# IEEE 802.15.4에서 확인 프레임을 위한 경량 인증 메커니즘

## (A Lightweight Authentication Mechanism for Acknowledgment Frame in IEEE 802.15.4)

허 준 † 홍 충 선 ††
(Joon Heo) (Choong Seon Hong)

**요 약** IEEE 802.15.4 표준에서 데이타 또는 명령프레임의 성공적인 수신과 검증은 확인(Acknowledgment) 프레임을 통해 수행되어 진다. 하지만, 현재의 표준에서는 확인 프레임을 위한 어떠한 보안 기능도 제공하고 있지 않으며, 악의적인 노드는 언제든지 확인 프레임을 이용한 공격이 가능하다. 본 논문에서는 IEEE 802.15.4 네트워크 환경에서 확인 프레임을 위한 링크 레이어(link-layer) 상의 개체 인증 메커니즘을 제안한다. 제안된 메커니즘은 인증을 위해 3비트의 값을 사용하므로 디바이스의 오버헤드를 크게 감소시킬 수 있다. 개체 인증에 사용되는 암호화된 비트 스트림은 연결설정(association) 과정을 통해 코디네이터로부터 디바이스에게 전달되어진다. 확률적인 이론과 시뮬레이션 결과를 통해 제안된 메커니즘이 MAC 레이어의 공격을 효과적으로 탐지할 수 있음을 증명한다.

**키워드** : IEEE 802.15.4, 확인 프레임, 경량 인증, 침입 탐지

***Abstract*** In IEEE 802.15.4 (Low-Rate Wireless Personal Area Network) specification, a successful reception and validation of a data or MAC command frame can be confirmed with an acknowledgment. However, the specification does not support security for acknowledgment frame; the lack of a MAC covering acknowledgments allows an adversary to forge an acknowledgment for any frame. This paper proposes an identity authentication mechanism at the link layer for acknowledgment frame in IEEE 802.15.4 network. With the proposed mechanism there is only three bits for authentication, which can greatly reduce overhead of device. The encrypted bit stream for identity authentication will be transmitted to device by coordinator within association process. Statistical method and simulation results prove that our mechanism is successful in handling MAC layer attack.

**Key words** : IEEE 802.15.4, acknowledgment frame, lightweight authentication, attack detection

## 1. 서 론

IEEE 802.15.4(LR-WPAN) 표준[1]은 퍼스널 개념의 네트워킹 디바이스를 위한 무선 및 미디어 엑세스 프로토콜을 정의하고 있다. 이 표준은 PHY 레이어와 MAC 서브 레이어를 정의하고 있으며 low-cost, low-power 소비 등을 주된 목표로 하고 있다. 이러한 목적을 달성하기 위해 전송방법 및 디바이스의 동작주기 등에서 기존의 무선 기술과 차별성을 가지고 있다. 무선 액세스 네트워크를 기반으로 하는 이 표준 기술은 간단하면서도 장시간 지속될 수 있는 특징을 가져야한다. 이 같은 기술은 유비쿼터스 센서 네트워크 및 제어 시스템에 널리 사용될 수 있을 것으로 기대되고 있다. 하지만, 이 표준이 폭넓게 활용되기 위해서는 확실한 보안 기술이 뒷받침 되어야 한다[1,2]. 전체적으로 IEEE 802.15.4 표준은 높은 보안 기능을 정의하고 있다. 128비트 AES 기반의 암호화/복호화 기능을 정의하고 있으며, 인증 코드의 길이를 통해 보안 레벨도 구분하여 기술하고 있다. 하지만, 이처럼 높은 수준의 보안 기능에도 불구하고 취약한 부분도 포함하고 있으며, 본 논문에서는 이러한 취약성 중에서도 심각한 위협요소로 작용할 수 있는 확인 프레임을 통한 공격을 탐지하는 메커니즘을 제안한다. IEEE 802.15.4 표준은 네 가지 프레임 형식을 정의하고

· This work was supported by MIC and ITRC Project.
† 학생회원 : 경희대학교 컴퓨터공학과
heojoon@khu.ac.kr
†† 종신회원 : 경희대학교 컴퓨터공학과 교수
cshong@khu.ac.kr
논문접수 : 2006년 4월 27일
심사완료 : 2007년 3월 16일

있으며, 그것은 비콘 프레임(beacon frames), 데이타 프레임(data frames), 확인 프레임(acknowledgment frames), 제어 프레임(control frames)이다. 표준에서는 확인 프레임을 제외한 세 가지 프레임의 무결성 보장과 데이타 필드의 견고성을 위해 선택적으로 보안 기능을 사용할 수 있도록 정의하고 있으나 확인 프레임의 경우 어떠한 보안 기능도 포함하고 있지 않다[1,3]. 이는 앞서 언급한 것처럼 간단한 표준 기술을 만들기 위해 간편화된 것일 수 있으나 확인 프레임의 경우 매우 빈번하게 사용되며, 제대로 전달되지 않거나 잘못된 형태로 전달될 경우 네트워크상의 노드들에 부하를 증가시킬 뿐 아니라, 심각한 위협요소가 될 수 있다. 본 논문에서는 IEEE 802.15.4 표준에서 확인 프레임을 위한 링크 레이어상의 경량화된 개체 인증 메커니즘을 제안한다.

제안하는 메커니즘은 현재 IEEE 802.15.4와 ZigBee에서의 보안 기술 및 프레임 형식은 그대로 유지하므로 데이타 암호화/복호화 및 무결성 검증, 보안 키 생성과 같은 보안 기술은 표준에서 제시하는 방법을 그대로 적용하면서 확인 프레임 자체만으로 인증 정보 교환이 가능하도록 설계하는 것에 목표를 두었다. 제안하는 방법은 보안의 관점에서 IEEE 802.15.4의 취약성으로 제기되고 있는 확인 프레임(Acknowledgment)을 인증할 수 있는 방법을 제시함에 있어서 프레임에서 사용가능한 필드로 남아 있는 3비트의 공간을 어떻게 활용하여 보안 기능을 추가할 것인지에 초점을 두고 있다. 이러한 3비트 공간의 사용은 보안 강도 측면에서 극명한 한계를 가질 수밖에 없으나 이미 표준에서 정의하고 있는 보안 기술과 함께 적용되므로 효과적으로 확인 프레임 인증에 사용할 수 있다. 본 논문에서 제안하는 메커니즘은 확인 프레임을 수신한 노드가 송신 노드로부터 전달된 프레임 안의 인증 비트 값을 검증함으로써 적합성을 판단하게 된다. 제안된 메커니즘은 3비트의 인증 값을 사용하므로 노드에서 발생할 수 있는 오버헤드를 감소시킬 수 있으며 인증코드 생성을 위한 암호학적 연산도 수행하지 않는다. 또한, 표준에서 정의하는 프레임 형식 중 사용 가능한(reserved bits) 부분을 이용함으로써 표준을 수정하지 않고 메커니즘이 적용 가능하도록 하였다. 본 논문에서 제안하고 있는 메커니즘의 주요 목적 중 하나는 에러 발생으로 인해 확인 프레임이 손실 될 수 있는 환경에서 공격자를 탐지하는 것이며, 이를 위해 확률적 이론에 근거한 방법을 제시하였다. 앞서 언급한 것처럼 단지 3비트만을 사용할 수 있다는 것은 보안 강도 측면에서 한계를 가질 수밖에 없으나 향후 더 많은 비트를 사용할 수 있는 경우 보안의 정도는 현저하게 증가할 수 있을 것이다. 본 논문은 현재 사용 가능한 필드를 효과적으로 활용함으로써 확인 프레임 인증에 활용하고 무선 환경에서의 공격과 프레임 손실을 확률적인 분석으로 예측하는 방법의 제안에 목적을 두었다.

