논문 2010-47TC-4-9

LR-WPAN에서 사전인증기법을 이용한 기기 인증 프로토콜

(Device Authentication Protocol for LR-WPAN using Pre-Authentication Mechanism)

이 성 형*, 김 재 현**

(Sung-Hyung Lee and Jae-Hyun Kim)

요 약

본 논문에서는 LR-WPAN을 위한 새로운 인증 프로토콜을 제안한다. 제안하는 프로토콜에서는 계층 구조를 이용한 인증을 수행하여 인증의 안전성 및 신뢰성을 확보한다. 또한 계층 구조에서 나타나는 효율성 감소 및 denial of service(DoS) 공격에 대한 취약점을 해결하기 위하여 정보 교환 횟수를 줄여 적합한 사용자 및 적합하지 않은 사용자를 인증할 때의 효율성을 제공하고 Local Authentication Key를 이용하여 트러스트 센터(trust center)와 참여자 기기 및 부모 노드와 참여자 기기 사이의 신뢰 관계를 확인한다. 제안하는 프로토콜의 성능 평가를 위하여 security 분석을 통해 안전성을 평가하며 GNY 분석을 통해 프로토콜의 신뢰성을 평가한다. 또한 DoS 공격 발생 시 네트워크에 참여중인 기기의 메시지 전송 횟수를 분석하여 DoS 공격에 대한 프로토콜의 안전성을 평가한다. 마지막으로 현재 LR-WPAN을 위한 표준인 ZigBee의 인증 프로토콜과 제안한 프로토콜을 LR-WPAN 기기에 구현하여 인증과정에 필요한 시간을 측정하고, 측정된 시간을 바탕으로 각 홉 수 별로 인증 완료 시간을 분석한다. 이 과정을 통하여 제안한 프로토콜이 기존의 인증 프로토콜보다 보안성이 강화되며 인증 완료시간을 홉 수에 따라 최대 30% 줄임을 확인하였다.

Abstract

This paper proposes a new authentication protocol for the LR-WPAN. In order to guarantee the reliability and safety of a protocol, this protocol uses the hierarchical authentication approach. In addition, in order to reduce the impact of the denial of service attack, the proposed protocol performs the authentication between a parent router and a joiner device prior to the authentication between a trust center and the joiner device. Moreover, this protocol reduces the authentication delay by decreasing the number of message exchanges during authentication procedure. This paper evaluates the safety of the proposed protocol by the security analysis and reliability of the proposed protocol by the GNY analysis. This paper also compares the number of message exchanges of the ZigBee authentication protocol and the proposed protocol when denial of service attack occurs to evaluate the resistance of the proposed protocol against the denial of service attack. We also analyze the delay for authentication of the joiner device through the implementation of both protocols. Those results show that the proposed protocol effectively protects networks from the denial of service attack and reduces the time for authenticating the joiner device up to maximum 30% as the number of hops increases.

Keywords : Authentication, LR-WPAN, SKKE, Security

I. 서 론

최근 무선 네트워크 기술과 무선기기 기술이 향상됨에 따라 이러한 기술을 이용하여 저전력, 저비용으로 무선 네트워크를 구성하는 기술에 대한 관심이 높아지고 있다. 특히 무선 네트워크 중에 낮은 송신 전력 및 낮은 전송 속도로 통신을 수행하는 네트워크를 저속 근

* 학생회원, 아주대학교 전자공학과
(Ajou University)
** 평생회원, 아주대학교 전자공학부
(Ajou University)
※ "본 연구는 지식경제부 및 정보통신산업진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음" (NIPA-2010-(C1090-1021-0011))
접수일자: 2008년11월13일, 수정완료일: 2010년4월13일

거리 무선 통신망(Low-Rate Wireless Personal Area Networks, LR-WPAN) 이라고 한다. LR-WPAN은 저전력으로 여러 기능을 오랫동안 수행할 수 있고, 저비용으로 많은 수의 기기를 이용해 네트워크를 구성할 수 있어 홈 네트워크, 산업 자동화, 건강, 군사 등에서 응용이 가능하다[1~3].

LR-WPAN에서 인증을 위하여 효율성 및 확장성이 상대적으로 좋은 분산형 인증 프로토콜(distributed authentication protocol)이 고려되고 있으나 ZigBee와 같은 표준에서는 안전성 및 신뢰성 확보를 위해 분산적으로 인증을 수행하는 방법보다는 계층 구조 및 트러스트 센터(trust center)를 이용하여 인증을 수행하는 방식을 이용한다[2]. 그러나 트러스트 센터를 이용할 경우 멀티 홉(multi-hop) 환경인 LR-WPAN에서는 트러스트 센터와 네트워크에 참여하는 참여자 기기(joiner device) 사이의 신뢰 관계뿐만 아니라 참여자 기기와 부모 노드(parent node)와의 신뢰 관계를 확인하여야 한다. 또한 트러스트 센터에 트래픽이 집중된다는 점을 고려하여야 하며 인증과정을 반복하여 트러스트 센터의 역할을 제대로 수행하기 어렵게 하는 Denial of Service(DoS)공격에 대처할 수 있어야 한다.

본 논문에서는 LR-WPAN에서 트러스트 센터를 이용하여 인증의 신뢰성 및 안전성을 확보하는 한편 트러스트 센터를 이용하는 인증 프로토콜에서 발생할 수 있는 문제점들을 해결한 새로운 인증 프로토콜을 제안한다. 제안하는 인증 프로토콜은 새로운 기기가 네트워크에 참여할 때 트러스트 센터와 바로 인증을 수행하지 않고 부모 노드와 1차적으로 인증을 수행한 후 1차 인증이 성공하였을 때 트러스트 센터와의 인증을 수행한다. 이를 통해 트러스트 센터의 부하를 줄이며 인증 반복을 이용한 DoS 공격이 이루어졌을 때의 피해를 줄인다. 또한 제안하는 프로토콜은 메시지 교환 횟수를 줄여 정보 교환 및 연산에 드는 오버헤드를 줄인다.

