Journal of Korea Multimedia Society Vol. 12, No. 9, September 2009(pp. 1323-1332)

순번을 이용한 고속의 안전한 무선 랜 2-Way 핸드쉐이크 기법

임 정 미†

요 약

본 논문은 IEEE 802.11i의 4-Way 핸드쉐이크의 취약점을 분석하고, 고속의 안전한 2-Way 핸드쉐이크 방식을 제안한다. PTK 생성에서 난수 대신에 순번(Sequence Number)을 사용하여, 재생공격, DoS 공격을 방지한다. 또한 Re-association Request 프레임과 Re-association Response 프레임을 변형하여 MS(Mobile Station)과 AP(Access Point) 사이의 상호 인증과, PTK(Pairwise Transient Key)의 도출을 가능하게 하여, 전송되는 메시지의 개수를 감소시켜, 4-Way 핸드쉐이크보다 고속의 핸드오프 방식을 제안한다. 그리고 고속의 안전한 핸드오프를 제안하는 기존의 기법들과 비교 분석한다.

Fast and Secure 2-Way Handshake Mechanism using Sequence Number in Wireless LAN

Lim Jeong mi†

ABSTRACT

In this paper, we analyze security weakness of 4-Way Handshake in IEEE 802.11i and propose fast and secure 2-Way Handshake mechanism. Compute PTK(Pairwise Transient Key) using sequence number instead of random numbers in order to protect Replay attack and DoS attack. Also, proposed 2-Way Handshake mechanism can mutual authenticate between mobile station and access point and derive PTK using modified Re-association Request and Re-association Response frames. And, compare with others which are fast and secure Handoff mechanisms.

Key words: 802.11i(802.11i), 4-Way Handshake(4-Way 핸드쉐이크), handoff(핸드오프), 2-Way Handshake(2-Way 핸드쉐이크), sequence number(순번), DoS attack(서비스 거부 공격), Replay attack(재생 공격)

1. 서 론

최근 802.11[1] 무선 네트워크 기반의 VoIP(Voice over IP), 멀티미디어 활용, 데이터 전송 등의 인터넷 서비스가 많이 사용되고, 빠르게 발전하고 있다.

특히 시간에 민감한 VoIP 애플리케이션의 경우에는, MS(Mobile Station)의 이동성으로 인하여 현재의 AP(Access Point)에서 다른 AP로 로밍 할 때, 핸드오프 시간이 길어지면 데이터 전송의 끊김이 발생한다. 그러므로, 802.11 무선 네트워크 환경에서 빠르고 안전한 핸드오프의 중요성이 강조되고 있다.

현재의 IEEE 802.11 표준의 보안 결점을 해결하기 위하여, 802.11i[2] 작업 그룹은 RSN(Robust Security Network)을 제안했다. RSN의 과정은 그림 1과 같다. MS는 개방시스템(open-system) 인증을 이용하여 AP에게 자신을 인증한다. MS와 AP는 서

※ 교신저자(Corresponding Author) : 임정미, 주소 : 충남 천안시 안서동(330-714), 전화 : 041)550-1576, FAX : 041) 550-3460, E-mail : redpig3@dankook.ac.kr

접수일 : 2009년 8월 3일, 수정일 : 2009년 8월 23일
완료일 : 2009년 8월 30일

† 정회원, 단국대학교 교양학부 강의전임 강사

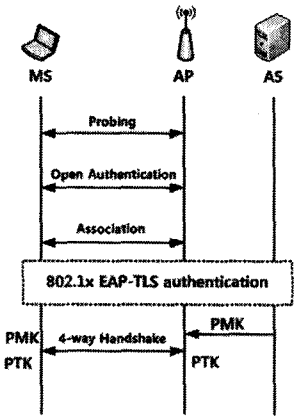

그림 1. 초기 전체 인증 과정

로 (Re)Association Request 메시지와 (Re) Association Response 메시지를 주고받아 Association 한다. 이렇게, MS와 AP 사이의 접속이 이뤄지면, 둘 사이의 공통키인 PMK(Pairwise Master Key)를 생성한다. PMK는 미리 공유된 키를 사용하거나, 그림 1과 같이 AS(Authentication Server)를 두어 EAP-TLS 인증과 같은 IEEE 802.1X 인증을 통해서 생성된다. AS는 생성된 PMK를 안전하게 AP로 전달한다. 그 후 AP와 MS는 4-Way 핸드쉐이크를 통하여 상호인증하고, AP와 MS 사이의 전송되는 데이터 프레임을 보호하기 위한 세션키 PTK를 도출한다.

고속의 안전한 핸드오프를 위하여 선행인증(Pre-Authentication)과 PKD(Proactive Key Distribution)[3]를 이용하여 지연시간을 단축시키는 연구가 많이 진행되고 있다. 그러나 본 논문에서는 MS와 AP 사이의 상호인증과 PTK 도출을 위한 4-Way 핸드쉐이크 단계에서의 보안 취약점[4,5]을 분석하고, 4-Way 핸드쉐이크보다 고속의 안전한 2-Way 핸드쉐이크를 제안한다. DoS 공격과 재생 공격을 방지하기위하여 PMKSA(PMK Security Association)에 0으로 초기화된 순번을 추가하고, 이 순번을 이용하여 PTK를 생성하고, RR(Re-association Request) 프레임과 RP(Re-association resPonse) 프레임을 변형하여 메시지의 개수를 줄이는 방식을 제안한다.

