LR-WPAN 환경에서 이동성지원을 위한 매커니즘 설계

박철현° 홍충선
경희대학교 컴퓨터공학과
khchpark@networking.khu.ac.kr°, cshong@khu.ac.kr

A Design of Mechanism for Mobility in LR-WPAN Environment

Chul Hyun Park° Choong Seon Hong
Dept. of Computer Engineering , Kyung Hee University Graduate School

요 약

IEEE 802.15.4 LR-WPAN기술은 250Kbps의 낮은 전송속도와 저렴한 비용, 그리고 긴 배터리 수명과 간단한 구조 및 연결성을 제공하여, 10m 이내의 작은 범위 내에서 무선 연결을 요구하는 분야에 적합한 표준으로 개발되었다. 그에 따른 응용으로는 홈네트워크 및 제어를 위한 용도로 사용될 수 있다. 하지만 IEEE 802.15.4 LR-WPAN에는 이동성에 대한 기능 및 지원을 고려하지 않고 설계되었기 때문에, 응용서비스 제공시 제약사항이 존재한다. 본 논문에서는 WPAN 디바이스(IEEE 802.15.4)가 동일한 PAN(Personal Area Network)에서 안전하게 이동할 수 있는 모델을 제시한다.

1. 서 론

최근 보급이 진전되고 있는 홈네트워크 산업은 가정 내 가전기기의 디지털화와 인터넷 이용의 확산으로 TV, 컴퓨터, 디지털 카메라, 가전기기(냉장고, 세탁기, 에어콘 등), 센서장치(가스 및 전등 제어) 등 모든 가전기기들의 상호 통신은 물론 외부에서도 원격 제어의 필요성과 그 편리성에 따라 향후 급격히 증가 될 것으로 예상된다. 가정 내 디지털기기의 증가에 따라 유선은 기존의 가정에서는 새로운 배선 공사가 요구되거나, 다양해진 기기(TV, 리모콘, PDA, 디지털 카메라 등)들을 수용하기에는 적합하지 않다.

무선 네트워크 기술은 약 50~100m영역 내에서 데이터 전송을 위한 WLAN기술과 비교적 짧은 거리(10m정도) 내에서 비교적 적은 사용자간에 정보를 전달하는 데 목적이 있는 저 전력소모 네트워크 WPAN 기술이 현재 표준화 되고 있으나, 가정 내의 활동 영역과 이동성 및 가전기기의 특성을 고려해 보면, 개선해야 할 점이 많이 드러나고 있다. 본 연구에서는 WPAN 디바이스(IEEE 802.15.4)가 동일한 PAN(Personal Area Network)[1]에서 안전하게 이동할 수 있는 모델을 제시한다.

2. IEEE 802.15.4 네트워크 구성 및 보안

IEEE 802.15.4 LR WPAN기술은 250Kbps의 낮은 전송속도와 저렴한 비용, 그리고 장시간의 배터리 수명과 간결한 구조 및 연결성을 제공하여, 10m 이내의 작은 범위 내에서 무선 연결을 요구하는 분야에 적합한 표준으로 개발되었다. 주요 적용 분야는 홈오토메이션이나 상황인지 시스템, 센서 및 모니터링, 제어 시스템 등으로 활용 할 수 있다.

디바이스 타입으로는 FFD(Full Function Device)[1][2]와 RFD(Reduced Fuction Device)[1][2]가 있다. FFD는 FFD 또는 RFD와 통신할 수 있으며, 팬 코디네이터(PAN Coordinator)[1][4], 코디네이터(Coordinator)[1] 그리고 디바이스(Device)로 동작할 수 있다. 또한 최소의 리소스와 메모리 용량을 갖는 RFD는 FFD와 통신이 가능하며, RFD간에는 통신할 수 없다. 또한 디바이스로만 동작이 가능하다. 또한 가능한 네트워크 구성으로는 Star, Peer-to-Peer 구조가 가능하다. 주소는 16bit 또는 64bit 주소를 사용한다. 그리고 코디네이터는 네트워크 설정, 비컨 전송, 노드 관리, 노드 정보 저장 등의 기능을 수행할 수 있다.