본 논문은 다음과 같이 구성된다. Ⅱ장에서는 현재까지 제안된 LR-WPAN을 위한 기기 인증 프로토콜과 각각의 문제점에 대해 살펴보며 Ⅲ장에서 새로운 인증 프로토콜을 제안하고 프로토콜의 세부 절차를 설명한다. Ⅳ장에서 제안한 인증 프로토콜의 성능을 평가하고 Ⅴ장에서 결론을 맺는다.

Ⅱ. 관련 연구

1. ZigBee의 인증 프로토콜

분산형 인증 프로토콜은 안전성 및 신뢰성이 부족하기 때문에 트러스트 센터를 중심으로 계층 구조를 형성하여 인증을 수행하는 프로토콜을 이용하게 된다. 이러한 인증 프로토콜 중에서 대표적인 인증 프로토콜로 ZigBee 표준의 인증 프로토콜[2]을 들 수 있다. ZigBee의 인증 프로토콜은 Symmetric-Key Key-Establishment (SKKE) 프로토콜을 이용해 트러스트 센터와 참여자 기기 사이의 인증을 수행하는 과정 및 Entity Authentication(EA) 프로토콜을 이용하여 부모 노드와 참여자 기기 사이의 인증을 수행하는 과정으로 나뉜다.

ZigBee의 인증과정은 그림 1과 같다. 그림에서 A<B>는 메시지 A를 통해 데이터 B가 전송됨을 의미한다. 또한 QEx는 기기 x가 생성한 임의의 수를 의미하며 $MacTag$는 두 기기가 주고받은 QEx 및 갖고 있던 키를 이용하여 계산한 해쉬값을 의미한다. 우선 인증 수행 이전에 트러스트 센터와 참여자 기기 사이에는 마스터키가 미리 분배되어 있고, 트러스트 센터와 부모 노드 사이에는 암호화를 위한 링크키가 생성되어 있으며 서로 네트워크 키를 알고 있다. 참여자 기기가 네트워크에 들어오면 SKKE 프로토콜을 수행해 트러스트 센터와 참여자 기기 사이의 상호 인증 및 링크키 생성을 수행한다. 이때 만약 트러스트 센터와 참여자 기기가 2홉 이상 떨어져 있는 경우 두 기기 사이에 위치한 라우터(router)들이 두 기기 사이의 메시지를 라우팅한

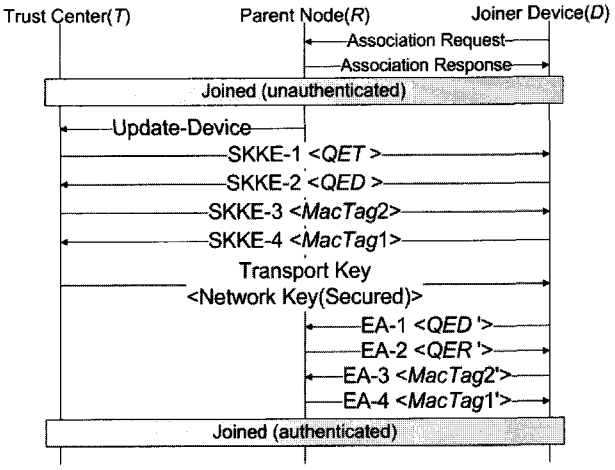

그림 1. ZigBee 기기 인증 프로토콜의 메시지 교환
Fig. 1. The device authentication procedure in ZigBee.

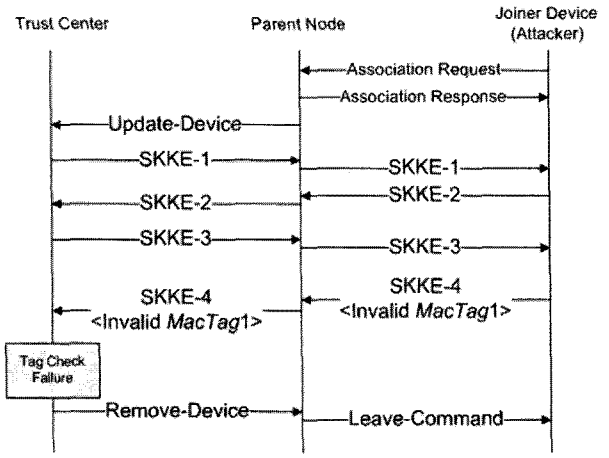

그림 2. ZigBee에서 적합하지 않은 사용자가 인증 수행 시 발생하는 메세지

Fig. 2. Exchanged messages when a malicious user tries the device authentication.

다. SKKE 프로토콜이 끝나면 트러스트 센터는 네트워크 키를 링크키로 암호화하여 참여자 기기에게 전송한다. 트러스트 센터와 참여자 기기가 1홉 떨어진 경우에는 여기서 인증이 완료되며, 2홉 이상 떨어져 있는 경우 참여자 기기가 네트워크 키를 수신 후 부모 노드와 참여자 기기가 EA을 수행해 인증과정을 완료한다.

ZigBee 보안 프로토콜에서 트러스트 센터와 참여자 기기 사이에 마스터키가 미리 설정되어 있다면, 공격자는 인증에 성공할 수 없으며 링크키나 네트워크키를 알 수 없어 임의의 메시지를 라우팅하게 할 수도 없다. 그러나 ZigBee 인증 프로토콜에서는 트러스트 센터가 SKKE 프로토콜을 시작하여 SKKE-4 메시지를 수신함으로써 참여자 기기가 트러스트 센터와 동일한 마스터키를 갖고 있는지 판단한다. 따라서 공격자 기기가 인증을 시도할 때 그림 2와 같이 트러스트 센터 및 트러스트 센터와 참여자 기기 사이에 위치하는 라우터들이 메시지를 전송하기 때문에, 공격자 기기가 인증 요청을 반복한다면 트러스트 센터 및 라우터의 전송 효율이 떨어지며 트러스트 센터나 라우터가 배터리를 소진해 네트워크 일부 또는 전체가 마비될 수 있다.