본 논문의 구성은, 2장에서는 4-Way 핸드쉐이크의 기능과 보안상의 취약점을 설명하고, 이를 보완할 수 있는 다른 기법들을 소개한다. 3장에서는 4-Way 핸드쉐이크 프로토콜의 단점을 보완하는 2-Way 핸드쉐이크 방식을 제안하고, 4장에서는 제안하는 프로토콜을 분석하고 기존의 방식과 비교한다. 5장에서는 결론을 맺는다.

2. 4-Way 핸드쉐이크와 같은 기능을 하는 핸드오프 기법들

2.1 4-Way 핸드쉐이크 프로토콜의 단계와 특징

MS는 IEEE 802.1x Supplicant와 IEEE 802.11MAC으로 나뉘고, AP는 IEEE 802.1x Authenticator와 IEEE 802.11 MAC으로 나뉜다. 그림 2와 같이, 4-Way 핸드쉐이크는, Supplicant와 Authenticator 사이에 4개의 메시지를 주고받는다. Supplicant와 Authenticator는 인증 단계에서 생성된 PMK를 이용하여 PTK를 생성하고, 두 개체사이의 상호 인증을 목적으로 한다.

세션키 PTK는 식 (1)과 같이 계산된다.

$$PTK = prf(PMK, SNonce, ANonce, AP, MS) \quad \text{식 (1)}$$

이때, prf는 키 생성 함수이고, ANonce와 SNoce는 각각 Authenticator와 Supplicant에 의해서 생성된 난수이다. AP와 MS는 각각, Authenticator와 Supplicant의 802.11 MAC 주소이다. msg1, msg2, msg3, msg4는 다른 메시지 종류를 나타내고, MICPTK()은 PTK를 이용하여 만들어진 MIC (Message Integrity Code) 값이다. 4-Way 핸드쉐이크의 각 단계별로 전송되는 값 전체를 4H1, 4H2,

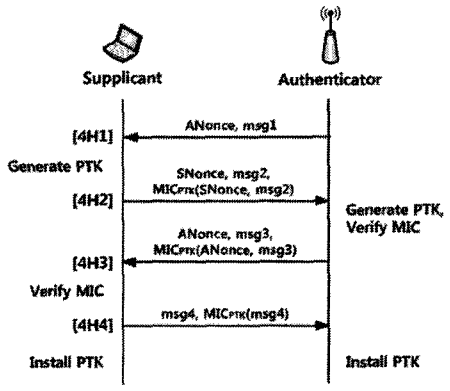

그림 2. 기본 4-Way 핸드쉐이크

4H3, 4H4로 나타낸다. 4-Way 핸드쉐이크의 과정은 먼저, Authenticator가 난수 ANonce를 생성하여 Supplicant로 4H1을 전송한다. 4H1을 수신한 Supplicant는 자신이 생성한 SNonce를 이용하여 PTK를 생성하고, SNonce와 PTK를 이용한 MICPTK를 Authenticator에게 보낸다. 4H2를 수신한 Authenticator는 이전에 자신이 생성한 ANonce와 Supplicant로부터 받은 SNonce를 이용하여 PTK를 생성할 수 있으므로 MICPTK를 확인할 수 있다. MICPTK가 정상적으로 확인이 되면, Authenticator는 Supplicant도 같은 PMK를 갖고 있음을 알 수 있어 정당한 Supplicant임을 인증하고, 도출된 PTK를 이용하여 이전에 생성한 ANonce와 MICPTK를 포함한 4H3을 Supplicant에게 전송한다. 4H3을 수신한 Supplicant 또한 MICPTK를 확인하여 Authenticator가 정당한 Authenticator인 것이 인증되면 PTK를 설치하고 4H4를 Authenticator에게 전송한다. 이때, 4H4는 보안적 의미 없이, 단순하게 4H3을 잘 받았고 정상적으로 PTK를 설치했다는 의미에서 전송된다. Authenticator는 Supplicant로부터 수신한 4H4를 확인한 후 PTK를 설치한다.

Supplicant와 Authenticator은 수신한 MICPTK() 값이 유효하지 않으면 수신한 메시지를 버린다. timeout1과 timeout2는 각각, Supplicant와 Authenticator에서의 시간간격(time interval)을 나타낸다. 4-Way 핸드쉐이크에서 Authenticator와 Supplicant는 시간간격을 처리하는 방법이 다르다. 그림 3과 같이, Supplicant는 성공적인 802.1x EAP-TLS 인증 후, timeout1이내에 4H1이 수신되지 않으면 재시도 없이 Dis-associate, De-authenticate 한다. 그러나, 그림 4와 같이, Authenticator는 timeout2 이내에 보낸 메시지에 대한 응답을 메시지의 응답을 받지 못하면,

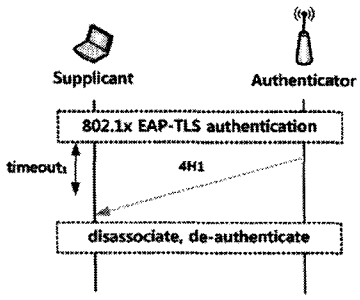

그림 3. Time interval in Supplicant

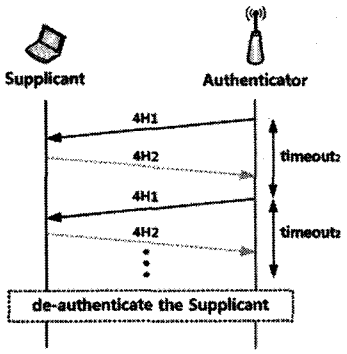

그림 4. Time interval in Authenticator

정해진 재전송 회수만큼 반복해서 메시지를 재전송하고, 그 후에도 응답을 받지 못하면 Supplicant를 De-authenticate 한다.