보안 관련 서비스로는 MAC의 PIB[1]에 의해서 제어되는데, unsecured모드[1][2], ACL모드[1][2] 그리고 secured모드[1][2]로 크게 3가지 모드로 동작한다. 지원되는 보안 서비스로는 접근제어, 데이터 암호화, 프레임 무결성[4], Sequential Freshness[1][2][3][4]가 있다. Unsecured 모드에서는 보안에 대한 어떤 서비스도 제공하지 않는다[2]. 이 모드는 보안적인 요소들이 요구되지 않는 서비스에 적합하다. 또한 물리적으로 안전해, 별다른 보안적인 요소가 필요 없는 경우에 사용 될 수 있다. ACL모드에서, MAC에는 통신할 수 있는 디바이스에 대한 리스트를 저장하고 있다. 하지만 ACL모드에서는 암호화에 대한 서비스를 제공하지 않는다. Secured모드는 ACL을 이용한 접근제어 및 데이터 암호화, 프레임 무결성, Sequential Freshness을 지원한다. Security Suite에 따라 지원되는 기능이 조금씩 차이는 있지만 이 모드에서는 기본적으로 접근제어를 수행하도록 설계되어 있다[2].

Unsecured모드를 제외하고 Security를 활성화된 상태로 통신하는 경우, 장치 간의 유효한 링크는 ACL(Access Control List)에 저장된 장치의 정보를 기반으로 판별한다. 즉, 장치는 들어오는 프레임의 근원지 장치의 정보가 ACL

This work was supported by MIC

에 없다면, 그 프레임은 폐기한다. 링크를 성립하는데 있어, ACL정보는 가장 중요한 정보이다. ACL은 Address, PanID[1], 보안 레벨을 정의하는 SecuritySuite[1] 그리고 링크사이에서 사용되는 Key를 포함하는 SecurityMeterial[1]로 구성되어있다.

3. 제 안 사 항

기존 시스템에서 디바이스의 이동에 따른 결합 후 재인증 절차를 수행해야 하는 비효율성과 그에 따른 디바이스 신뢰성에 대한 문제에 대해서 설명하고 이를 개선하기 위한 방안에 대해서 설명한다.

3.1 기존 IEEE 802.15.4 에서의 이동성

IEEE 802.15.4에서 디바이스와 코디네이터 사이에 결합(association)을 하기 위한 절차를 그림 1과 같다.
디바이스는 코디네이터 에게 결합 요청 명령(Association request command)[1][2]를 보낸다. 코디네이터는 상황에 맞는(수락 또는 거절) Association request command를 보낸다. 결합이 성립된 후 상위 레이어의 정해진 절차에 따라 인증(Authentication)하게 된다. 즉, 장치와 장치사이의 결합(association)만을 정의하고 있고, 인증을 위한 절차는 상위 정의하도록 하고 있다.

