지그비 네트워크에서의 동적 인증 방법1)

김성윤*, 추상호*, 김호원*
*부산대학교 컴퓨터공학과
e-mail:kims7y4@pusan.ac.kr

Dynamic Authentication Method for ZigBee Network

Seongyun Kim*, Sangho Chu*, Howon Kim*
*Dept of Computer Engineering, Pusan National University

요 약

지그비 보안 인증 방법은 총 4가지가 있으며, 하나의 네트워크는 특정 인증 방법을 선택하여 그 인증 방법을 통해서만 보안 인증이 가능하다. 이는 효율적이고 유연한 지그비 네트워크를 구성하는 데의 한 계점으로 작용하기에, 본 논문에서는 현재 표준 인증 방법의 한계점과 동적 인증 방법의 필요성, 동적 인증을 위한 표준 프로토콜 수정 내용을 제시한다. 이를 통해 타 네트워크와의 인증, 인증 방법의 다양성 부여를 통한 보안성 강화가 가능하다.

1. 서론

지그비(ZigBee)는 지그비 얼라이언스(ZigBee Alience)에서 IEEE 802.15.4의 맥(MAC)과 물리(PHY) 계층 기반에 네트워크 계층과 응용서비스 계층을 정의한 기술로, 환경에 따라 5-500m 정도의 근거리 무선 통신이 가능하고 저전력, 칩셋 가격이 저비용, 프로토콜 구현이 단순하다는 특성[1]을 가지고 있어 근거리 무선통신 네트워크 유비쿼터스 환경을 구축하는데 있어 핵심역할을 할 것으로 예상된다. 이러한 특징으로 인해 지그비는 홈 네트워크, 국방, 감시, 방법, 시설물 관리 등 매우 다양한 분야의 응용 분야에서 사용되고 있다.

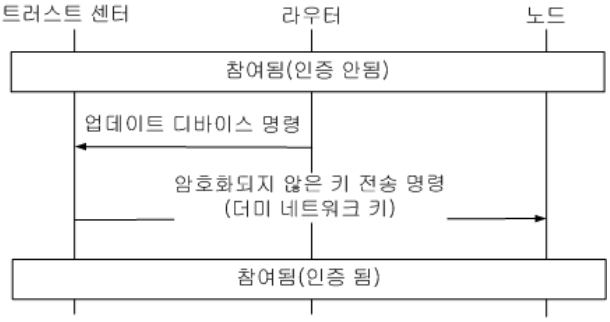
지그비 네트워크 인증(authentication)과정은 총 4가지 프로시져(procedure)로 나누어져 있고, 지그비 네트워크 사용자/설치자가 인증방법 중 하나의 방법 고정하여 선택하도록 되어있다. 하지만 고정된 인증 방법으로 인증이 이루어지기에 유연한 지그비 네트워크 구성이 힘들고, 보안 제공성의 다양화를 통한 보안성 강화 또한 제공하지 못한다. 논문의 나머지는 다음과 같이 구성된다. 2장에서 지그비 표준에서 정의되어 있는 네트워크 인증과정에 대해 알아보고, 3장에서 표준에서 제시된 인증방법의 한계점을 제시한 후 이를 개선한 지그비 네트워크 동적 인증 방법 아이디어를 제시한다. 4장에서는 결론 및 향후 연구 뱡향에 대해 기술한다.

2. 지그비 인증과정

지그비 인증과정은 지그비 노드(이후 노드)가 보안 네트워크에 참여(join)한 후에 해당 노드가 네트워크의 한 일원으로 참여할 수 있는지를 결정하는 단계이다. 지그비 표준[2]에서는 미리 설정된(preconfigured) 활성(active) 네트워크 키, 미리 설정된 트러스트 센터(trust center) 마스터(master) 키, 미리 설정된 트러스트 센터 링크(link) 키를 통해 인증하는 방법과 미리 설정된 키가 없는 경우의 총 4가지의 인증방법을 제시하고 있다. 본 장에서는 각각의 인증과정의 프로시져에 대해 살펴본다.

2.1. 미리 설정된 활성 네트워크 키를 통한 인증 과정

네트워크에 참여한 노드가 활성 네트워크 키로 미리 설정되어 있을 경우, 그림 1과 같은 프로시져를 통해 인증과정이 이루어진다.