2.2 4-Way 핸드쉐이크 프로토콜의 취약점

4-Way 핸드쉐이크 과정에서, 정당한 Authenticator와 Supplicant는 4H1, 4H2, 4H3, 4H4를 주고받을 수 있다. 그러나 4H1의 메시지는 데이터를 보호 할 수 있는 보안적 요소가 없이 전송되기 때문에, 공격자에 의해서 ANonce 값의 변조가 가능하다.

예를 들어 그림 5와 같이, 정당한 Authenticator가 Supplicant에게 4H1을 보내고, Supplicant는 식 (1)을 이용하여 PTK를 생성하여 4H2를 Authenticator에게 보낸다. 정상적인 경우라면, 4H2를 수신한 Authenticator는 수신한 SNonce와 자신이 4H1을 보낼 때 사용했던 ANonce로 식 (1)에 의해서 PTK를

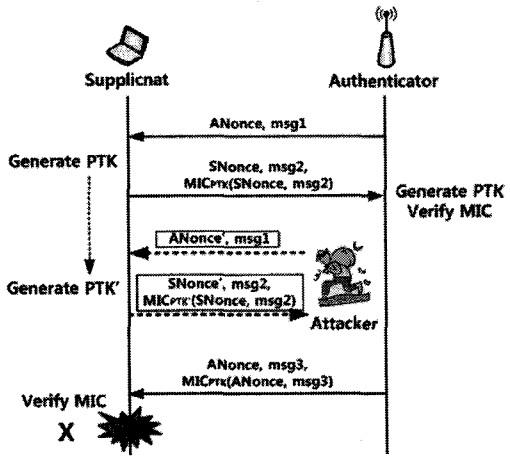

그림 5. 4-Way 핸드쉐이크에서 발생하는 Dos 공격

생성하여 MIC값이 정상적으로 확인이 되면 Supplicant에게 4H3을 보내야한다.

그러나 Authenticator가 4H3을 보내기 전에, 공격자가 ANonce를 위조한 ANonce'을 생성하여 4H1'을 Supplicant에게 보낼 경우, Supplicant는 ANonce를 사용한 PTK가 아닌 ANonce'를 사용하여 식 (2)와 같이 PTK'을 생성하여 4H2'을 공격자에게 전송한다.

$$PTK' = prf(PMK, SNonce, ANonce', AP, MS) \quad \text{식 (2)}$$

공격 사실을 모르는 Authenticator는 4H3를 생성하여 Supplicant에게 보내고, 4H3을 수신한 Supplicant는 PTK와 PTK'이 다르므로 Authenticator에게 4H4를 보내주지 않는다. 2.1에서 설명한 것과 같이, Authenticator는 정해진 timeout 이내에 응답(4H4)이 오지 않으면 4H3의 전송을 반복한다. 이와 같이 Authenticator가 4H2를 받은 후 4H3을 보내는 사이에 공격자가 4H1'을 반복적으로 보낼 경우 DoS 공격이 발생한다. 이 DoS 공격의 발생원인은 Authenticator가 Supplicant에게 보내는 4H1에 ANonce 값의 무결성을 보장할 수 있는 보안적 요소가 없기 때문이다. 보안적 요소가 없어 보호받지 못하는 4H1 메시지가 4-Way 핸드쉐이크의 가장 기본적인 취약점이다. 즉, 4-Way 핸드쉐이크는 Supplicant와 Authenticator 사이의 상호인증과 PTK 도출하지만, 보안상의 취약점으로 공격의 대상이 된다.

2.3 4-Way 핸드쉐이크 기능을 대신하는 핸드오프 기법들

EAP/TLS 인증을 변형한 방법[6]으로, 4-Way 핸드쉐이크에 사용되는 4개의 메시지를 2개씩 나누어 선행인증(pre-authentication) 단계에서 2-Way 핸드쉐이크하고, 재인증(re-authentication) 단계에서 나머지 2-Way 핸드쉐이크를 사용한다. 선행 인증단계에서 그림 6의 EAP-TLS:empty, EAP-Success 메시지를 그림 7과 같이 난수 SNonce와 MIC 값을 첨부하여 EAP-TLS(SNonce), EAP-Success (ANonce, MIC)로 변경하여 상호인증과 PTK를 도출한다. 그림 7에서 2H1, 2H2는 각각, 2-Way 핸드쉐이크의 첫 번째, 두 번째 메시지를 의미하고, EPTK()는 PTK로 암호화하는 것을 의미한다. 재인증 단계에서의 2-Way 핸드쉐이크에서는 선행인증 단계에서 생성

