unsecured mode - Secured mode · Processing outgoing frames in secured mode · Processing incoming frames in secured mode	- Outgoing frame security procedure - Outgoing frame key retrieval procedure - Incoming frame security procedure - Incoming frame security material retrieval procedure - KeyDescriptor lookup procedure - Blacklist checking procedure - DeviceDescriptor lookup procedure - Incoming security level checking procedure - Incoming key usage policy checking procedure

- 유입보안수준확인 절차 (Incoming security level checking procedure)
- 유입키사용정책확인 절차 (Incoming key usage policy checking procedure)

〈표 1〉에서는 IEEE 802.15.4-2003과 2006의 보안서비스 및 보안절차의 차이점 비교결과를 나타내었다. 표에서 보듯이 보안서비스를 접근제어, 데이터암호, 프레임 무결성, 시퀀스 프레쉬니스 등 기술적 용어로 나누던 것을 보안서비스의 의미를 사용자가 더욱 명확히 이해할 수 있도록 데이터 기밀성, 데이터 인증, 재연방지로 변경하였고, 보안 키 사용의 유연성을 높이기 위해 보안절차를 3가지 모드에서 9가지 절차로 세분화하였다. 이에 따라 IEEE 802.15.4-2006에서는 보안 관련 MAC PIB 속성들도 2003에 비해 보다 세분화되었다.

IV. 결 론

무선 센서 네트워크 또는 무선 에드혹 네트워크는 아주 제한적인 전력 소모가 요구되는 고정형, 휴대형 또는 이동형 디바이스의 저속 데이터 전송속도의 무선 통신 기술이 필요한 분야로, IEEE 802.15.4 물리 계층과 MAC 계층의 표준안 제정에 따라 연구 개발에 박차를 가할 수 있게 되었다.

본고에서는 IEEE 802.15.4 MAC 기능의 핵심적인 부분만 간략히 기술하였다. 즉, 슈퍼프레임 구조, CSMA-CA 메커니즘, 데이터 전송모델, 채널 스캔, PAN의 시작과 재정렬, 가입 절차, 탈퇴 절차, 동기화, GTS 할당 및 관리 방법들이 다루어졌다.

2006 버전에서 수정된 보안기술 부분에 대해서는 상기의 MAC의 기능 설명과는 분리하여 별도로 보안 기술에 대해서 소개하였다. 보안 관점에서 보면 무선 에드혹 네트워크에서의 디바이스는 저비용이고, 컴퓨팅 파워, 가용 저장능력 및 전원 사용 능력에 극히 제한적이어서, 암호 알고리즘과 프로토콜의 선택에서 제한적일 수밖에 없고 보안 구조의 설계에 제약이 따른다. 따라서 대부분의 보안 기능들은 상위 계층에 구현될 수 있을 것이며, 무선 에드혹 네트워크에서의 데이터 보호를 위해 MAC 계층과 상위 계층과의 긴밀한 협

력 관계가 요구되는데, 이 부분에 대한 연구가 앞으로 계속 진행되어야 할 것으로 보인다.

추후 계획된 표준 개정에서는 성능을 더 개선할 수 있으면서 정확한 실시간 위치 서비스가 가능한 새로운 무선 물리 계층에 대한 사항이 추가될 예정이다.

참고문헌

[1] IEEE Std 802.15.4, Part 15.4: Wireless Medium Access Control(MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs), 1 October 2003.

[2] IEEE Std 802.15.4, Part 15.4: Wireless Medium Access Control(MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs), 8 September 2006.

[3] S. C. Ergen. "ZigBee/IEEE 802.15.4 Summary", 10 September 2004(http://www.eecs.berkeley.edu/~csinem/academic/publications/zigbee.pdf).

[4] P. Raronti, et al. "Wireless sensor networks: A survey on the state of the art and the 802.15.4 and ZigBee standards", Computer Communications archive Volume 30 , Issue 7 , pp. 1655-1695, May 2006.

약 력

조 무 호

1980년 경북대학교 학사
1989년 청주대학교 석사
1998년 충북대학교 박사
1983년 ~ 2000년 한국전자통신연구원 이동통신연구소 책임연구원
2000년 ~ 현재 경주대학교 교수
관심분야 : WPAN, 센서네트워크, 홈네트워크 MAC 기술

김 광 식

1991년 경북대학교 학사
1997년 충북대학교 석사
2000년 충북대학교 박사
1991년 ~ 2000년 한국전자통신연구원 무선방송연구소 선임연구원
2000년 ~ 2002년 (주)투니텔 연구소장
2002년 ~ 2005년 한국전자통신연구원 정보보호연구단 선임연구원
2005년 ~ 현재 특허청 사무관
관심분야 : CDMA이동통신, 네트워크정보보호, WPAN, 표준특허 정책