2. Parent-Child 키 연결 알고리즘

ZigBee 인증과정에서 인증에 필요한 시간을 줄이기 위해 Parent-Child 키 연결 알고리즘[3]이 제안되었다. 이 알고리즘은 라우터와 참여자 기기 사이에서만 인증을 수행하기 때문에 트러스트 센터로 데이터가 전송되지 않아 인증 반복을 이용한 공격에 대처할 수는 있다.

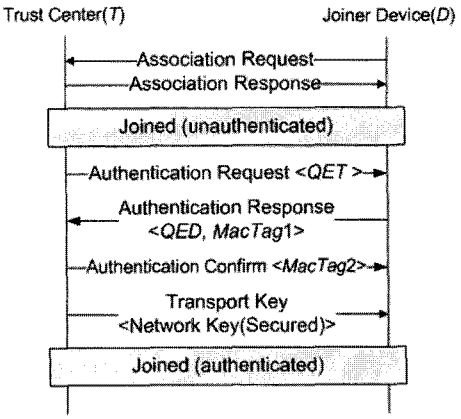

그림 3. 제안하는 인증 프로토콜의 메시지 교환 (1홉의 경우)

Fig. 3. Procedure of the proposed device authentication protocol (1-hop).

그러나 마스터키를 각 기기에 미리 설정(master key preconfigured)하는 경우에 각 기기의 마스터키가 모두 동일해야 한다는 제약이 있다. 또한 트러스트 센터와 인증을 수행하지 않아 참여자 기기가 트러스트 센터의 신뢰도를 알 수 없기 때문에 트러스트 센터가 키 유지 및 관리 작업을 수행할 때 참여자 기기가 트러스트 센터로부터 받는 정보를 신뢰할 수 없다.

III. 제안하는 인증 프로토콜

본 논문에서는 ZigBee 인증 프로토콜에서 발생하는 문제점을 해결하고 인증 과정에 필요한 시간을 줄이기 위하여 새로운 인증 프로토콜을 제안한다. 제안하는 프로토콜은 ZigBee에서 사용하는 키인 마스터키, 링크키, 네트워크키를 사용한다고 가정한다. 또한 트러스트 센터와 참여자 기기 사이에는 동일한 마스터키가 미리 분배되어 있으며 트러스트 센터와 부모 노드는 네트워크 키 및 둘 사이의 링크키를 알고 있다고 가정한다. 추가적으로 제안하는 인증 프로토콜에서는 ZigBee 인증 프로토콜의 문제점을 해결하기 위하여 부모 노드와 참여자 기기 사이에 Local Authentication Key(LAK)가 미리 분배되어 있다고 가정한다.

제안하는 프로토콜에서는 LAK를 이용하여 참여자 기기가 트러스트 센터와 인증을 수행하기 전에 부모 노드와 참여자 기기 사이에 인증을 수행하는 사전 인증(pre-authentication)을 하게 되며 이를 통해 인증 요청 반복을 이용한 DoS 공격을 방지한다. 또한, 인증에 소요되는 시간을 줄이기 위하여 인증과정에서 교환되는

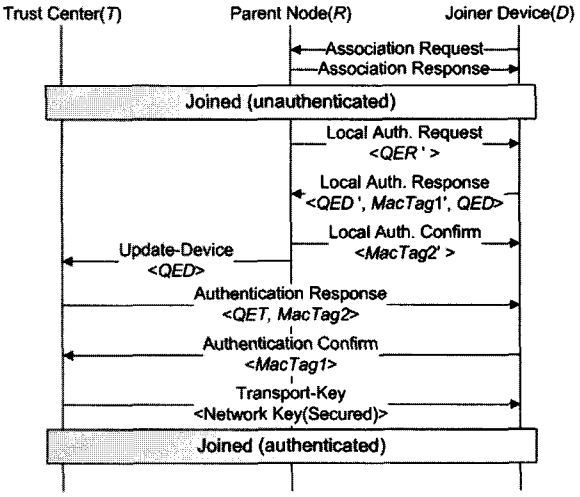

그림 4. 제안하는 인증 프로토콜의 메시지 교환 (2홉 이상의 경우)

Fig. 4. Procedure of the proposed device authentication protocol(2-hops or more).

데이터들을 가능한 적은 수의 메시지를 이용하여 교환하도록 하였다.

제안한 프로토콜에서 각 기기가 전송하는 메시지는 트러스트 센터와 참여자 기기가 1홉 떨어진 경우 그림 3과 같으며, 2홉 이상 떨어진 경우 그림 4와 같다. 다음은 제안하는 인증 프로토콜을 이용할 때 2홉 이상 떨어진 참여자 기기가 네트워크에 참여하는 경우 인증을 위한 각 기기에서의 세부 동작을 설명한 것이다. (트러스트 센터와의 인증과 라우터와의 인증에서 사용되는 데이터들을 구분하기 위하여 라우터와의 인증에 사용되는 데이터들에는 ′ 기호를 붙였다.)

가. 주요 연산

- ID_x : 기기 x의 기기 주소
- QEx 또는 QEx' : 기기 x가 생성한 16 byte 길이의 임의의 수
- $MacTag1' = h(LAK, ID_D, ID_R, QED', QER')$
- $MacTag2' = h(LAK, ID_R, ID_D, QER', QED')$
- $MacTag1 = h(MK, ID_D, ID_T, QED, QET)$
- $MacTag2 = h(MK, ID_T, ID_D, QET, QED)$
- 링크키 $= h(MK, ID_T, ID_D, QET, QED)$

($h()$는 해쉬함수를 의미한다. 링크키의 경우 $MacTag$와는 다른 해쉬함수를 사용한다.)

나. 가정

① 암호화 및 해쉬 알고리즘은 대칭키 기반 알고리즘을 이용한다.

② 모든 라우터와 모든 참여자 기기는 동일한 LAK를 가지고 있다.

③ 트러스트 센터와 부모 노드 사이에는 비밀키가 공유되어 보안이 유지된 통신을 수행할 수 있다.

④ 메시지에는 송신자의 기기 주소가 포함되어있다.