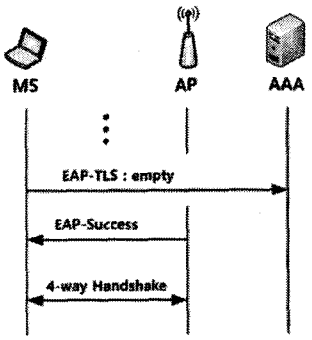

그림 6. 4-Way 핸드쉐이크

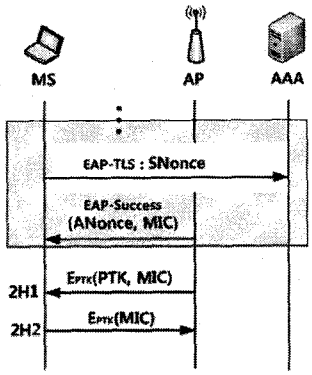

그림 7. 2-Way 핸드쉐이크

된 PTK값을 이용하여 PTK와 MIC값을 PTK로 암호화하여 전송하여 MS가 정당한 PMK와 PTK를 사용하고 있는지 확인할 수 있다. 그러나 이 방식은 선행 인증 단계에서 첫 번째 메시지의 SNonce 값이 MIC 값도 없이 평문으로 전송되기 때문에, DoS 공격과 재생공격을 받을 수 있다.

3-Way 핸드쉐이크 방식[7]은, 그림 2의 기존의 4-Way 핸드쉐이크 방식에서 4H4를 제외하는 방식이다. 2.1에서와 같이, 4H4는 4H3을 잘 받았다고 Supplicant가 Authenticator에게 보내주는 응답으로, 생략하여도 상호인증과 PTK 생성에는 문제가 없다. 단, 2.1의 그림 4와 같이 Authenticator가 4H3을 보낸 후 응답을 받지 못하면, 4H3을 몇 차례 재전송하므로 4H3의 timeout 주기가 끝날 때까지 데이터를 보낼 수 없다. 3-Way 핸드쉐이크 방식은 4H4 과정에서 MIC_{PTK} 값을 만들고, 검증하는데 걸리는 시간보다 재전송하는 편이 낫다고 제안하였다. 그러나, 4H1의 ANonce가 보안 기법을 적용하지 않는 형태이므로 2.2와 같은 공격이 발생한다.

한 개의 난수와 2개의 카운터[7]를 이용하여 2-Way 핸드쉐이크하는 방식은, Authenticator가 난수 ANonce를 생성하고, SNonce 대신에 함수 f()를 통하여 f(ANonce)를 사용한다. 그러므로 Authenticator는 2H1을 보내기 이전에 PTK의 생성이 가능하다. 이 방식은 재생공격을 방지하기 위하여 2개의 카운터 BC(Boot Counter)와 TC(Time Counter)를 2H1에 삽입한다. 즉, Authenticator 인척 하는 공격자는 같은 ANonce값을 가지고 2H1을 재생할 수 있으므로 카운터 값이 꼭 필요하다. 그러나 이 방식은, 카운터 값의 동기화가 어렵다는 단점을 갖고 있다.

Enhanced 2-Way 핸드쉐이크 방식[8]은 기존의 4-Way 핸드쉐이크 방식에서 Authenticator와 Supplicant가 각각 1개의 난수를 생성하는 것에 비하여, Authenticator가 ANonce와 함께 큰 난수 RNonce를 생성한다. 그림 8과 같이 Authenticator는 자신이 생성한 난수 ANonce와 큰 난수 RNonce, 자신의 MAC 주소와 같은 식별자 AP를 PMK로 암호화 한 2H1을 Supplicant에게 보낸다. Supplicant는 PMK를 알고 있으므로 2H1을 복호화 하여 자신이 생성한 SNonce와 Authenticator에게서 받은 RNonce를 PMK로 암호화하여 다시 보낸다. 또한, 자신이 생성한 난수 SNonce로 2.1의 식 (1)에 의하여 PTK를 생성하고 설치한다. Authenticator는 자신이 이전에 보낸 RNonce가 맞는지 확인하여 맞으면 PTK를 설치한다. 이 방식은 2-Way 핸드쉐이크의 두 개의 메시가 모두 PMK에 의해서 암호화 되므로 DoS 공격이 방지된다. 또한, 두 개의 메시지 모두 난수 값을 전송하므로 재생 공격을 방지할 수 있다. 그러나, 이 방식은 RNonce를 위한 저장 공간이 요구된다.

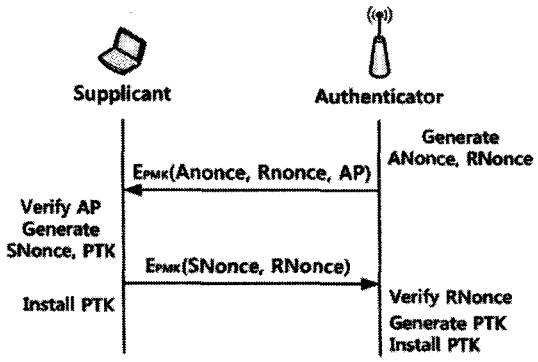

그림 8. Enhanced 2-Way 핸드쉐이크

3. 2-Way 핸드쉐이크 프로토콜을 이용한 PTK의 생성

4-Way 핸드쉐이크는 Supplicant와 Authenticator 사이의 상호 인증과, 안전한 데이터의 전송을 위하여 세션키 PTK를 도출하는 과정이다. 그러나, 2장의 내용과 같이 4-Way 핸드쉐이크는 보안상 취약점을 갖고 있어, DoS 공격이나 재생 공격이 발생한다. 2.2에서는 4-Way 핸드쉐이크와 같은 역할을 하는 대체 기법들을 소개하였다. 그러나, 2.2의 방식들은 전송되는 메시지의 개수를 줄여 고속의 핸드오프는 가능하나, 보안상의 취약점이 남아있거나, 취약점을 해결하기 위한 추가적인 저장이 필요함을 알 수 있다. 본 논문에서는 고속의 핸드오프 과정을 위하여, IEEE 802.11 (Re)Association 메시지와 결합한 2-Way 핸드쉐이크를 제안하여 메시지의 개수를 줄이고, PTK 계산에서 난수 대신에 순번을 사용하여 2.1장에서 설명한 4-Way 핸드쉐이크의 보안상의 취약점을 개선하여 고속의 안전한 핸드오프 방식을 제안한다.