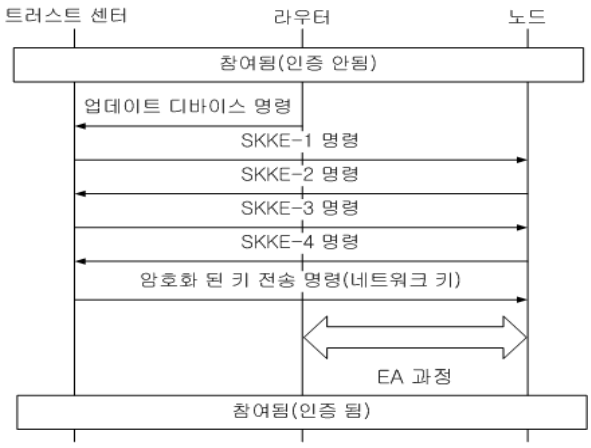
(그림 1) 활성 네트워크 키를 통한 인증 과정

참여한 노드를 인증하기 위해 라우터는 업데이트 디바이스 명령(update-device command)를 통해 해당 노드가 인증을 요청함을 트러스트 센터에 알리고, 트러스트 센터는 해당 노드를 네트워크의 일원으로 수락할지 여부를 결정하고, 수락할 경우, 네트워크 키 값이 모두 0인 더미 네트워크 키(dummy all-zero network key)를 전송(transport-key command)함으로써 인증과정이 완료된다.

1) "이 논문 또는 저서는 2010년 교육과학기술부로부터 지원받아 수행된 연구임" (지역거점연구단육성사업/차세대물류IT기술연구사업단)

2.2. 미리 설정된 트러스트 센터 마스터 키를 통한 인증 과정

네트워크에 참여한 노드가 트러스트 센터 마스터 키로 미리 설정되어 있을 경우, 그림 2와 같은 프로시저를 통해 인증과정이 이루어진다.



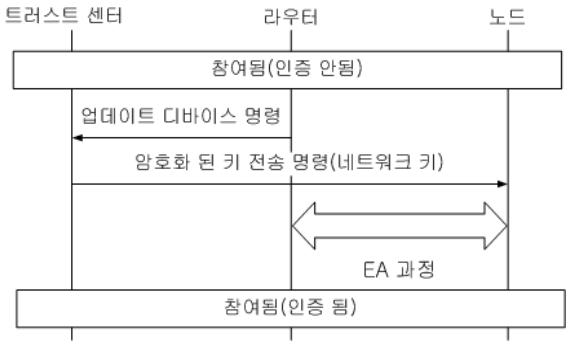
(그림 2) 트러스트 센터 마스터 키를 통한 인증 과정

참여한 노드를 인증하기 위해 라우터는 업데이트 디바이스 명령를 통해 해당 노드가 인증을 요청함을 트러스트 센터에 알리고, 트러스트 센터는 해당 노드를 일원으로 수락할 경우, SKKE(symmetric-key key establishment) 프로토콜을 수행하여 두 노드가 공유하고 있는 마스터 키를 통해 두 노드간의 링크 키를 도출한다. SKKE 프로토콜이 완료되면 트러스트 센터는 현재 활성 네트워크 키를 도출된 링크 키로 암호화 하여 해당 노드에 전송한다. 이를 받은 노드는 전송받은 활성 네트워크 키가 정당한지 여부를 확인하기 위해 EA(mutual symmetric-key entity authentication) 과정을 자신의 부모 노드(여기서는 라우터)와 수행하게 되고, EA 프로토콜이 종료되게 되면 인증이 완료된다.

2.3. 미리 설정된 트러스트 센터 링크 키를 통한 인증 과정

네트워크에 참여한 노드가 트러스트 센터 링크 키로 미리 설정되어 있을 경우, 그림 3과 같은 프로시져를 통해 인증과정이 이루어진다.

참여한 노드를 인증하기 위해 라우터는 업데이트 디바이스 명령를 통해 해당 노드가 인증을 요청함을 트러스트 센터에 알리고, 트러스트 센터는 해당 노드를 네트워크의 일원으로 수락할 경우, 이미 링크키가 존재하기에 SKKE 프로토콜을 수행하지 않고 현재 활성 네트워크 키를 해당 링크 키로 암호화 하여 해당 노드에 전송한다. 이를 받은 노드는 전송받은 네트워크 키가 맞는지 여부를 확인하기 위해 EA 과정을 수행하게 되고, EA프로토콜이 종료되게 되면 인증이 완료된다.



(그림 3) 트러스트 센터 링크 키를 통한 인증 과정

2.4. 미리 설정된 키가 없을 시의 인증과정

미리 설정된 키 값이 없을 경우, 해당 네트워크에서 트러스트 센터 마스터 키, 트러스트 센터 링크 키, 활성 네트워크 키를 통한 인증과정 중 네트워크 구성원들 간의 미리 약속된 인증 방법으로 인증을 한다. 다만 인증과정을 수행하기 전, 인증과정에 해당하는 키를 평문으로 전송을 한 이후 인증과정 수행한다는 점만 다르다. 키를 평문으로 전송하기 때문에 해당 인증과정의 사용은 권장되지 않는다.