본 논문은 다음과 같이 구성되었다. 2장에서는 LR-WPAN과 ZigBee 표준에서의 보안 기술에 대하여 설명한다. 또한 IEEE 802.15.4 구성 디바이스와 네트워크 형태, 표준에서 확인 프레임의 사용 및 취약성 그리고 코디네이터와 디바이스 사이의 연결설정 과정에 대하여 간단하게 설명한다. 3장에서는 확인 프레임을 위한 경량화된 개체 인증 메커니즘에 관하여 설명한다. 4장에서는 확률적 이론에 근거한 공격 탐지 방법과 성능평가 결과 그리고 제안된 메커니즘이 IEEE 802.15.4 표준에 적용되기 위한 방법에 관하여 기술한다. 마지막으로 결론 및 향후 과제에 관하여 언급한다.

## 2. 관련 연구

### 2.1 IEEE 802.15.4 보안 기술

Low_Rate Wireless Personal Area Networks (LR-WPANs) 은 전송 프레임의 보안을 제공하기 위해 아래와 같은 서비스를 정의하고 있다[1].

- Access Control(접근제어)
- Data Encryption(데이타 암호화)
- Frame Integrity(프레임 무결성)
- Sequential Freshness(중복전송 방지)

데이타 암호화, 프레임 무결성 및 중복전송 방지를 위해 AES-CCM 알고리즘을 사용한다. 데이타 암호화는 128비트의 AES알고리즘을 적용하여 보안의 강도를 높이고 있으며, 프레임 무결성은 메시지 인증코드의 길이를 32비트, 64비트, 128비트로 다양화하여 보안 레벨을 세분화 하였다. 또한 중복전송 방지는 카운터(CTR)의 적용여부에 따라 선택적으로 사용할 수 있도록 하였다. 이러한 보안 기술은 어플리케이션에 따른 보안 강도의 차등 적용이 가능하며, 암호와 및 복호화 기능이 하드웨어적으로 구현되므로 연산속도와 오버헤드를 감소시킬 수 있다. 표 1은 LR-WPANs의 보안 레벨과 기능을 요약하여 설명하고 있다.

또한, 표준에서는 어플리케이션이 어느 정도의 보안을 요구하느냐에 따라 Unsecured 모드, Access Control

표 1 LR-WPANs의 보안 기술

| Suite | B | A | E | I | S |
|---|---|---|---|---|---|
| AES-CTR | 0 | Y | Y | N | Optional |
| AES-CCM-128 | 128 | Y | Y | Y | Optional |
| AES-CCM-64 | 64 | Y | Y | Y | Optional |
| AES-CCM-32 | 32 | Y | Y | Y | Optional |
| AES-CBC-MAC-128 | 128 | Y | Y | Y | N |
| AES-CBC-MAC-64 | 64 | Y | Y | Y | N |
| AES-CBC-MAC-32 | 32 | Y | Y | Y | N |

(B: Bits of integrity, A: Access Protection, E: Encryption, I: Integrity, S: Sequential Freshness)

List 모드, Secured 모드로 구분하여 적용할 수 있도록 하고 있다. 그러나, 표 1에서 언급하고 있는 보안 기술이 적용되기 위해서 반드시 필요한 보안 키(key) 생성 및 관리는 상위레이어(ZigBee)에서 생성되는 키를 사용하게 된다.

### 2.2 ZigBee 보안 기술

앞 절에서 LR-WPANs 보안 기술에 관해 설명하였다. ZigBee 표준에서의 보안 서비스는 하위 레이어와 직접적으로 연관되어 있다[4]. ZigBee 보안 기술의 특징은 각 레이어(MAC, NWK, APL)에서 생성되는 프레임은 각 레이어에서 데이타 암호화 및 무결성 검증을 위한 연산을 수행하도록 되어 있다는 것이다. 이러한 기능을 담당하는 SSP(Security Service Provider)가 모듈 형태로 존재하게 된다(그림 1 참조). 또한, 암호화와 인증코드 생성이 함께 되는 CCM 알고리즘 대신 이 두 가지를 구분하여 선택할 수 있도록 CCM* 알고리즘을 제안하여 SSP에 구현되도록 정의하였다.

특히, APL 레이어에서는 아래와 같은 보안 서비스가 제공되어야 한다.

- Key establishment
- Transport key
- Update device
- Remove device
- Request key
- Switch key

상위 레이어에서의 대부분의 서비스가 키 설정(key establishment)및 관리에 초점을 맞추고 있으나, 아직까지 현실적이고 효율적으로 키를 생성하고 관리하는 방법에는 한계를 가지고 있다. 상위 레이어(ZigBee)에서 생성되는 다양한 키는 MAC레이어(LR-WPAN)의 보안 서비스를 위해서도 사용된다[4].

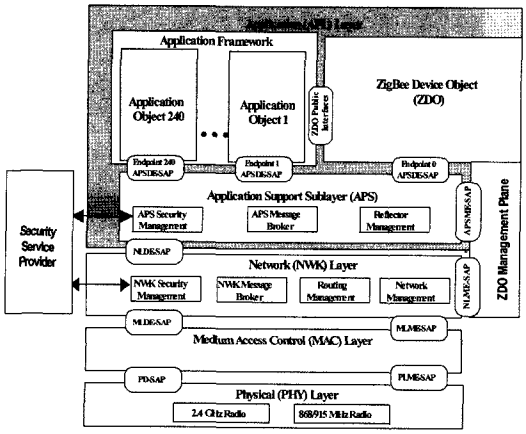



그림 1 ZigBee 표준과 보안 기술

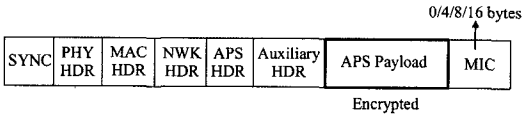



그림 2 APS레이어 데이타의 암호화와 인증

ZigBee에서의 암호화와 인증은 APS레이어와 NWK 레이어에서 각각 처리된다. 그림 2는 APS레이어에서 AES-CCM*알고리즘을 통해 암호화와 인증코드를 생성했을 경우의 프레임 형식을 나타내고 있다.