3.1 순번에 기반 한 2-Way 핸드쉐이크 프로토콜 제안

MS가 새로운 AP로 로밍 할 때, PMK, PMKID로 구성된 새로운 PMKSA와 Lifetime이 MS의 802.1x Supplicant와 새로운 AP의 802.1x Authenticator에 생성되어 있다. 본 논문에서는 Supplicant와 Authenticator의 PMKSA안에 각각 0으로 초기화 된, SN_{MS}, SM_{AP}의 추가적인 생성을 제안한다.

MS가 새로운 AP로 로밍을 하고, Re-association 하기로 결정 했을 때, 본 논문에서 제안하고 있는 순번을 추가한 Re-association 과정은 그림 9와 같다. Supplicant는 SN_{MS}를 1 증가시키고, 식 (3)에 의하여

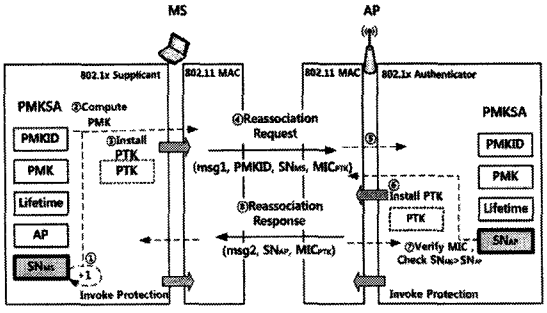

그림 9. 순번을 추가한 Re-association 과정

PTK를 계산하고, 순번 SN_{MS}와 함께 PTK를 IEEE 802.11 MAC에 설치한다. 기존의 PTK 생성 계산식은 식 (1)과 같으나, 본 논문에서 제안하고 있는 방식은 재생 공격을 방지하기 위하여, ANonce, SNonce 대신에 SN_{MS}를 사용한다.

$$PTK = prf(PMK, SN_{MS}\ AP, MS) \quad \text{식 (3)}$$

MS의 802.11 MAC은 AP의 802.11 MAC에게 (msg1, PMKID, SN_{MS}, MIC_{PTK})로 구성된 RR 프레임을 전송한다. 이때, msg1은 SSID(Service Set Identifier), Listen Interval, 현재 연결되어 있는 AP의 MAC 주소와 같은 파라미터의 리스트를 나타낸다. RR 프레임은 MIC_{PTK}에 의해서 보호된다.

RR 프레임을 수신한 AP의 802.11 MAC은 수신한 RR에 있는 PMKID에 기반 한 PMKSA를 찾기 위하여 Authenticator에게 MS, PMKID, SN_{MS}를 전달한다. RR 프레임의 처리 방법은 그림 10과 같다. Authenticator는 PTK를 계산하고, AP의 802.11 MAC에 설치한다. PTK를 이용하여 MIC 값을 검증하고, 검증이 실패하면 RR 프레임은 버려지고, 성공하면 SN_{MS}이 SN_{AP}보다 큰 값인지 체크한다. SN_{MS}는 RR 프레임을 보내기 전에 1이 증가되므로, RR 프레임이 최근의 것이거나, 정당한 MS에게서 온 것이라면, SN_{MS}는 SN_{AP}보다 크다. 위와 같은 순번 확인을 보안조건이라 한다. $SN_{MS} > SN_{AP}$이면, (msg2, MS_{AP}, MIC_{PTK})로 구성된 RP를 MS의 802.11 MAC으로 보낸다. 이때, msg2는 AID(Association ID)와 Status Code의 파라미터 리스트를 나타낸다. RR 프레임이 Authenticator에게 전송되고, MIC 값이 성공

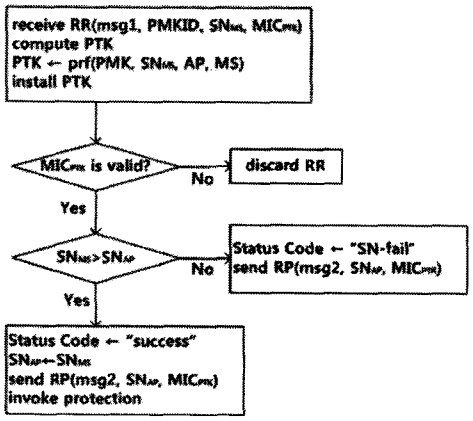

그림 10. Re-association Request 처리 순서도

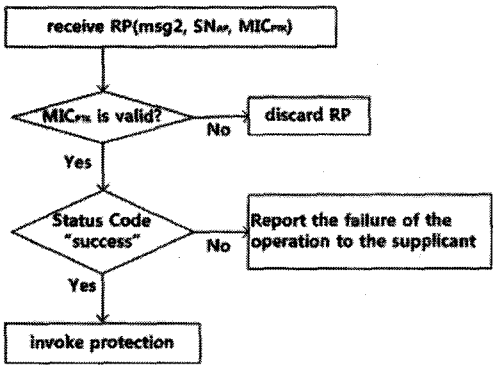

그림 11. Re-association Response 처리 순서도

적으로 검증되고, 보안 조건까지 만족하면, Status Code는 "success"으로 세팅한다. RP 프레임 또한, MIC_{PTK}로 보호된다. $SN_{MS} \leq SN_{AP}$이면, RR 프레임은 재생된 프레임으로 간주되고, Status Code는 "SN-fail"로 세팅된다.