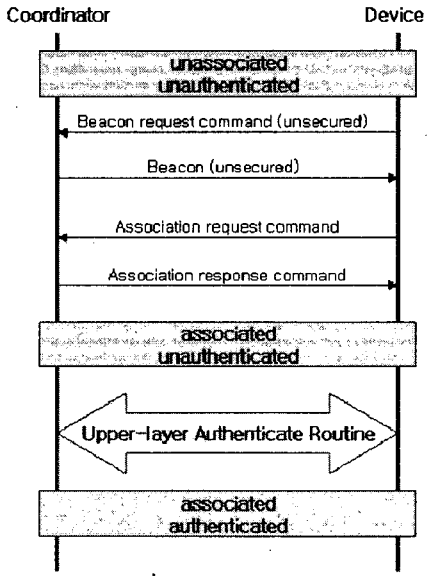

그림 1. Association 절차

이러한 절차는 그림 2에서와 같이, 동일 PAN내에서 디바이스가 이동해 다른 코디네이터에게 결합을 요청할 때, 재인증을 받아야 하며, 재인증시 신뢰성에대한 문제를 야기할 수 있다.
그림 2는 디바이스가 동일한 PAN환경에서 이동하는 겨우를 보여준다. e는 디바이스를 나타내며, a,b,c,e는 코디네이터를 의미한다. 디바이스 e는 코디네이터 a와 결합과 인증과정을 거쳐 신뢰된 링크가 성립된 상태이다. 또한 코디네이터 a-b-c-d도 신뢰된 링크를 수립하고 연결되어 있는 상태이다. 디바이스 e는 코디네이터 b와 서비스를 위한 멀티 홉(multi-hop) 통신을 하고 있는 상태에서 디바이스 e가 f방향으로 이동할 경우, 코디네이터 a의 통신 영역에서 벗어나기 때문에 e와 b는 통신을 할 수 없게 된다.
e가 방향 f로 이동한 후에, e는 원활한 통신을 위한 scan 절차를 통해 통신이 가능한 d를 발견하고, d와 결합(Association)을 시도 할 것이다. 하지만 d는 e에 대한 정보를 가지고 있지 않기 때문에, 신뢰성 있는 링크를 수립할 수 없기 때문에, d는 b와의 서비스를 위한 통신을 할 수 없다.

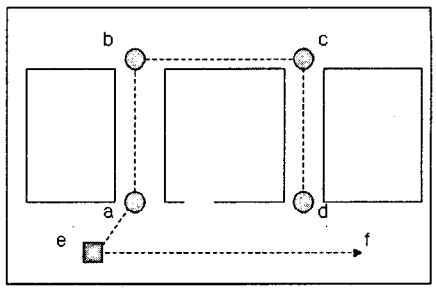

그림 2. 동일 PAN에서 디바이스의 이동

3.2 개선 방안

앞에서 제시한 문제는, 디바이스의 결합을 수용하는 코디네이터가 디바이스에 대한 정보를 보유하고 있다면 해결될 수 있다. 즉, 디바이스가 이동하는 경우, 디바이스는 결합을 요청하는 코디네이터에게 Association request command (결합 요청 명령)을 보내는 대신 제안하는 Re-Association request command(재결합 요청 명령)을 보내고, 새로운 코디네이터는 이전의 코디네이터에게 디바이스의 정보(ACL)를 전달 받는 방법을 통해 해결 될 수 있다. 그림 3은 위에서 설명한 절차를 보여준다.

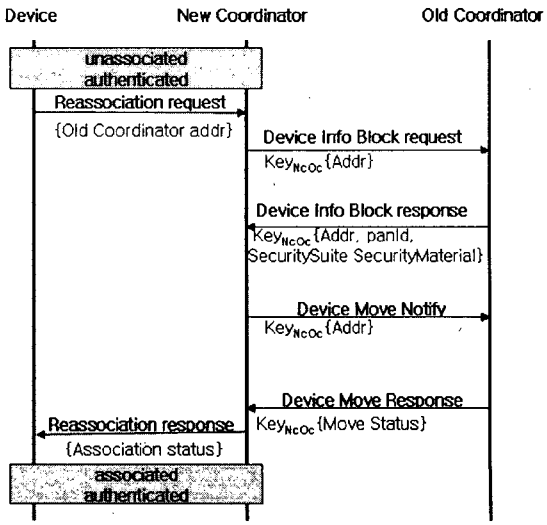

그림 3. 제안하는 Re-association 절차

디바이스는 새로운 코디네이터에게 이전의 코디네이터의 주소를 포함하는 Re-association request명령을 보내고, 새로운 코디네이터는 이전의 코디네이터에게 디바이스의 정보(Address, panID, SecurityMaterial, SecuritySuite)를 요청하고 받게 된다. Coordinator간의 통신은 미리 설정된 정보에 의해서, IEEE 802.15.4에서 표준으로 사용되는 AES암호화 알고리즘으로 암호화된 통신을 하게 된다. 즉, 디바이스의 정보는 암호화 되어 이전 코디네이터로부터 새로운 코디네이터로 전송되고, 새로운 코디네이터와 디바이스는 통신이 가능한 상태로 된다. 그리고 Device의 이동을 통지하고(Device move Notify) 그에 대한 응답을 받고, 코디네이터간의 통신을 마친다. 이동에 대한 통지는 OSI참조 모델에서의 네트워크 계층에서 라우팅을 결정하는데 사용될 수 있으며, 이전의 코디네이터가 저장하고 있는 디바이스의 정보를 삭제하는데 사용될 수 있다. 디바이스의 정보에 대한 삭제 여부는 시스템의 목적 및 능력을 고려해서 결정되어야 할 부분이다. 마지막으로 재결합(Re-association)에 대한 응답으로 새로운 코디네이터는 디바이스로 Re-association response 명령을 전송하고 모든 절차를 종료한다.