APS 페이로드 부분은 암호화되어 전송되며, 인증코드는 보안 레벨에 따라 0/32/64/128비트 중 하나를 선택하여 프레임 마지막에 추가하게 된다. 이러한 정보는 부가헤더(Auxiliary)에 포함되어 전송되며 부가헤더는 수신노드의 복호화와 인증코드 확인을 위한 정보를 제공한다. 이 정보 중 핵심이 되는 부분은 보안레벨과 키 식별자의 구분이다. 부가헤더는 3비트를 사용해 8가지 보안레벨 중에 한 가지를 사용했음을 나타내며 2비트의 키 식별자를 통해 4가지의 키(link key, network key, key-transport key, key-load key)중 어떤 키를 사용해 암호화와 인증코드를 생성했는지 나타내게 된다. 또한 ZigBee에서는 CCM* 알고리즘을 정의하여 사용하고 있으며, 이 알고리즘은 암호와와 인증을 선택적으로 사용할 수 있는 장점을 가지고 있다. 네트워크 레이어(NWK)도 이와 동일한 방법으로 암호화와 인증코드 생성하게 되며, 각 레이어에서 생성되는 프레임은 해당 레이어에서 처리된다.

### 2.3 IEEE 802.15.4 구성 디바이스

IEEE 802.15.4에서는 두 가지 형태의 디바이스를 정의하고 있는데, FFD(Full Function Device)와 RFD(Reduced Function Device)이다. FFD는 어떠한 네트워크 구조에도 사용될 수 있고, RFD 및 다른 FFD 들과 통신할 수 있으며, PAN 코디네이터(Coordinator), 코디네이터, 단순 디바이스 세 가지 중 하나의 모드로 동작할 수 있다. 그러나 RFD는 스타형의 구조에만 사용될 수 있으며, 하나의 FFD와만 통신할 수 있도록 제한된다.

본 논문에서는 연결설정(association)을 결정할 수 있는 코디네이터가 중앙에 존재하고 여기에 FFD 및 RFD가 스타 형태로 연결되어 있는 네트워크 토폴로지를 기본 형태로 가정한다. 따라서, 새로운 디바이스가 네트워크에 결합할 경우 우선적으로 코디네이터에게 연결설정 요청 메시지를 보낸 후 응답을 기다려야 하며, 코디네이터는 이를 수용하기 위한 판단 알고리즘을 가지고 있어야 한다.

### 2.4 MAC 프레임 구조

IEEE 802.15.4의 표준 MAC 프레임은 무선 미디어의

특성을 고려하여 최소의 구성요소를 갖는 한편 프로토콜이 단순하고도 융통성 있도록 설계되었다. MAC 프레임은 헤더, 가변 길이의 페이로드, 그리고 푸터(footer)의 3부분으로 이루어져 있다[1,2]. MAC 헤더는 프레임 제어 필드와 주소 필드를 포함한다. 프레임 제어 필드는 프레임 타입, 보안, 그리고 주소 필드의 포맷과 내용을 지정하고, 이외 수신측으로부터의 이 프레임에 대한 확인 메시지가 필요한지도 나타낸다. 주소 필드는 프레임 제어 필드에 명시된 것으로 근원지나 목적지 주소를 포함한다. MAC 페이로드는 처리 중인 트랜잭션 타입에 특정한 정보를 포함하고, 상위 프로토콜 계층의 사용을 위해 여러 필드로 논리적으로 나누어질 수 있다.

마지막으로 MAC 푸터는 ITU-T 16비트 순환 잉여검사(CRC) 표준 알고리즘에 기초한 16 비트 프레임 검사 시퀀스(FCS)로 이루어진다. 일반적인 MAC 프레임 구조는 그림 3과 같다. IEEE 802.15.4 표준은 비콘(Beacon), 데이타(Data), 확인(Acknowledgment)과 MAC 명령어(MAC command)의 네 가지 MAC 프레임 타입을 정의하고 있다[2].

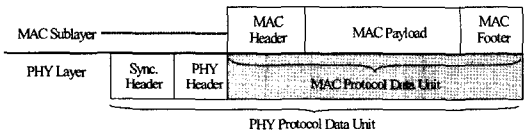



그림 3 일반적인 MAC 프레임 구조

**· 비콘(Beacon) 프레임**

비콘(beacon)을 사용하는 네트워크에서 FFD는 비콘 프레임을 전송할 수 있는데, 이 프레임의 주소 필드는 근원지 PAN ID와 근원지 디바이스 주소를 포함한다. 네트워크가 스타, 클러스터 트리, 혹은 또 다른 형태의 토폴로지인 경우에 상관없이 그 네트워크 내의 FFD만이 비콘 프레임을 전송할 수 있다.

**· 데이타(Data) 프레임**

데이타 프레임은 MAC 부계층이 데이타를 전송하는데 사용된다. 주소 필드는 근원지와 목적지의 PAN ID와 디바이스 ID를 포함한다. 네트워크가 스타, 클러스터 트리, 혹은 또 다른 토폴로지인가에 무관하게 모든 네트워크 디바이스들은 데이타 프레임을 사용할 수 있다. 이 프레임은 상위 프로토콜 계층에의 서비스로서 주 데이타 페이로드를 제공한다.

**· 확인(Acknowledgment) 프레임**

확인 프레임은 프레임의 성공적인 수신을 메시지의 원 송신 노드에게 알릴 목적으로 MAC 부계층이 전송한다. 수신 메시지에 확인 요청이 표시되어 있고, FCS 검사 결과 이상이 없을 때만 수신 노드는 확인 프레임을 생성한다. 확인 프레임은 MAC 헤더에 주소 필드와 MAC 페이로드를 포함하지 않는다. 확인 프레임을 수신하면 네트워크 디바이스는 먼저 이를 기다리고 있었는지, 또한 수신된 프레임 시퀀스 번호(sequence number)가 기다리던 번호인지를 체크한다. 이 검사를 통과하지 못한 확인 프레임은 버려진다. 확인 프레임도 네트워크가 스타, 클러스터 트리, 혹은 또 다른 토폴로지인가에 관계없이 네트워크 내의 모든 디바이스가 사용할 수 있다. 이 프레임은 상위 계층 프로토콜을 위한 서비스로 종단간 메시지 제어를 위한 데이타 수신 확인 기능을 제공한다.

**· MAC 명령어(MAC Command) 프레임**

MAC 부계층이 발송하는 MAC 명령어 프레임은 모든 MAC 명령어 프레임 타입의 MAC 제어 전송(MAC control transfers)을 담당한다. MAC 명령어 프레임의 MAC 페이로드는 MAC 명령어 타입과 MAC 명령어 페이로드의 두 필드로 구성되어 진다. MAC 명령어 페이로드는 각 명령어 타입에 고유한 정보로 이루어진다.