Status Code 코드가 "success"로 세팅된 RP 프레임을 전송한 후에, AP의 802.11 MAC는 SN_{AP}와 SN_{MS}사이에 동기화가 되도록, 즉 SN_{AP}값이 SN_{MS}가 되도록 Authenticator에게 지시한다. 마지막으로, Authenticator는 암호화된 Data 프레임들을 처리하기 위하여 AP의 802.11 MAC의 보호 기능을 실시한다.

그림 11과 같이, RP 프레임을 수신하면, MS의 802.11 MAC은 먼저 MIC 값을 검증한다. 검증이 성공적이지 않으면, RP를 버린다. MIC 검증이, 성공적이면 msg2의 Status Code의 값이 "success"인지 확인한다. "success"가 아니면, Supplicant에게 Re-association의 실패를 알린다. "success"이면, MS의 802.11 MAC은 RP 프레임의 성공적인 수신을 Supplicant에게 알리고, Supplicant는 MS의 802.11 MAC의 보호 기능을 실시한다.

3.2 현재 AP와의 초기 Association과 Re-association

MS가 AP를 통해서 네트워크에 처음 접속할 때, 그림 1과 같이, Association, IEEE 802.11x EAP-TLS 인증, 4-Way 핸드쉐이크 순으로 진행된다. 이때, 4-Way 핸드쉐이크는 PMK 기반이기 때문에, 반드시 성공적인 IEEE 802.1x EAP-TLS 인증 이후에 실행되어야한다. 그러므로, Association 단계

와 4-Way 핸드쉐이크 단계를 하나의 Association 단계나 Re-association 단계로 결합할 수 없다. 802.1x 인증은 AP에서 802.1x uncontrolled port를 통해서 이뤄지고, 성공적인 Association 후에 MS에게 할당되기 때문에, AP와의 Association은 IEEE 802.1x EAP-TLS 인증 이후에 실행되어야 한다. 결과적으로, 본 논문에서 제안하고 있는 Re-association 과정은, Association과 802.1x 인증 후에 4-Way 핸드쉐이크 대신에 수행 되어야만 한다. 이런 경우, 같은 AP에게로의 Re-association의 목적은 상호인증과, 키 확인을 위한 PTK의 도출이다. IEEE 802.11에서, MS가 같은 AP와의 Association을 유지하고 있는 동안, Re-association은 현재 설정되어있는 Association의 Association 상태를 변경시키는 역할을 한다.

4. 제안 방식의 분석과 기존 방식과의 비교

4.1 순번의 보안 조건

본 논문에서 제안하고 있는 2-Way 핸드쉐이크의 순번의 역할은, 재생 공격을 방어하기 위하여, 각 Re-association 세션마다 새로운 PTK를 생성하는 것이다. MS와 AP에 대해서 동일한 PMKSA들이 생성될 때, 두 개의 순번 SN_{MS}와 SN_{AP}는 초기값이 0으로 같다. 결과적으로, 현재 또는 새로운 AP와 Re-association 할 때마다, MS는 SN_{MS}를 1씩 증가시킨다. 또한, Re-association이 성공하면, AP는 SN_{AP}를 SN_{MS}-SN_{AP}만큼 증가 시킨다. RR 프레임이 AP로 전송될 때, 성공적인 Rssociation에 대한 순번의 보안 조건은 $SN_{MS} > SN_{AP}$이다. 일반적인 조건에서는 SN_{MS}-SN_{AP}=1이고, $SN_{MS} - SN_{AP} > 1$ 인 경우는 그림 12와 같이 두 가지 경우이다. RR_i와 RP_i은 각각, Re-association Request와 Re-association Response 프레임을 의미하고, i = 1, 2, 3, ..., 값으로 각 프레임과 결합되는 프레임의 순번을 의미한다.

첫째, 그림 12의 Session A의 경우이다. t_1시간에 AP로 RR_i를 보낼 때, MS는 AP와 새로운 세션을 시작한다. 이때, RR_i가 FCS(Frame Check Sequence) 에러와 같은 이유로, 성공적으로 AP에 도달하지 못했다면, ReassociateFailureTimeout 이 만기된 후에, RR_{i+1}은 보내질 것이다. ReassociateFailureTimeout은 IEEE 802.11에서 Re-association 절차가 끝난 후