다. 트러스트 센터의 동작 절차

① 부모 노드에게서 Update-Device 메시지를 수신하면 메시지 안의 QED를 저장한다.

② QET를 생성하고 $MacTag1$, 링크키를 계산한다. QET 및 $MacTag1$을 Authentication Response메시지에 실어 참여자 기기에게 전송한다.

③ 만약 참여자 기기에게서 Authentication Confirm 메시지를 수신하면, $MacTag1$을 계산한 후 Authentication Confirm 메시지 안의 $MacTag1$과 일치하는지 확인한다. 일치하지 않을 경우 Remove-Device 메시지를 부모 노드에게 전송하고 프로토콜을 중단한다.

④ 두 $MacTag1$이 일치하는 경우 Transport-Key 메시지를 이용하여 참여자 기기에게 네트워크 키를 전송한다(링크키로 암호화 한다).

라. 부모 노드의 동작 절차

① 참여자 기기의 Association을 마치면 QER'을 생성하여 Local Authentication Request 메시지에 실어 참여자 기기에게 전송한다.

② 만약 참여자 기기에게서 Local Authentication Response 메시지를 수신하면 메시지 안의 QED', QED를 저장한 후 $MacTag1'$을 계산하여 Local Authentication Response 메시지의 $MacTag1'$과 일치하는지 확인한다. 일치하지 않을 경우 Leave Command 메시지를 참여자 기기에게 전송하고 프로토콜을 중단한다.

③ 두 $MacTag1'$가 일치하는 경우 $MacTag2'$을 계산한 후 Local Authentication Confirm 메시지에 실어 참여자 기기에게 전송한다.

④ Update-Device 메시지를 트러스트 센터에게 전송한다. 이 때 QED를 같이 전송한다.

마. 참여자 기기의 동작 절차

① Association 완료 후 Local Authentication

Request 메시지를 수신하면 Local Authentication Request 메시지 안의 QER'을 저장한 후 QED'과 QED를 생성하고 $MacTag1'$을 계산한다. QED, QED', $MacTag1'$을 Local Authentication Response 메시지에 실어 부모 노드에게 전송한다.

② 부모 노드에게서 Local Authentication Confirm 메시지를 수신하면 $MacTag2'$을 계산하여 Local Authentication Confirm 메시지 안의 $MacTag2'$과 일치하는지 확인한다. 일치하지 않을 경우 Leave Command 메시지를 부모 노드에게 전송하고 프로토콜을 중단한다.

③ 두 $MacTag2'$이 일치할 경우 트러스트 센터에게서 Authentication Response 메시지를 수신하면 메시지 안의 QET를 저장하고 $MacTag2$, 링크키를 계산한다. 그리고 계산한 $MacTag2$가 Authentication Response 메시지 안에 있는 $MacTag2$와 일치하는지 확인한다. 일치하지 않을 경우 Leave Command 메시지를 부모 노드에게 전송하고 프로토콜을 중단한다.

④ 두 $MacTag2$가 일치한다면 $MacTag1$을 계산하여 Authentication Confirm 메시지로 전송한다.

⑤ Transport-Key 메시지를 수신하면 메시지 안의 네트워크 키를 저장한다.

Ⅳ. 성능 평가

1. Security 분석

본 절에서는 다양한 공격 유형들을 고려하여 제안한 인증 프로토콜이 각각의 공격들을 방어할 수 있는지에 대해 서술하고 프로토콜의 안전성을 평가한다[5].

가. 도청 (Eavesdropping)

도청은 공격자가 네트워크에서 송수신되는 메시지들을 가로채어 키나 중요한 메시지를 알아내는 공격 기법이다. 제안하는 프로토콜에서는 마스터키, LAK 키가 직접 노출되지 않고 해쉬값만 전송한다. 따라서 공격자가 도청을 통해 마스터키나 LAK를 알아낼 수 없기 때문에 제안하는 프로토콜은 도청에 대해 안전하다.

나. 재사용 공격 (Replay attack)

재사용 공격은 공격자가 네트워크에서 송수신되는 메시지를 가로채어 수집해 두었다가 공격자가 이를 그대로 재송신하여 프로토콜 교란 등을 발생시키는 공격 유형이다. 제안하는 프로토콜에서는 한 번의 인증을 수행할 때 두 기기가 임시로 생성한 임의의 수를 사용하여 해쉬값을 생성한다. 따라서 공격자가 이전에 사용한 값을 사용하여도 공격 대상이 문자열을 새로 생성하므로 해쉬값이 달라져 공격 대상이 메시지가 변경되었다는 것을 알 수 있기 때문에 공격자가 이전에 얻은 해쉬값을 사용할 수 없다. 따라서 제안하는 프로토콜은 재사용 공격에 대해 안전하다.

다. 메시지 변조 (Message modification)

메시지 변조 공격은 공격자가 임의로 메시지의 일부분을 수정하여 프로토콜 교란 등을 발생시키는 공격 유형이다. 제안하는 프로토콜은 해쉬값 $MacTag$를 전송하므로 공격 대상이 $MacTag$를 통하여 메시지가 변조되었는지 확인할 수 있다. 따라서 제안하는 프로토콜은 메시지 변조에 대해 안전하다.

2. 인증 반복 공격에 대한 대응

이 절에서는 인증 프로토콜을 이용한 DoS 공격이 발생하였을 때 공격이 네트워크에 미치는 영향에 대해 알아본다. 인증 프로토콜을 이용한 DoS 공격이 발생하였을 경우에 각 기기는 인증 프로토콜에 필요한 정보 교환을 위해 메시지를 전송하게 되지만 이 때 전송하는 메시지는 네트워크에 불필요한 메시지 전송이다. 따라서 이 메시지 수가 많을수록 프로토콜이 DoS 공격에 취약하다는 것을 의미한다.