이러한 프레임들은 ZigBee에서의 보안 기술처럼 링크 키(*link key*)를 사용해 암호화 및 인증코드 생성할 수 있도록 정의되어 있으나 확인 프레임에서는 사용할 수 없다. 그림 4에서는 암호화 처리되는 부분을 나타내고 있으며 데이타 무결성 검증을 위해 인증코드를 생성하는 경우 프레임의 뒷부분에 포함시키게 된다.

| MAC Header | | | MAC Payload | MAC Footer |
|---|---|---|---|---|
| Frame control | Sequence number | Addressing Fields | Encrypted | FCS |

**Data frame format**

그림 4 MAC 프레임의 암호화와 인증

### 2.5 확인 프레임의 사용과 보안 취약성

IEEE 802.15.4 표준에서 데이타 또는 명령 프레임의 성공적인 전송과 검증은 확인(acknowledgment) 프레임에 의해 수행된다. 만약 송신 노드가 특정 시간이 지나도 확인 프레임을 수신하지 못한다면, 송신 노드는 전송이 실패한 것으로 판단하고 프레임 전송을 재시도 한다. 만약 최대 3번의 재시도 후에도 확인 프레임을 수신하지 못하면 송신 노드는 전송이 완전히 실패한 것으로 판단한다[1]. 이러한 확인 프레임은 전송되어진 프레임이 브로드캐스트 주소를 가지고 있지 않고, 송신 노드가 확인 프레임을 요청한 경우 수신 노드로부터 발생된다. 표준에서 정의하고 있는 확인 프레임의 형식은 매우 간단하다: 2 바이트의 프레임 컨트롤 필드, 1바이트의 시퀀스 번호, 그리고 2바이트의 CRC코드이다.

하지만, IEEE 802.15.4 표준은 확인 프레임의 보안

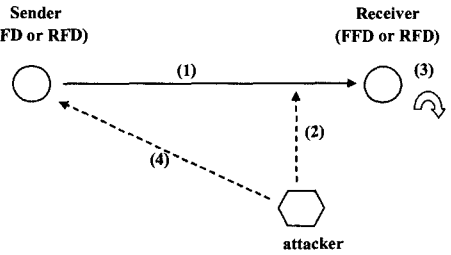



그림 5 확인 프레임을 통한 공격의 예

기능을 위한 어떠한 정의도 포함하고 있지 않다. 이러한 취약점은 공격자로 하여금 확인 프레임을 통한 공격을 용이하게 한다. 공격자는 단지 오리지널 프레임에 적합한 시퀀스 번호를 생성함으로써 옳지 않은 확인 프레임을 생성해 낼 수 있으며 이것은 매우 간단한 방법이다. 그 이유는 시퀀스 번호는 공개된 상태로 전송되기 때문이다. 그림 5는 이러한 취약성으로 인해 발생할 수 있는 공격의 예를 설명하고 있다.

(1) 송신 노드는 수신노드에게 패킷을 전송하면서 확인 프레임 요청필드(ACK Request)를 통해 정상적으로 패킷을 수신할 경우 시퀀스 번호를 사용해 확인 프레임을 보내줄 것을 요청한다.
(2) 공격노드는 패킷이 전송되는 순간에 간섭신호(interference)를 발생시켜 패킷에 오류가 발생하도록 한다.
(3) 수신노드는 수신한 패킷의 CRC값이 유효하지 않음을 확인하고 해당 패킷을 폐기한다.
(4) 공격노드는 시퀀스번호를 사용해 확인프레임을 생성하고 이를 송신노드에게 전송해 패킷이 제대로 전송되었다고 판단하도록 한다.

이러한 확인 프레임의 보안상의 취약성으로 인해 특정 프레임의 전송의 결과가 잘못 파악될 수 있으며, 그 결과 네트워크를 구성하는 디바이스들의 과부하 및 네트워크 전체에 심각한 위협을 가져올 수 있다[1,3,5]. 더욱이 확인 프레임은 페이로드 부분이 없어 보안을 위해 프레임을 활용하기 어렵다. 전통적인 보안방식을 통해 해쉬코드나 인증을 위한 데이타를 생성하는 것이 보안 강도의 측면에서 더욱 안전하겠으나 확인 프레임의 구조상 이러한 방법은 적용하기 어렵다.

### 2.6 코디네이터와 디바이스의 연결설정

IEEE 802.15.4 표준에서 모든 디바이스는 연결설정(association) 명령어를 요청하고 응답할 수 있는 기능을 포함하고 있다. 만약 새로운 디바이스가 코디네이터와 연결설정하기를 원한다면, 디바이스는 연결설정 요청 명령어를 생성하고 이것을 코디네이터에게 보낸다. 이때의 코디네이터는 특정 PAN ID와 주소를 가지고 있다. 만약 디바이스가 성공적으로 연결설정 요청 명령어를 전송하였다면, 디바이스는 이에 대한 응답으로 확인 프레임을 기다린다. 만약 일정 시간 이후에도 확인 프레임을 받지 못한다면, 연결설정 요청 명령어 프레임의 전송은 재시도 된다. 코디네이터가 연결설정 요청 명령어를 수신하게 되면, 코디네이터는 특정 알고리즘을 사용해 해당 디바이스를 수락할 것인지 또는 거절할 것인지 결정하게 된다. 그 후 코디네이터는 연결설정 응답 명령어를 생성하고, 이를 연결설정을 요청한 디바이스에게 보낸다[1].

## 3. 제안 사항

본 논문에서 제안하는 보안 메커니즘은 IEEE 802.15.4 네트워크에서 확인(acknowledgment) 프레임의 보안 취약성을 해결하기 위한 경량화 된 개체 인증 방법의 제시에 목적을 두고 있으며, 현재의 표준 형식을 수정하지 않고 사용가능하도록 하였다. 기존의 암/복호화 방법이나 인증코드를 통한 인증방법과 달리 본 논문에서 제안된 방법은 수신 노드로부터의 확인 프레임 안에 포함되어 있는 연속적인 비트 값을 통해 해당 확인 프레임이 정당한 디바이스로부터 발생되었는지를 확인하게 된다. 이러한 방법은 암호화, 복호화 및 인증코드를 생성하기 위한 연산과정을 거치지 않으므로 송신 및 수신 노드의 오버헤드를 크게 감소시킬 수 있다. 또한, 현재 표준에서 정의하고 있는 프레임 형식 및 통신과정을 변경하지 않으므로 적용하기 용이한 특징을 가지고 있다. 이는 매우 중요한 요소로써 현재의 IEEE 802.15.4의 내용을 기반으로 개발되고 있는 칩을 비롯한 장비들에 적용하기 위해서는 표준에서 정의하는 내용을 크게 수정하지 않으면서 보안 기능을 높일 수 있어야 한다.

• 용어정의(notation)

본 논문에서 제안하고 있는 경량 인증 메커니즘에서, 각 기능을 담당하는 모듈과 이러한 과정을 통해 발생하는 값들을 표 2와 같은 기호로 정의하여 사용한다.

그림 6은 본 논문에서 제안하는 경량 인증 메커니즘의 전체 동작과정을 나타내고 있다. 각 모듈 및 세부 동작과정은 아래 각 절에서 설명한다.