3. 지그비 동적 네트워크 인증 방법 제시 및 활용 방안

3.1. 현재 인증 방법의 한계점

현재 지그비 네트워크 인증 과정의 한계점은 네트워크 전체가 하나의 인증과정 방식을 공유하고 있고, 해당 방식으로만 인증이 가능하다는 점이다. 즉, 해당 네트워크가 활성 네트워크 키를 통한 인증방법을 선택했다면 트러스트 센터 마스터 키 또는 트러스트 센터 링크 키를 통한 인증과정을 사용하여 인증이 불가능 하다는 점이다. 한 네트워크의 노드들이 사용할 인증과정을 약속하였기에 현재 지그비 표준하에서는 어떠한 문제점이 발생하지 않지만, 보다 유연하고 효율적인 네트워크 구성을 위해 지그비 동적 네트워크 인증 방법이 필요하다.

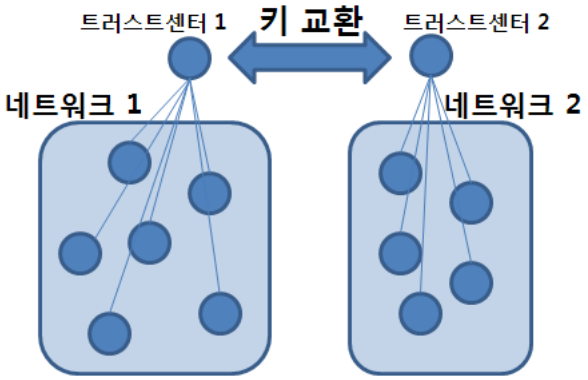
3.2. 동적 인증 방법의 필요성

지그비 표준에서는 높은 보안 모드(high security mode)와 표준 보안 모드(standard security mode)의 두 가지 보안 모드가 존재한다. 높은 보안 모드의 경우 상업(commercial)적으로 사용되는 것을 권장하고 있으며, 표준 보안 모드의 경우 거주(residential) 지역에 사용되는 것을 권장하고 있다. 이에 따라 인증 과정을 차별화 하고 있는데, 표준 보안 모드에서는 활성 네트워크 키를 통한 인증 방법을 사용하고, 높은 보안 모드에서는 활성 네트워크 키를 포함하여 트러스트 센터 마스터 키, 트러스트 센터 링크 키를 통한 인증과정이 가능하도록 되어있다.

현재 표준에서는 구현된 지그비 네트워크는 인증 방법이 하나로 고정되어 있기 때문에, 지금 인증 방법 그 이상의 높은 보안을 제공하지 못한다. 하지만 네트워크 인증

방법을 변경할 수 있다면 해당 네트워크는 더 높은 보안성을 제공할 수 있다. 즉, 활성 네트워크 키로 인증하는 네트워크에서 트러스트 센터 마스터/링크 키로의 인증과정 변경이 가능한 것이다.

또한 그림 4의 경우처럼 두 개 이상의 다른 지그비 네트워크 간의 노드 인증이 필요한 어플리케이션의 경우, 현재 표준에 따르면 해당 지그비 네트워크들이 같은 인증방식을 사용해야 인증이 되는 반면, 동적으로 인증방법을 선택할 수 있다면 트러스트 센터는 노드에 맞는 인증방법으로 선택하여 인증과정을 처리할 수 있어 보다 효율적이고 유연한 네트워크 구성이 가능하게 된다. 예를 들어, 그림 4의 네트워크 1이 활성 네트워크 키를 통해 인증하고, 네트워크 2가 트러스트센터 링크 키를 통해 인증을 한다고 가정했을 때, 네트워크 1의 한 노드가 네트워크 2로 이동하였을 시, 현재 지그비 표준으로는 인증할 수 있는 방법이 존재하지 않는다. 하지만 동적으로 인증방법을 선택할 수 있다면, 네트워크 2의 트러스트 센터는 해당 노드의 인증방법을 확인하고 해당 인증방법으로 인증이 가능하게 된다. 이처럼 더 유연한 네트워크 구성이 가능하다.