ZigBee의 인증 프로토콜 및 제안한 인증 프로토콜이 공격자를 인증하기 위해 필요한 메시지 수를 분석하기 위하여 트러스트 센터와 공격자 사이의 홉 수에 따라 정보 교환 과정에서 발생하는 메시지 교환 횟수 N_D를 계산한다. ZigBee의 인증 프로토콜 및 제안하는 프로토콜에서 공격자를 인증할 경우에 발생하는 정보 교환 과정은 각각 그림 2 및 그림 5와 같다. N_D는 정보 교환 과정에서 메시지 전달의 위치(그림에서 화살표) 및 전달 횟수를 이용하여 구할 수 있다. h를 트러스트 센터와 참여자 기기 사이의 홉 수, $N_{D,TR}$을 트러스트 센터와 부모 라우터 사이의 메시지 전달 횟수, $N_{D,RD}$를 부모 라우터와 참여자 기기 사이의 메시지 전달 횟수라고 하면 N_D는 식 (1)과 같이 나타난다.

$$N_D = (h-1) \times N_{D,TR} + N_{D,RD} \quad (1)$$

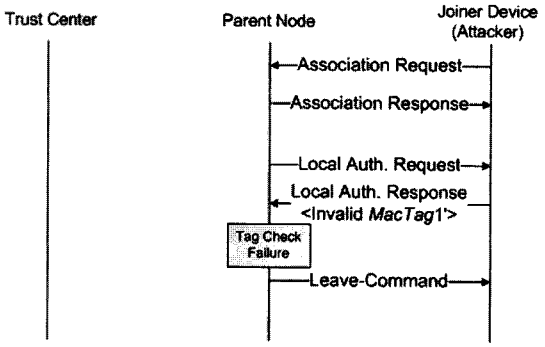

그림 5. 공격자 기기가 인증을 시도할 경우의 제안한 인증과정의 메시지 교환

Fig. 5. The information exchanges when an attacker tries to join the network.

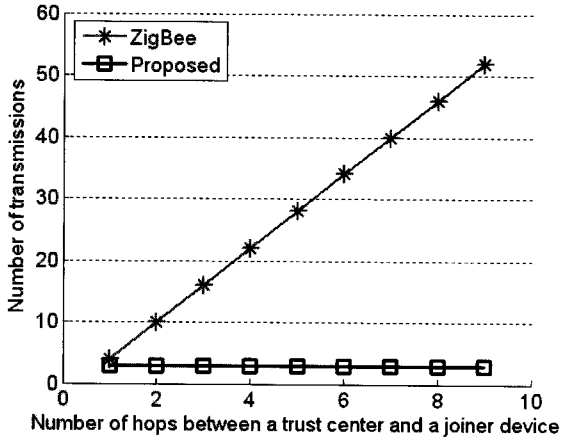

그림 6. 참여자 기기가 잘못된 마스터키를 사용할 때 트러스트 센터와 라우터들이 전송하는 메시지 수

Fig. 6. Estimated number of transmissions by a trust center and routers when an attacker tries to join the network.

위 식을 이용하여 ZigBee의 인증 프로토콜 및 제안하는 인증 프로토콜을 사용 시에 각 기기들이 전송하는 메시지의 수를 합하여 홉 수별로 나타내면 그림 6과 같다. 그림 6에서 제안하는 프로토콜은 홉 수가 증가하여도 전송하는 메시지 수는 증가하지 않음을 확인할 수 있다. 그림 5와 그림 6에서 볼 수 있듯이 제안하는 인증 프로토콜이 인증 반복을 이용한 공격에 효과적으로 대처하기 때문에 DoS 공격 시 배터리가 소모되는 기기를 부모 노드로만 제한하고, 필요 없는 메시지 전송을 줄여 트러스트 센터 및 전송 경로에 위치한 라우터들의 전력 소모, 네트워크 효율 감소를 유발하지 않음을 알 수 있다.

3. GNY 분석

본 절에서는 암호화 프로토콜의 수행을 이해하기 위한 체계적인 방법인 GNY 논리[6]를 이용하여 프로토콜의 신뢰성을 살펴본다. GNY 논리에서 사용하는 기호 및 규칙에 대한 설명은 [6]을 참고하기 바란다.

가. 가정

각 기기는 자신의 기기 주소(ID_x), 자신이 생성한 임의의 수(QEx 또는 QEx'), 키(마스터키 $MK_{T,D}$ 및 LAK LAK)를 갖고 있다. 임의의 수는 각 기기가 해당 세션에 스스로 생성하므로 각 기기는 임의의 수가 재사용되지 않았음을 알고 있다. 또한 각 기기는 상대방 기기가 인증을 수행할 수 있다는 것을 믿고 자신이 사용하는 키가 상대방과 공유되어 있다고 믿어야 한다. 아래는 이러한 가정들을 GNY 논리로 표현한 것이다.

$$T \ni ID_T, T \ni ID_R, T \ni MK_{T,D}, T \ni QET,$$
$$T \mid \equiv \#(QET),$$
$$T \mid \equiv D \mid \Rightarrow D \mid \equiv *,\ T \mid \equiv T \xleftrightarrow{MK_{T,D}} D,$$
$$R \ni ID_T, R \ni ID_R, R \ni ID_D, R \ni LAK, R \ni QER',$$
$$R \mid \equiv \#(QER'),$$
$$R \mid \equiv D \mid \Rightarrow D \mid \equiv *,\ R \mid \equiv R \xleftrightarrow{LAK} D,$$
$$D \ni ID_D, D \ni ID_R, D \ni LAK, D \ni MK_{T,D},$$
$$D \ni QED, D \ni QED',$$
$$D \mid \equiv \#(QED), D \mid \equiv \#(QED'),$$
$$D \mid \equiv T \mid \Rightarrow T \mid \equiv *,\ T \mid \equiv T \xleftrightarrow{MK_{T,D}} D,$$
$$D \mid \equiv R \mid \Rightarrow R \mid \equiv *,\ R \mid \equiv R \xleftrightarrow{LAK} D.$$