본 논문에서는 코디네이터와 디바이스 간에는 비밀키(secret key)를 공유한다는 것을 가정한다. 현재의 표준에서는 키 설정 및 공유 방법에 관한 부분은 상위 레이어의 방법을 따를 것을 제시하고 있으며, 이에 따라 ZigBee Alliance에서는 Security Service Specification을 정의하고 대칭키 기반의 키 설정 메커니즘을 제시하고 있다[4]. 본 논문에서 코디네이터와 디바이스간의 키 설정 방법은 ZigBee 표준에서 설정되는 키를 사용한다. 현재의 표준에 적용할 수 있는 방법은 확인 프레임의

표 2 용어 정의

| 기 호 | 의 미 |
|---|---|
| *C, D* | 코디네이터(Coordinator),<br>디바이스 (Device) |
| *ASG* | 인증 셋 생성기<br>(Authbit Sets Generator) |
| *SNG* | 셋 넘버 생성기<br>(Set Numbers Generator) |
| *ASC* | 인증 셋 체인<br>(Authbit Sets Chain) |
| $\{S\}_{CD}$ | *C*와 *D*가 공유하는 인증을 위한<br>*n*-비트 스트림. |
| *SP(k)* | *ASC*에서 *k*번째 셋을 가리키는 포인터<br>(Set Pointer) |
| $\{Authbit\}_{SP(k)}$ | *SP(k)*가 가리키는 셋의 3비트 인증 값 |

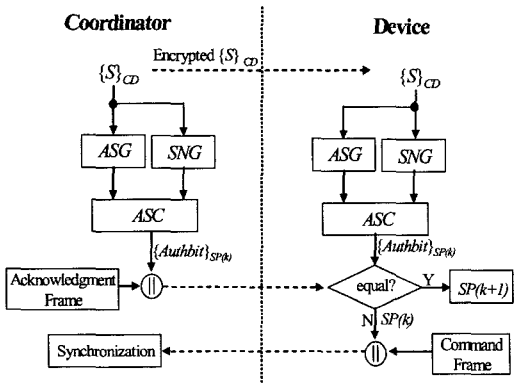



그림 6 경량 인증 메커니즘

프레임 제어 필드를 사용하는 방법이 가장 실효적이라고 볼 수 있으며 이 값은 3비트이다.

확률적으로 생각해볼 때 악의적인 디바이스는 이러한 비밀 키를 가지고 있지 않으므로 디바이스가 생성해 내는 3비트의 값을 연속적으로 *i*번 정확하게 맞출 확률은 $8^{-i}$ 보다 작다고 할 수 있다.

### 3.1 *Authbit Set*과 *Set Number*

먼저, 연결설정(association) 과정에서 코디네이터가 디바이스의 연결 요청을 수락하게 되면 코디네이터는 그림 7과 같은 암호화된 $\{S\}_{CD}$를 디바이스에게 전송한다. 앞서 언급한 바와 같이 IEEE 802.15.4 표준에서 데이타 프레임은 메시지 보호 기능을 가지고 있으므로 비밀 키를 사용하여 암호화된 $\{S\}_{CD}$를 전송함으로 악의적인 디바이스는 이 스트림을 알 수 없다. $\{S\}_{CD}$는 송신 노드와 수신 노드 간의 동일한 인증 체인을 생성하는 기본적인 데이타로 사용되어지며, 네트워크의 정책에 따라 일정 기간이 지난 후 갱신하거나, 재전송 할 수 있다.

다음 과정에서 코디네이터와 디바이스는 $\{S\}_{CD}$를 사용해 그림 8에서 설명하고 있는 *ASG*와 *SNG* 메커니즘

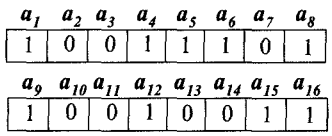
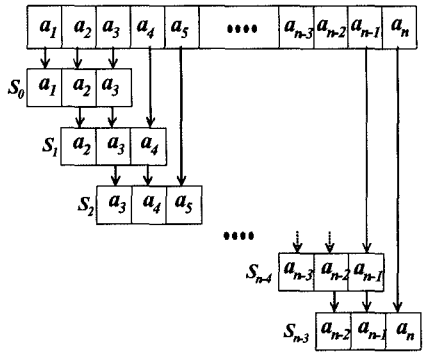
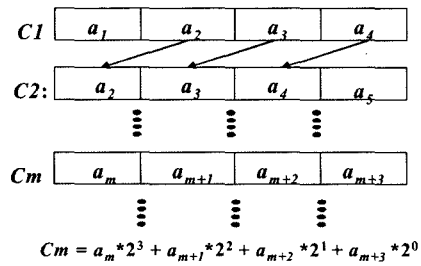



그림 7 *n*-bits $\{S\}_{CD}$의 예 (*n*=16인 경우)




(a) *ASG* scheme




(b) *SNG* scheme

그림 8 (a) *Authbit Sets*과 (b) *Set Numbers* 생성 메커니즘

을 통해 (a) *Authbit Sets*과 (b) *Set Numbers*를 생성한다.

- $S_m = \{a_{m+1}, a_{m+2}, a_{m+3}\}$
- $C_m = a_m*2^3+a_{m+1}*2^2+a_{m+2}*2^1+a_{m+3}*2^0$

예를 들어, 코디네이터와 디바이스가 그림 7에서 전송된 예와 같은 $\{S\}_{CD}$를 사용한다면,

- $S_0$={1,0,0}, $S_1$={0,0,1}, $S_2$={0,1,1}, $S_3$={1,1,1}과 같은 *Authbit Sets*이 생성되며,
- $C1=a_1*2^3+a_2*2^2+a_3*2^1+a_4*2^0$
  $=1*2^3+0*2^2+0*2^1+1*2^0=9$
- *C2*=3, *C3*=7

과 같은 *Set Numbers*가 생성된다. 마지막 과정으로 *ASG*와 *SNG*를 통해 생성된 *Authbit Set*과 *Set Number*는 3비트 단위의 인증 체인 값 구성에 사용된다.

*ASC* 메커니즘의 예는 그림 9와 같으며 그림에서의 세부 비트 값은 그림 7에서 예로 든 스트림을 사용했을

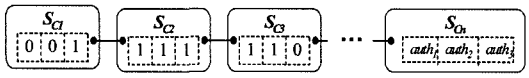



그림 9 *ASC* scheme

경우이다. 즉, *SNG*를 통해 *C1*=9, *C2*=3, *C3*=7이 생성되었으므로 인증 체인의 첫 번째는 $S_9$, 두 번째는 $S_3$, 그 다음은 $S_7$의 순서로 구성된다.

이러한 인증 체인은 코디네이터와 디바이스에서 동일한 순서와 비트 값으로 생성되고, 확인 프레임을 보내는 노드(코디네이터 또는 디바이스)는 다음 절에서 설명할 포인터가 가리키고 있는 비트 값(3비트)을 확인 프레임 안에 포함하여 보내며, 이러한 확인 프레임을 받은 노드(코디네이터 또는 디바이스)는 이 비트 값이 현재 자신의 포인터가 가리키고 있는 비트 값과 일치하는지를 비교하여 인증을 하게 된다.