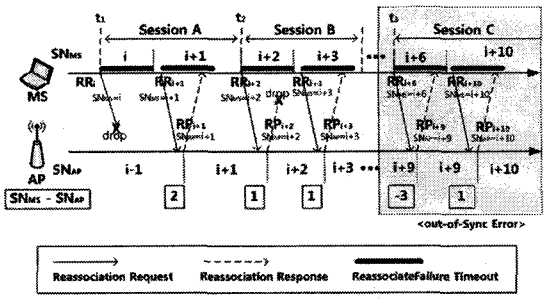

그림 12. 순번의 보안 조건

시간 제한선을 명시하는 값이라고, 정의 되어 있다. AP가 RR_{i+1}을 받으면, RR_{i+1}에 있는 MIC를 검증하고, 보안 조건을 체크한다. RR_{i+1}의 SN_{MS}가 i+1이고, AP에 저장되어 있는 SN_{AP}가 i-1이다. 이런 경우, SN_{MS}-SN_{AP}>1이기 때문에 SN_{MS}과 SN_{AP}에 대한 보안 조건은 만족된다. 그때, SN_{MS}-SN_{AP} 만큼 SN_{AP}를 증가시키고, RP_{i+1}은 MS에게로 돌아오게 될 것이다.

둘째, 그림 12의 Session B의 경우이다. t_2시간에 AP로 보낸 RR_{i+2}이, AP에서 MIC 검증이 성공하고, $SN_{MS}(=i+2) > SN_{AP}(=i+1)$이 순번 보안 조건에 만족하여 성공적으로 처리되었다. SN_{MS}-SN_{AP}만큼 SN_{AP}를 증가시키고, RR_{i+2}에 대응하는 RP_{i+2}를 MS로 보낸다. 그러나, RP_{i+2}가 FCS 에러와 같은 이유로 MS에 정상적으로 도착하지 않았다고 가정하자. 이때, ReassociateFailureTiomout이 만기된 후에, RR_{i+3}은 AP에게 보내지고, $SN_{MS}(=i+3) > SN_{AP}(=i+2)$의 보안 조건 또한 만족한다.

4.2 Out-fo-Sync 에러에 대한 복구

SN_{MS}와 SN_{AP}가 보안 조건에 만족하지 않을 때, SN_{MS}와 SN_{AP}는 out-of-sync라고 정의하자. 어떠한 경우에도, RR_{j1}(j1는 SN_{MS}을 의미)에서 SN_{MS}가 AP에 저장된 SN_{AP}보다 작거나 같으면, AP는 MS에게 알려야한다. 먼저, msg2의 Status Code가 "SN-fail"로 세팅되고, 이것은 SN_{MS}와 SN_{AP}가 out-of-sync임을 의미한다. (msg2, SN_{AP}, MIC_{PTK})로 구성된 RP_{j2}가 MS로 보내어 지고, PTK는 SN_{MS}를 기반으로 계산된다. 여기서 J2= SN_{AP}이다. MS는 $SN_{MS} \leq SN_{AP}$이므로 out-of-sync가 발생한 것을 알게 되고, 이런 경우 out-of-sync 에러를 복구하는 두 가지 방법이 있다. 하나는 보안 조건을 만족하게 하기 위해서, MS의 PMKSA에 있는 SN_{MS}를 SN_{AP}-SN_{MS}+1만큼 증

가시키는 것이다. 예를 들어 그림 12의 out-of-sync와 같이, (i+9)-(i+6)+1(=4) 만큼 SN_{MS}를 증가시키는 것이다. 다른 하나의 방법은 MS와 AP에서 0으로 초기화 된 순번을 갖는 새로운 PMK를 만들기 위해서 MS와 AS사이의 IEEE802.1x EAP-TLS 인증을 초기화 하는 것이다.

4.3 PTK 설치와 보호 실행

IEEE 802.11에서는 Data, Control, Management의 3가지 프레임이 존재한다. 4-Way 핸드쉐이크는 Data 프레임에 캡슐화 되어있다 Re-association Request와 Re-association Response 프레임은 Management 프레임의 일부이다. 암호화가 적용될 수 있는 프레임은 단지 Data 프레임이다. 4-Way 핸드쉐이크의 경우, 핸드쉐이크 프로토콜 동안 도출되는 PTK의 사용은 두가지 경우이다. 첫째, 4H2, 4H3, 4H4를 MIC를 이용하여 무결성을 보장할 때, PTK를 이용하여 MIC_{PTK}를 이용한다. 두 번째, 데이터 세션동안 안전한 데이터의 전송을 위하여, 데이터 프레임을 암호화하는 경우이다. 핸드쉐이크가 끝난 후에, IEEE 802.11 MAC의 암호화 기능을 실행하는 방법이 있어야만 한다. 4H4가 Authenticator에 의해서 성공적으로 처리되기 전에 암호화 기능이 실시된다면, PTK 값이 도출되지 않았으므로, 4-Way 핸드쉐이크는 실패한다. 반면에 2-Way 핸드쉐이크에서는 Re-association과 같은 Management 프레임은 결코 암호화되지 않기 때문에, IEEE 802.11 MAC은 암호화 기능이 미리 실시되어도, 암호화/복호화를 시도하지 않는다.

4.4 Management 프레임의 보호

Re-association 과정에서 삽입되는 PTK 도출의 장점은 RR과 RP 프레임은 보호될 수 있다는 것이다. 그러므로, RR과 RP 프레임은 PTK가 알려지지 않으면 공격자에 의해서 위조되지 않는다. 원래의 IEEE 802.11 프로토콜에서, Management 프레임은 어떠한 보안 기법에 의해서도 전체적으로는 보호되지 않는다. 즉, 공격자들은 Management 프레임들을 위조할 수 있고, De-authentication과 Disassociation 하도록 하는 DoS 공격을 유발할 수 있다. 그러나, IEEE 802.11w[9]이 Management 프레임에게 보안을 제공한다.