나. 분석 목적

이 프로토콜의 목적은 각 기기가 마스터키, LAK를 서로 공유하고 상대방이 그 키를 갖고 있다는 것을 믿는 것이며 마스터키와 LAK가 두 기기 사이에 공유되었다는 상대방의 믿음을 아는 것이다. 아래는 이러한 분석 목적을 GNY 논리로 표현한 것이다.

$$T \mid \equiv T \xleftrightarrow{MK_{T,D}} D,\ T \mid \equiv D \ni MK_{T,D},$$
$$T \mid \equiv D \mid \equiv T \xleftrightarrow{MK_{T,D}} D,$$
$$R \mid \equiv R \xleftrightarrow{LAK} D,\ R \mid \equiv D \ni LAK,$$

$R|\equiv D|\equiv R\overset{LAK}{\longleftrightarrow}D,$

$D|\equiv T\overset{MK_{T,D}}{\longleftrightarrow}D, D|\equiv D\ni MK_{T,D},$

$D|\equiv T|\equiv T\overset{MK_{T,D}}{\longleftrightarrow}D,$

$D|\equiv R\overset{LAK}{\longleftrightarrow}D, D|\equiv R\ni LAK,$

$D|\equiv R|\equiv R\overset{LAK}{\longleftrightarrow}D.$

다. 이상화된 프로토콜

GNY 논리를 이용하여 검증을 하기 위해서는 프로토콜을 이상화된 프로토콜로 표현하여야 한다. 제안하는 프로토콜을 이상화된 프로토콜로 표현하면 아래와 같다.

1) $D\lhd(*ID_R, *QER').$

2) $R\lhd(*H(LAK, ID_D, ID_R, QED', QER'), *ID_D, *QED, *QED').$

3) $D\lhd(ID_R, *H(LAK, ID_R, ID_D, QER', QED')).$

4) $T\lhd(*ID_D, *QED).$

5) $D\lhd(*ID_T, *QET, *H(MK_{T,D}, ID_T, ID_D, QET, QED)).$

6) $T\lhd(ID_D, *H(MK_{T,D}, ID_T, ID_D, QED, QET)).$

라. 해쉬값의 의미 확장성

이 프로토콜에서 해쉬값은 해쉬값에 사용된 키가 송신자와 수신자 사이에 공유된 비밀이라고 믿는 것을 의미하게 된다. 따라서 해쉬값은 다음과 같이 의미가 확장될 수 있다.

$$H(Key, ID_A, ID_B, QEA, QEB)\sim>A|\equiv A\overset{Key}{\longleftrightarrow}B.$$

마. 논리적 분석

논리적 분석은 이상화된 프로토콜을 GNY 논리로 해석하는 과정이며 분석을 통해 분석 목적을 확인하면 프로토콜이 신뢰성이 있음을 증명할 수 있다. 본 증명에서는 부모 노드가 참여자 기기가 LAK를 갖고 있음을 신뢰하고 LAK가 두 기기 사이의 공유된 비밀임을 신뢰하는 과정에 대해서만 보이겠다. 참여자 기기가 트러스트 센터를 믿는 것과 트러스트 센터 및 부모 노드가 참여자 기기를 믿는 것에 대한 확인은 위 과정과 같은 방법을 적용하면 알 수 있다. 4가지 경우에 대하여 아래와 같이 적용하면 분석 목적을 모두 얻을 수 있다.

이상화된 프로토콜 과정 2)에서 T1, T2, P1, P3, P4 규칙을 적용하면 식 (2)을 얻는다.

$$\begin{aligned}&R\ni ID_D, R\ni QED',\\&R\ni H(LAK, ID_R, ID_D, QER', QED'),\\&R\ni(LAK, ID_R, ID_D, QER', QED').\end{aligned}\quad(2)$$

식 (2)는 부모 노드가 참여자 기기의 기기 주소, 서로 생성한 임의의 문자열, 해쉬값을 갖고 있음을 의미한다. 식 (2)에 R5, R6 규칙을 적용하면 식 (3)을 얻을 수 있다.

$$\begin{aligned}&R|\equiv\phi(LAK, ID_R, ID_D, QER', QED'),\\&R|\equiv\phi(H(LAK, ID_R, ID_D, QER', QED')).\end{aligned}\quad(3)$$

식 (3)은 부모 노드가 메시지를 인식할 수 있음을 의미한다. 식 (3)에 F1, F10 규칙을 적용하면 가정 $R|\equiv\#(QER')$에 의해 식 (4)를 얻을 수 있다.

$$\begin{aligned}&R|\equiv\#(LAK, ID_R, ID_D, QER', QED'),\\&R|\equiv\#(H(LAK, ID_R, ID_D, QER', QED')).\end{aligned}\quad(4)$$

식 (4)는 각각의 데이터가 재사용되지 않았음을 의미한다. 식 (4)에 I3와 I6 규칙을 적용하면 식 (5)를 얻는다.

$$\begin{aligned}&R|\equiv D|\sim(LAK, ID_R, ID_D, QER', QED'),\\&R|\equiv D|\sim H(LAK, ID_R, ID_D, QER', QED'),\\&R|\equiv D\ni(LAK, ID_R, ID_D, QER', QED').\end{aligned}\quad(5)$$

식 (5)는 부모 노드가 각 데이터들이 참여자 기기에 전송되었다는 것을 확인하여 참여자 기기를 인증하고 참여자 기기가 각 데이터를 갖고 있다는 사실을 확인하였다는 의미이다.

마지막으로 식 (5)에 P3, J2 규칙과 합리성 규칙 (rationality rule)을 적용하면 식 (6)을 얻는다.

$$R|\equiv D\ni LAK,\ R|\equiv D|\equiv R\overset{LAK}{\longleftrightarrow}D.\quad(6)$$

식 (6)은 참여자 기기가 LAK를 갖고 있음 및 참여자 기기가 LAK를 두 기기 사이에 공유된 비밀이라고 믿고 있음을 부모 노드가 확신한다는 의미이다.

앞서 서술하였듯이, 위 과정을 나머지 경우에 대하여 모두 적용하여 보면 분석 목적을 모두 얻을 수 있다. 이는 각 기기가 모든 상대방 기기를 믿을 수 있게 됨을

의미하므로 제안하는 인증 프로토콜을 이용할 경우 각 기기 사이의 신뢰성이 보장된다고 할 수 있다.