### 3.2 *Set Pointer*를 사용한 동기화

*ASC*가 생성된 후 코디네이터와 디바이스의 셋 포인터 (Set Pointer)는 *SP(1)*, 즉 인증 체인의 첫 번째 셋을 가리키며 동기화 된다. 동기화가 이루어진 이후부터 확인 프레임을 보내는 노드는 *ASC*에서 현재 자신의 *SP(k)*가 가리키는 셋의 3비트 값인 $\{Authbit\}_{SP(k)}$을 프레임에 포함시켜 보낸다. 확인 프레임을 송신하는 노드는 이 값을 포함하여 보낸 후 포인터를 다음 셋으로 한 단계 이동시키므로 *SP(k+1)*에 포인터가 위치하게 된다. 확인 프레임을 수신한 노드는 프레임 안에 포함된 3비트의 값이 자신의 $\{Authbit\}_{SP(k)}$값과 일치하는지를 확인한다. 만약 이 값이 동일하다면 수신 노드의 포인터도 *SP(k+1)*로 이동한다. 그러나, 만약 $\{Authbit\}_{SP(k)}$값이 일치하지 않을 경우, 명령어(command) 프레임을 사용해 현재의 *SP(k)*값을 송신 노드에게 전달하면서 포인터를 동기화시키고, 확인 프레임을 다시 보낼 것을 요청한다.

*SP(k)*의 동기화 메커니즘은 그림 10에서 설명하고 있다. s는 두 노드 사이에서 현재까지 발생한 동기화 횟수를 나타내며 다음 절에서 설명될 확률 기반의 공격 판별에 사용된다. 이 그림에서는 코디네이터를 수신 노드로 가정한다. 즉, 코디네이터가 확인 프레임을 디바이스로부터 받는 경우이다.

**Synchronization algorithm**

// Coordinator receives acknowledgment frame with $[\{Authbit\}_{SP(k)}]_{device}$
if $[\{Authbit\}_{SP(k)}]_{device} = [\{Authbit\}_{SP(k)}]_{coordinator}$ then
*SP(k+1)*
else if $[\{Authbit\}_{SP(k)}]_{device} \neq [\{Authbit\}_{SP(k)}]_{coordinator}$ then
*s* ++
Coordinator → Device:
Command frame {*SP(k)*, retransmission after synchronization}

그림 10 동기화 메커니즘

## 4. 확률적 분석 및 IEEE 802.15.4에서의 적용

### 4.1 확률적 분석

제안된 인증 메커니즘의 주된 목적의 하나는 에러로 인해 확인 프레임의 손실이 발생할 수 있는 무선 환경에서 인증 비트 값이 다른 이유가 공격에 의한 것인지, 손실에 의한 것인지 판단하는 것이다. 본 논문에서는 제안된 인증 메커니즘을 분석하고 확률적인 이론을 통해 확인 프레임을 보내는 노드의 정당성을 판단할 수 있는 확률적 방법을 제시한다. 그림 10의 알고리즘에서 $[\{Authbit\}_{SP(k)}]_{device}$와 $[\{Authbit\}_{SP(k)}]_{coordinator}$가 일치하지 않는 이유는 두 가지의 가능성으로 나누어 볼 수 있다. 첫째 송신 노드와 수신 노드의 *SP(k)*가 동기화 되어 있지 않거나, 둘째 확인 프레임을 보낸 송신 노드가 악의적인 공격자인 경우이다. 에러가 발생하지 않는 완벽한 채널 환경에서 정당한 송신 노드와 수신 노드의 동기화 문제는 쉽게 파악하여 해결 할 수 있다. 하지만, 에러로 인한 확인 프레임의 손실이 발생할 수 있는 무선 네트워크에서 수신 노드는 비동기화의 문제가 공격자로 인한 것인지 아니면 무선 채널 상에서 발생한 손실 때문인지 결정하기 어렵다. 본 논문에서는 이러한 환경에서 공격자를 판별하기 위해 WLAN 환경에서 1비트 기반의 인증 메커니즘을 제안했던 기존 연구 [6,7]에서의 이론을 참조하여, 확률적 방법을 제안한다.

우선 두 노드 사이에서 현재까지 송수신한 전체 확인 프레임의 수를 $n$으로 하고, 디바이스와 코디네이터 사이에 행해진 동기화 수를 $s$, 에러로 인한 확인 프레임의 손실률을 $r(0 \le r \le 1)$로 설정할 경우 아래와 같은 이론을 도출할 수 있다.

**[이론]**

확인 프레임을 송신한 노드를 $D$라 하면, $D$가 공격자일 확률은 $\frac{1}{8}$, 다시 말해, $P(D=attacker)=\frac{1}{8}$이고 $P(D=legitimate)=\frac{7}{8}$이다.

전체 확인 프레임의 개수($n$)와 현재까지의 동기화 회수($s$)를 통해 확률적으로 정리하면 송신 노드가 공격 디바이스일 확률 $P(D=attacker \mid n, s)$는 식 (1)과 같다.

$$P(D=attacker \mid n, s) = \frac{2^{-n}}{2^{-n} + 7^{*} r^{s}(1-r)^{n-s}} \quad (1)$$

**[증명]**

송신디바이스와 수신 노드 사이 전송된 전체 확인 프레임의 개수($n$)와 동기화 회수($s$)에 따른 확률 값에서 정당한(legitimate) 노드와 공격(attacker) 노드의 관계는 다음과 같다.

$$P(D=legitimate \mid n, s)=1-P(D=attacker \mid n, s).$$

Bayer의 공식에 따라, 식 (2)를 유추할 수 있다. (at.:attacker, leg.:legitimate를 의미함)

$$P(D=attacker \mid n,\ s) = \frac{P(n,s|D=at.)*P(D=at.)}{P(n,s|D=at.)*P(D=at.)+P(n,s|D=leg.)*P(D=leg.)} = \frac{P(n,s|D=at.)}{P(n,s|D=at.)+7*P(n,s|D=leg.)} \quad (2)$$

먼저, 송신 노드가 공격 노드일 경우를 생각해보면 공격자는 $ASC$를 알 수 없다. 이 경우 $P(n,\ s\ |D=attacker)$은 식 (3)과 같이 정리될 수 있다:

$$P(n,\ s\ |D=attacker) = \binom{n}{s} * 2^{-n} \quad (3)$$

다음으로 송신 노드가 정당한 노드인 경우를 생각해 보면, 확인 프레임 손실률이 $r$이고, 동기화 회수가 $s$인 경우

$P(n,\ s \mid D=legitimate)$는 식 (4)로 정리될 수 있다:

$$P(n,\ s \mid D=legitimate) = \binom{n}{s} * r^{s}(1-r)^{n-s} \quad (4)$$

식 (2),(3),(4)를 정리하면 식 (1)을 유추할 수 있다.

다시 말해,

$$P(D=attacker|n,s) = \frac{2^{-n}}{2^{-n}+7*r^{s}(1-r)^{n-s}}.$$

### 4.2 공격 노드 판별

그림 11은 4.1절에서 유추한 식을 사용해 확인 프레임을 전송한 노드가 정당한 노드일 확률을 계산한 것이다.