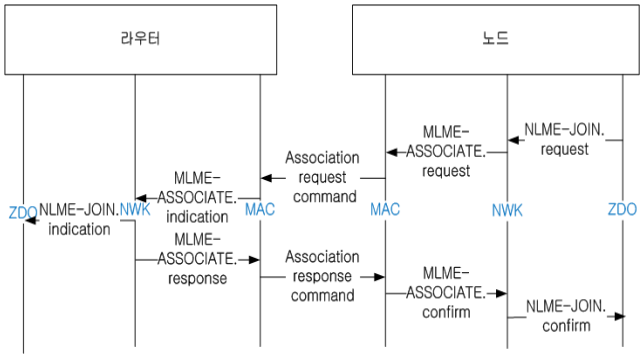


(그림 4) 다른 네트워크 간의 상호 인증이 가능하게 하는 동적 인증 방법

3.3. 지그비 동적 인증 방법 프로토콜

지그비 네트워크에서 노드가 동적으로 인증 방법을 선택하고 트러스트 센터가 해당 노드의 인증 방법을 확인하기 위해서는 노드가 인증 방법 즉, 활성 네트워크 키, 트러스트 센터 마스터/링크 키를 통한 인증 중 자신의 인증 방법 정보를 라우터로 전송하고, 이를 트러스트 센터까지 전송할 수 있도록 수정하여야 한다. 그러기 위해서 인증과정이 수행되기 이전의 참여(join)과정에서 노드는 인증방법을 전송하여야 한다. 지그비 네트워크 참여 과정은 그림 5와 같다.

지그비 표준에서 노드는 참여 과정의 시작으로 NLME-JOIN.requet 프리미티브를 호출하는데, 해당 프리미티브에 인증종류 정보를 추가하도록 수정하여야 하고, 이에 응답하는 NLME-JOIN.indication 프리미티브 또한 인증종류 정보를 담을 수 있도록 수정하여야 한다. NLME-JOIN.request에서 호출되는 IEEE 802.15.4 MLME-ASSOCIATE.request 프리미티브 파라미터를 표1에서 살펴보면, 지그비 표준에서 사용하지 않는 KeyIdMode 파라미터가 존재하는 것을 확인할 수 있다.[3] 이를 활용해서 인증종류 정보를 전송할 수 있으며, MLME- ASSOCIATE.indication 프리미티브 또한 동일한 파라미터를 사용할 수 있다. NLME-JOIN.indication 이후 발생하는 인증 프리미티브인 APSME-UPDATE-DEVICE.request/indication의 경우에도 해당 노드의 인증종류 정보를 전송할 수 있도록 수정하여야 한다.



(그림 5) 지그비 네트워크 참여 과정

<표 1>MLME-ASSOCIATE.request 프리미티브 파라미터[3]

이름	타입
LogicalChannel	정수
ChannelPage	정수
CoordAddrMode	정수
CoordPANID	정수
CoordAddress	디바이스 주소
CapabilityInformation	비트 맵
SecurityLevel	정수
KeyIdMode	정수
KeySource	0, 4, 8 바이트 셋
KeyIndex	정수

<표 2>KeyIdMode 값에 따른 키 정보

KeyIdMode 값	인증 종류
0x00	활성 네트워크 키
0x01	트러스트센터 마스터 키
0x02	트러스트센터 링크 키
0x03	키 없음

4. 결론

본 논문에서는 지그비 표준의 네트워크 보안 인증과정을 살펴보고, 이를 통하여 표준에서 제시한 인증 방법의 한계점을 알아보았다. 또한 동적 인증 방법의 필요성과 해당 프로토콜을 위해 수정해야할 내용을 알아보았다. 기존 네트워크 인증방법은 변경 할 수가 없어서 유연한 네트워크 구성이 어렵고 기존 네트워크에 더 높은 보안성을 제공하기 어려웠던 반면, 본 논문에서 제시한 동적 인증 방법을 적용할 경우 노드의 인증 방법을 트러스트 센터가 알게 함으로써 이에 따라 트러스트 센터가 동적으로 해당 노드의 인증을 가능하게 할 수 있었다. 본 연구는 향후 다른 네트워크 간의 상호 인증과 안전한 키 교환에 활용될 수 있을 것으로 사려 된다.

참고문헌

[1] Patrick Kinney "ZigBee Technology: Wireless Control that Simply Works“ http://www.zigbee.org/LearnMore/WhitePapers.aspx

[2] ZigBee Alliance, “ZigBee Specification”, Document 053474r17, 2008년 1월

[3] IEEE computer society, “Part 15.4: Wireless Medium Access Control(MAC) and Physical Layer(PHY) Specifications for Low-Rate Wireless Personal Area Networks(WPANs)”, 2006년 6월