4. 인증 처리 시간

제안하는 인증 프로토콜 기기 사이의 인증을 수행할 수 있다는 것과 인증을 완료하는데 소요되는 시간을 줄일 수 있다는 것을 확인하기 위하여 ZigBee 기기에 ZigBee 표준의 인증 프로토콜 및 제안한 인증 프로토콜을 구현하였다. 사용한 기기는 그림 7과 같은 Aiji-ZDB Ver. 2.0이며 구현 환경은 표 1과 같다.

실험을 통하여 그림 8과 같이 인증과정 중 기기들이 주고받은 메시지를 얻을 수 있었으며, 이를 통하여 인증이 성공적으로 이루어짐을 확인하고 1홉 및 2홉에서 실제로 인증에 소요되는 시간을 측정할 수 있었다. 인증에 소요된 시간은 ZigBee의 인증 프로토콜의 경우 1홉에서 약 100ms, 2홉에서 약 280ms였으며 제안한 프로토콜은 1홉에서 약 90ms, 2홉에서 약 215ms였다.

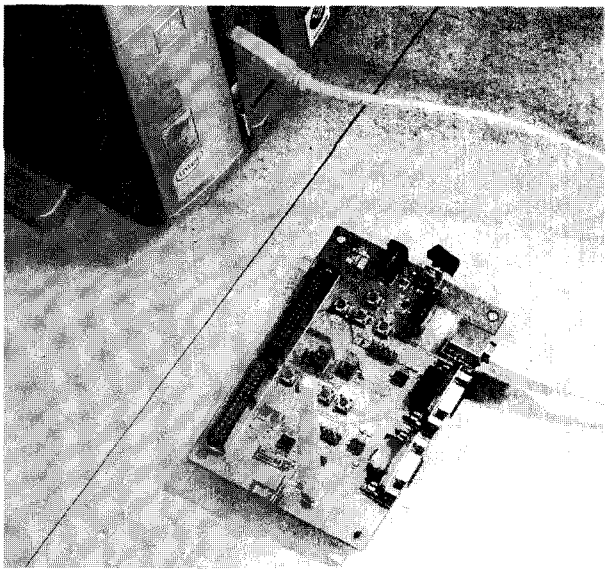

그림 7. 프로토콜 구현에 사용한 기기(Aiji-ZDB Ver 2.0)
Fig. 7. The device that was used in the experiments. (Aiji-ZDB Ver. 2.0)

표 1. 프로토콜 구현 환경
Table 1. The environment of protocol implementation

기기명	Aiji ZDB Version 2.0
Chipset	Chipcon CC2430 (supports 802.15.4)
ZigBee 버전	Release 16[7]
패킷 캡쳐 프로그램	Chipcon General Packet Sniffer for IEEE 802.15.4 MAC
장소	실내 20m 이내
측정 항목	1, 2홉에 대한 인증 완료 시간

3홉 이상의 경우는 라우팅 과정이 추가된다는 것 이외에는 메시지 교환 및 처리 과정이 2홉과 동일하기 때문에 측정을 하지 않았다. 대신에 각 프로토콜 당 약 10회의 측정을 통해 인증 시간 분석에 필요한 값을 얻었으며, 계산을 통해 더 많은 홉 수에서 인증을 완료 하는데 필요한 시간을 분석하였다.

각 홉 수별로 인증을 완료하는데 걸리는 시간을 구하기 위하여 다음 값들을 설정하고 분석을 위한 계산을 수행하였다. 우선 메시지를 전송한 후 acknowledgment 메세지를 받을 때까지 걸리는 시간 t_{ack}는 bit rate가 250$kbps$이기 때문에 메시지의 비트당 약 1/250ms로 측정되었다. 또한 라우팅을 위하여 한 기기에서 하나의 메시지를 다음 기기로 전달하는데 걸리는 시간인 routing delay t_{rout}는 약 10ms로 측정되었다. 따라서 t_{ack}및 t_{rout}를 다음과 같이 설정하였다.

$$t_{ack} = \frac{8bits}{250kbps} = 0.032ms/byte,\ t_{rout} = 10ms.$$

또한 각 기기가 자신이 목적지인 메시지를 APS 계층에서 처리하여 다음 메시지를 전송할 때까지 걸리는 시간은 메시지 별로 달랐지만 인증 시에 그 전체 합은

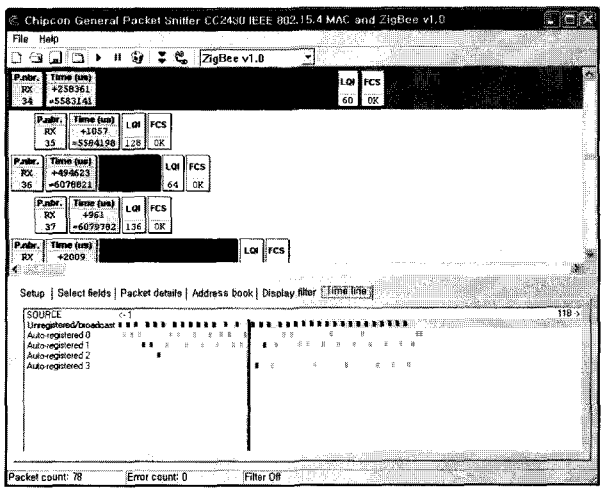

그림 8. 실험 과정에서 얻은 메세지
Fig. 8. The captured messages during experiments.

표 2. 각 프로토콜의 처리 지연
Table 2. The processing delay of each protocols.