이 값에서 $n$=10, 분석 값은 $r$=10%, 20%, 30% 일 경우이다. 예를 들어, 프레임 손실률($r$)이 20%인 네트워크 환경에서 동기화가 4번 발생했을 경우 전송 노드가 정당한 노드일 확률은 80%에 근접하지만 동기화가 5번 발생했을 경우는 50% 미만이다. 따라서 어느 정도의 신뢰 수준을 결정하고, 동기화에 따른 정당한 노드의 확률이 그 수준 이하가 될 경우 공격 노드로 추정할 수 있다. 그림 11과 같은 확률적 값을 근거로 현재까지의 전체 확인 프레임의 개수와 동기화 횟수에 따른 공격 노드 판단이 가능하게 되는 것이다.

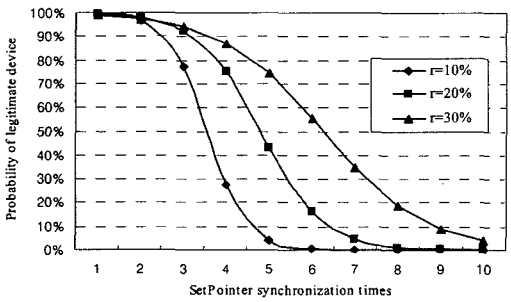



그림 11 송신 노드가 정당한 노드일 확률

### 4.3 성능 평가

논문에서 제안하는 방법의 성능평가를 위해 MATLAB[8]을 사용하였다. 제안하는 방식은 LR-WPAN과 ZigBee의 보안 기술 및 정의된 프레임을 유지하는데 초점을 맞추어 인증을 위해 3비트만을 사용하였다. 따라서, 보안 강도의 측면에서는 한계를 드러내고 있으며 그 결과를 그림 12에서 확인할 수 있다. 그러나, 만약 제안된 방식이 인증코드로 4비트, 5비트 또는 그 이상의 필드를 사용할 수 있다면 보안 강도의 문제는 해결될 수 있을 것이다.

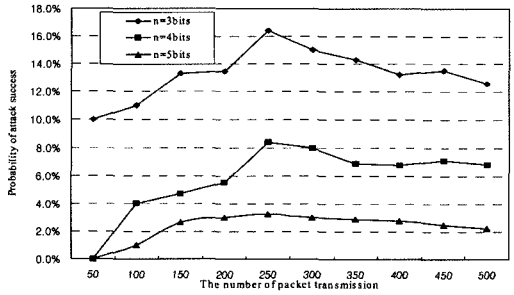



그림 12 인증코드와 공격 성공률

또한, 제안된 방식을 적용하기 위해서는 코디네이터와 디바이스가 앞서 설명한 인증 코드 생성관련 모듈을 가지고 있어야 하고 동기화를 필요로 하므로 통신 지연 및 추가적인 오버헤드를 가지게 된다. 그림 13은 인증코드 사용으로 인한 통신지연의 결과를 보여주고 있다.

그림 14는 확인 프레임 인증 방법을 사용하지 않는 상태에서 공격 노드의 공격빈도(a)에 따라 얼마만큼의 재전송이 발생되는지의 결과를 나타내고 있다. 본 논문에서 제안하는 방식은 인증 체인 생성을 위한 연산과 오버헤드를 가지고 있으나, 이러한 확인 프레임의 인증 절차 없이 공격이 발생할 경우 패킷 재전송을 통한 네트워크의 부하가 매우 클 수 있음을 알 수 있다.

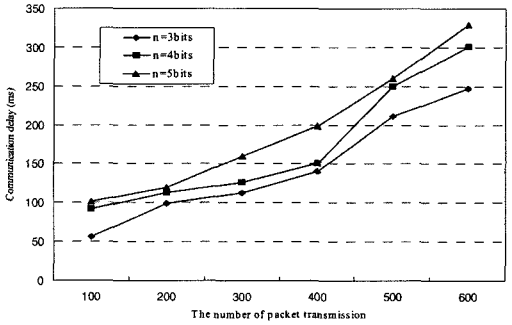



그림 13 인증코드 사용에 의한 통신 지연

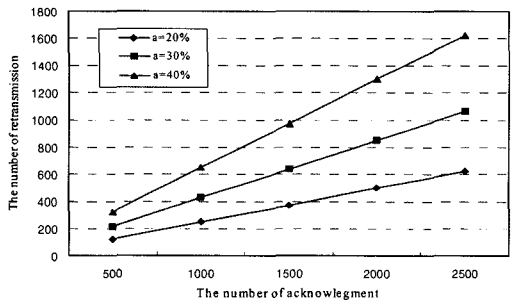



그림 14 공격노드에 의한 재전송 오버헤드

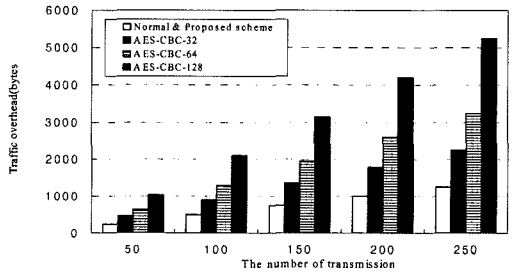



그림 15 트래픽 바이트(traffic byte) 오버헤드

그림 15는 트래픽 바이트 오버헤드의 측정결과를 나타내고 있다. 본 논문에서 제안하는 방식은 표준에서 예약비트로 정의된 3비트를 사용하고 있으므로 인증을 위해 추가적으로 프레임을 생성하지 않는다. 그러나 확인 프레임의 보안 문제점의 해결책으로 제시된 기존의 방법[5]처럼 AES-CBC를 사용해 인증코드를 생성하고 이를 활용할 경우 최대 128비트의 프레임을 추가적으로 생성하게 된다. 그림 15에서는 본 논문에서 제안하는 방식과 인증코드를 추가적으로 생성할 경우의 결과를 비교하여 나타내고 있다.

### 4.4 IEEE 802.15.4 표준에의 적용

또한, 본 논문에서는 기존의 IEEE 802.15.4 표준에 제안된 메커니즘을 어떻게 적용할 수 있는지 기술한다. 제안된 메커니즘을 위해서는 여분의 비트가 필요하지만, 기존의 IEEE 802.15.4 MAC 프레임 형식을 수정하지 않고 예약된 비트(reserved bits)를 사용한다. 이것은 제안된 메커니즘이 기존의 프레임 구조 및 동작과정을 따른다는 것을 의미하며 정당한 노드들이 제안된 인증 메커니즘을 사용할 경우 가용성을 높일 수 있게 된다.

그림 16은 IEEE 802.15.4 표준에서 정의하고 있는 일반적인 확인 프레임의 구조와 프레임 컨트롤 필드를 보여주고 있다. 본 논문에서 사용하는 3비트 $\{Authbit\}_{SP(k)}$ 값은 그림 16에서 보이는 것처럼 확인 프레임의 프레임 컨트롤 필드 중 사용 가능한 3비트 안에 포함되어 전달된다.