제안에 의해 MAC계층에 추가적으로 생성해야하는 명령으로는 재결합요청(Re-association request)와 재결합 응답(Re-association response)명령이 있다. 기존의 명령과 제안하는 명령은 표 1에서 볼 수 있으며, 명령 프레임 구조는 그림 4에서 볼 수 있다.

표 1. Command frame 종류

Command frame identifier	Command name	
0x01	Association request	
0x02	Association response	
0x03	Disassociation notification	
0x04	Data request	
0x05	PAN ID conflict notification	
0x06	Orphan notification	
0x07	Beacon request	
0x08	Coordinator realignment	
0x09	GTS request	
0x0a	Reassociation request	Reserved
0x0b	Reassociation response	0x0a – 0xff

제안한 절차대로 수행이 완료되면, 기존 시스템과 달리, 상위계층에서 이루지는 인증(Authentication)절차를 수행하지 않고, 바로 통신할 수 있다. 이는 이전의 코디네이터와 인증절차를 마치고 새로운 코디네이터로 이동했기 때문에, 이전 코디네이터와 디바이스 사이에서 맺은 인증정보를 새로운 디바이스에게 적용함으로서 추가적인 오버헤드 없이 통신할 수 있다. 즉, 디바이스는 기존에 맺은 신뢰성을 가지고 다른 코디네이터로 이동하기 때문에 안전하게 이동할 수 있다.

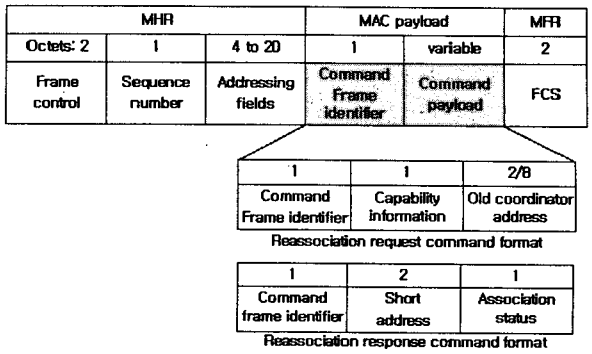

그림 4. 명령 프레임 구조

4. 결 론

본 논문에서는 IEEE 802.15.4 LR-WPAN 디바이스가 동일한 PAN(Personal Area Network)에서 안전하게 이동할 수 있는 모델을 제시하였다. 이동하는 디바이스는 새로운 코디네이터에게 Association request command(결합 요청 명령)을 보내는 대신 제안하는 Re-Association request command(재결합 요청 명령)을 보내고 코디네이터간에 디바이스의 인증정보를 주고받음으로서, 디바이스는 기존에 맺은 신뢰성을 가지고 다른 코디네이터로 이동하기 때문에 안전하게 이동할 수 있다.

향후과제로는 구현을 통해, 기존 시스템과 제안한 동작을 하는 장치와의 호환성 문제를 검증하고, 전체 시스템의 동작에 따른 오버헤드의 비교가 필요하다.

참고문헌

[1] IEEE 802.15.4-2003 IEEE Standard for Information technology - Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs)

[2] Gutierrez, Jose A., Callaway, Edgar H., Barrett, R. "Low-Rate Wireless Personal Area Networks", Inst of Elect & Electronic, 2003

[3] Naveen Sastry, "Security Considerations for IEEE 802.15.4 Networks", WiSE' 04, October 1, 2004

[4] http://www.ieee802.org/15/pub/TG4.html