Protocol	Single hop	Multiple hops
ZigBee	95.115 *ms*	196.248 *ms*
Proposed	85.414 *ms*	159.203 *ms*

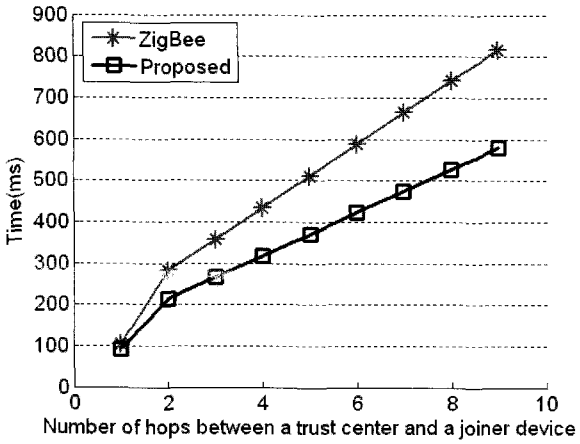

그림 9. 각 프로토콜의 인증 완료 시간
Fig. 9. Estimated authentication delay.

거의 일정하였다. 따라서 처리 지연 t_{proc}는 실험에서 얻은 메시지에서 각 메시지들을 처리하는 시간들을 더하여 표 2와 같이 설정하였다.

트러스트 센터와 참여자 기기 사이의 홉 수를 h, 부모 노드와 참여자 기기 사이에 전송된 메시지 길이의 총합을 L_{RD}(bytes), 트러스트 센터와 부모 노드 사이에서 교환된 메시지 길이의 총합을 L_{TR}(bytes), 각 메시지가 라우팅 된 횟수의 총합을 N_R이라고 하면 인증 완료시간 t_{auth}는 식 (7)을 통하여 구할 수 있다.

$$t_{auth} = t_{rout} \times N_R + t_{ack} \times \{(h-1) \times L_{TR} + L_{RD}\} + t_{proc}. \quad (7)$$

식 (7)을 이용하여 인증 완료 시간을 홉 수 별로 구하면 그림 9와 같다. 그림 9에서 알 수 있듯이 제안하는 인증 프로토콜은 기존 인증 프로토콜보다 더 빠르게 인증을 마칠 수 있다. 또한 홉 수가 늘어남에 따라 인증 완료 시간이 최대 30% 감소함을 확인할 수 있었다. 이는 제안하는 인증 프로토콜이 기존 인증 프로토콜보다 개별 메시지의 길이는 늘어났지만 교환되는 메시지 수가 줄어들어 인증과정에서의 전체적인 오버헤드가 감소했기 때문이다.

V. 결 론

본 논문에서는 기존의 LR-WPAN을 위한 인증 프로토콜에서 발생 가능한 문제점들을 해결하기 위하여 LR-WPAN에서 효과적으로 인증을 수행하는 새로운 인증 프로토콜을 제안하고 여러 가지 성능 분석을 수행하여 제안한 프로토콜의 안전성, 신뢰성 및 효율성을 확인하였다. 제안하는 인증 프로토콜은 부모 노드와 참여자 기기가 먼저 인증을 수행하여 기존 인증 프로토콜에서 인증과정을 이용하는 DoS 공격 발생 시 트러스트 센터까지 필요 없는 트래픽을 전달하지 않기 때문에 DoS 공격에 대응한다. 또한 제안하는 프로토콜은 메시지 교환 횟수를 줄여 인증 완료 시간을 홉 수에 따라 최대 30%를 줄였기 때문에 인증 효율이 높아진다.

LR-WPAN에서 사용되는 프로토콜은 기기의 연산 능력과 저장 공간이 충분하지 않다는 점과 배터리 사용 효율이 좋아야 한다는 점을 고려해야 한다. 제안하는 프로토콜은 하나의 키를 추가하여 계층 구조를 이용한 인증 프로토콜에서 발생할 수 있는 DoS 공격을 막을 수 있으며 안전성을 확보하면서도 메시지 교환과정을 줄여 배터리 사용 효율이 기존 프로토콜보다 좋아진다. 따라서 제안한 프로토콜을 LR-WPAN에 적용한다면 네트워크가 더욱 안전하고 효율적이게 될 것이다.

참 고 문 헌

[1] IEEE computer Society, "IEEE Std. 802.15.4-2003: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specification for Low Rate Wireless Personal Area Networks," October 2003.
[2] ZigBee Alliance, "ZigBee Specification: ZigBee Document 053474r17," October 19, 2007.
[3] 서대열, 김진철, 김경목, 오영환, "ZigBee 센서네트워크에서 효율적인 Parent - Child 키 연결 알고리즘," 전자공학회논문지, 제 43권 TC편, 제 10호, 45-55쪽, 2006년 10월
[4] S. A. Camtepe, B. Yener, "Key Distribution Mechanisms for Wireless Sensor Networks: a Survey", Technical Report, Rensselaer Polytechnic Institute, March 2005.
[5] 이규환, 이주아, 김재현,"무선 메쉬 네트워크의 패스워드 기반 인증 프로토콜,"전자공학회논문지, 제 44권 TC편, 제 5호, 54-62쪽, 2007년 5월
[6] L. Gong, R. Needham, and R. Yahalom, "Reasoning about Belief in Cryptographic Protocols," in Proc. IEEE Symposium on Research in Security and Privacy, pp. 234-248, Oakland, CA, May 1990.
[7] ZigBee Alliance, "ZigBee Specification: ZigBee Document 053474r16," May 31, 2007.

저 자 소 개

이 성 형(학생회원)
2007년 아주대학교 전자공학부 학사 졸업.
2009년 아주대학교 대학원 전자공학과 석사 졸업.
2009년~현재 아주대학교 대학원 전자공학과 박사과정
<주관심분야 : WPAN 보안, 네트워크 설계 및 관리, 협력통신, MAC 프로토콜>

김 재 현(평생회원)-교신저자
1987년~1996년 한양대학교 전산과 학사 및 공학석사/공학박사 졸업
1997년~1998년 미국 UCLA 전기전자과 박사 후 연수
1998년~2003년 Bell Labs, Performance Modeling and QoS Management Group, 연구원
2003년~현재 아주대학교 전자공학부 부교수
<주관심분야 : 무선인터넷 QoS, MAC 프로토콜, IEEE 802.11/15/16/20, 3GPP, 국방 전술네트워크 등>