그림 17은 앞서 그림 7에서 설명한 $n$-bits $\{S\}_{CD}$를 전달하는 방법을 나타내고 있다. 데이타(Data) 프레임의 경우 페이로드 부분을 암호화 할 수 있는 보안 기능을 가지고 있으므로, 연결설정 과정이 성공할 경우 코디네이터는 $\{S\}_{CD}$를 생성하고 암호화하여 디바이스에게 보낸다. 또한, 앞서 인증 메커니즘에서 설명한바와 같이 확인 프레임을 수신한 노드가 인증에 실패할 경우 명령어 프레임을 사용해 $SP(k)$를 송신 노드에게 보내고, 동기화를 실행한 후 확인 프레임을 다시 보내도록 요청하게 된다.

이를 위해 그림 18의 (b)와 같이 새로운 명령어 형식인 Acknowledgment authentication fail을 정의하였다.

**Acknowledgment frame format**

| Octets: 2 | 1 | 2 |
|---|---|---|
| Frame control | Sequence number | FCS |

| Bits: 0-2 | 3 | 4 | 5 | 6 | 7-9 | 10-11 | 12-13 | 14-15 |
|---|---|---|---|---|---|---|---|---|
| Frame type | Security enabled | Frame pending | ACK. request | Intra-PAN | $\{Authbit\}_{SP(k)}$ | Dest. Addressing mode | Reserved | Source. Addressing mode |

그림 16 IEEE 802.15.4 표준에서의 확인(acknowledgment) 프레임 형식

**Data frame format**

| MAC Header | | | MAC Payload | MAC Footer |
|---|---|---|---|---|
| Frame control | Sequence number | Addressing Fields | Encrypted $n$-bits *Authbit* stream | FCS |

그림 17 데이타 프레임을 이용한 $\{S\}_{CD}$전송

**Command frame format**

| MAC Header | | | MAC Payload | | MAC Footer |
|---|---|---|---|---|---|
| Frame control | Sequence number | Addressing Fields | Command Type | MAC Command Payload | FCS |

(a) 명령어 프레임 형식

| Command Identifier | Command Type |
|---|---|
| 1 | Association Request |
| 2 | Association Response |
| 3 | Disassociation Notification |
| 4 | Data Request |
| 5 | PAN ID Conflict Notification |
| 6 | Orphan Notification |
| 7 | Beacon Request |
| 8 | Coordinator Realigment |
| 9 | GTS Request |
| | |
| 11-255 | Reserved |

(b) 인증 실패 명령어 정의

그림 18 명령어 프레임 형식 정의

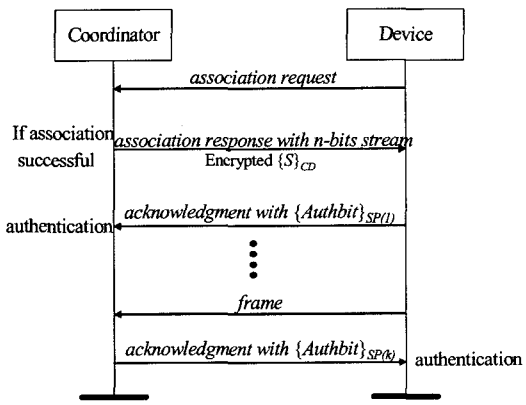



그림 19 연결설정 및 확인프레임 인증과정

이 명령어는 인증에 실패한 경우 발생되어 전달된다. 이 때 $SP(k)$ 값은 그림 18의 (a)와 같이 페이로드 부분에 포함시켜 보낸다. 그림 19는 초기 연결설정 과정부터 암호화된 $\{S\}_{CD}$의 전송과 $\{Authbit\}_{SP(k)}$를 통한 확인 프레임의 인증을 전체 시퀀스 차트 형식으로 나타내고 있다. 이 시퀀스 차트에서의 연결 설정 및 확인 프레임의 교환은 표준에서 정의하고 있는 순서 및 방법을 따른다.

## 5. 결론 및 향후과제

본 논문에서는 IEEE 802.15.4 네트워크에서 확인 프레임을 위한 경량화된 개체 인증 메커니즘을 제안하였다. 현재의 표준에서 확인 프레임은 페이로드 부분을 포함하고 있지 않다. 따라서, 표준에서 제안하고 있는 암호화 및 인증 방식을 그대로 적용할 수 없으며, 전통적인 보안 알고리즘도 사용하기 어렵다. 제안된 메커니즘은 송신 노드와 수신 노드간의 확인 프레임에 인증을 위한 3비트 값을 포함시키고 이를 사용해 개체 인증을 수행한다. 에러로 인한 손실이 발생할 수 있는 무선 네트워크 환경에서 손실과 공격을 구분할 수 있는 방법을 확률적 이론에 근거하여 제시하였으며, 현재의 표준을 수정하지 않고 제안된 메커니즘을 적용할 수 있는 방법에 대해서도 논하였다. 향후 과제로는 제안된 메커니즘을 실제 디바이스에 적용하여 정확한 성능 및 보안성을 테스트하고, 실제 적용에서 발생할 수 있는 문제점을 발견하여 해결해야 할 것이다.

## 참 고 문 헌

[1] "Wireless Medium Access Control and Physical Layer Specification for Low-Rate Wireless Personal Area Networks," IEEE Standard, 802.15.4-2003, May 2003.

[2] Jose A. Gutierrez, Edgar H. Callaway Jr and Raymond L. Barrett Jr, "Low-Rate Wireless Personal Area Networks," IEEE Press 2003.

[3] N. Sastry and D. Wagner, "Security Consideration for IEEE 802.15.4 Networks," Proc. of WiSe 2004, pp.32-42, September 2004.

[4] ZigBee Document, "Security Service Specification Version 1.00," at www.zigbee.org

[5] Yang Xiao, Sakshi Sethi, Hsiao Hwa Chen and Bo Sun, "Security Service and Enhancements in the IEEE 802.15.4 Wireless Sensor Networks," Proc. of IEEE GLOBECOM 2005, pp.1796-1800, November 2005.

[6] H. Johnson, A. Nilsson, J. Fu, S. F. Wu, A. Chen and H. Huang, "SOLA: A One-bit Identity Authentication Protocol for Access Control in IEEE 802.11," Proc. of IEEE GLOBECOM 2002, pp.768-772, November 2002.

[7] H. Wang, A. Velayuthan and Y. Guan, "A Lightweight Authentication Protocol for Access Control in IEEE 802.11," Proc. of IEEE GLOBECOM 2003, pp.1384-1388, December 2003.

[8] MATLAB, at www.mathworks.com

허 준

2002년 경희대학교 컴퓨터공학과(공학사). 2004년 경희대학교 컴퓨터공학과(공학석사). 2004년~현재 경희대학교 컴퓨터공학과 박사과정. 관심분야는 유무선 네트워크 보안, 보안 게이트웨이, Power Line Communication Security

홍 충 선

1983년 경희대학교 전자공학과(공학사) 1985년 경희대학교 전자공학과(공학석사) 1997년 Keio University, Department of Information and Computer Science (공학박사). 1988년~1999년 한국통신 통신망 연구소 수석 연구원 / 네트워킹연구실장. 1999년~현재 경희대학교 전자정보학부 부교수. 관심분야는 네트워크 보안, 인터넷 서비스 및 망관리 구조, 분산 컴포넌트 관리, IP 프로토콜, 센서 네트워크