4.5 4-Way 핸드쉐이크와 같은 역할을 하는 기법들과의 비교

4-Way 핸드쉐이크에 의해서 제공되는 보안 속성들은, 2.3의 관련 연구들과, 제안하고 있는 2-Way 핸드쉐이크에 의해서도 제공된다. RR과 RP 프레임에 있는, PTK 계산에 기반 한 두 개의 MIC_{PTK}는 검증된다. 성공적인 검증은 MS와 AP 모두 동일한 PTK를 가지고 있음을 나타내고, 동일한 PMK을 공유하고 있음을 의미한다. PMK는 MS와 AP사이에서만 공유되기 때문에 상호인증 또한 수행한다. 4-Way 핸드쉐이크와 3-Way 핸드쉐이크의 기본적인 취약점은 4H1메시지가 전체적으로 보호되지 않고 있어, DoS 공격이 발생할 수 있다. EAP-TLS 인증을 변형한 방법 역시, 선행 인증 단계에서 전송되는 EAP-TLS(SNonce) 메시지의 SNonce값이 평문으로 전송되기 때문에 DoS 공격과 재생 공격이 가능하다. 그러나, 제안된 RR과 RP 프레임 모두 PTK에 의해서 보호되기 때문에, DoS 공격은 제안된 2-Way 핸드쉐이크에서는 발생하지 않는다.

두 개의 구별되는 난수는 PTK 도출을 위해서 사용되기 때문에, 독립적인 두 개의 메시지 4H1과 4H2는 MS와 AP 사이에서 교환된다. 그러나, 2-Way 핸드쉐이크에서, 느슨하게 동기화된(loosely synchronized) 순번들은 새로운 PTK를 도출하는데 사용되고, 2-Way 핸드쉐이크는 Re-association 과정에 삽입된다. 그러므로, MS와 AP 사이에 교환되는 메시지의 개수는 훨씬 감소한다. MS가 새로운 AP와 Re-association 하기 위해서, 4-Way 핸드쉐이크는 6개의 메시지가 필요하고, 3-Way 핸드쉐이크는 5개의 메시지, EAP-TLS 인증을 변형 방식과 2개의 카운터를 이용한 방식, Enhanced 2-Way 핸드쉐이크 방식은 4개가 필요하다. 제안하고 있는 2-Way 핸드쉐이크는 Re-association에 대한 2개의 메시지만 필요하다.

PTK 계산과 확인은, 제안되는 2-Way 핸드쉐이크에서 IEEE 802.11 MAC에 의해서 실행되는 동안, 4-Way 핸드쉐이크를 비롯한 4개의 기법 역시, Supplicant와 Authenticator에 실행된다.

위에서 설명한, 2장의 기법들과 본 논문에서 제안하고 있는 2-Way 핸드쉐이크 방식을 비교를 정리하면 표 1과 같다.

표 1. 제안된 2-Way 핸드쉐이크 방식과 다른 방식들과의 비교

	4-Way	EAP-TLS 변형	3-Way	2-Counter	Enhanced 2-Way	제안 방식
PTK 도출 상호인증	○ ○	○ ○	○ ○	○ ○	○ ○	○ ○
DoS 공격 방지	×	×	×	○	○	○
Re-authentication과 PTK 도출 관련 메시지 개수	6 개	4개	5개	4개	4개	2개
MIC 계산과 확인	Supplicant / Authentic-ator	Supplicant / Authentic-ator	Supplicant / Authentic-ator	Supplicant / Authentic-ator	Supplicant / Authentic-ator	IEEE 802.11 MAC
Nonce	난수	난수	난수	난수, 카운터	난수	순번

5. 결 론

802.11i에서는 MS와 AP 사이의 상호인증과, 안전한 데이터 전송을 위한 세션키 PTK 생성을 위한 4-Way 핸드쉐이크에 대한 안전성(security)과 신뢰성(reliability)에 관한 연구가 진행되고 있다. 2.1과 같이 4-Way 핸드쉐이크는 보안의 취약성으로 인하여 DoS 공격이 발생함을 알 수 있었다. 4-Way 핸드쉐이크를 대신하는 기법들이 제안되고 있으나, 메시지의 개수를 줄여 고속의 핸드오프는 가능하나, 안전성이 부족하거나, 안전성을 위해서는 추가 저장이 필요함을 알 수 있었다. 본 논문의 제안 기법에서는 2장의 기법들의 단점을 보완하기 위하여 메시지의 개수를 줄여 빠르고, 순번을 이용하여 공격을 방지하는 고속의 안전한 핸드오프 기법을 제안하였다.

참 고 논 문

[1] IEEE 802.11, Wireless LAN Medium Access Control(MAC) and Physical Layer(PHY) specifications, IEEE Standard, 2007.

[2] IEEE 802.11i, Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications : Medium Access Control(MAC) Security Enhancements, IEEE Standard, 2004

[3] Arunesh Mishra, Min-ho Shin and William A. Arbaugh, "Pro-active Key Distribution using Neighbor Graphs," IEEE Wireless Communications, vol. 11, 2004.

[4] C. He and C. Mitchell, "Analysis of the 802.11i 4-way Handshake," Proceedings of the ACM Workshop on Wireless Security, pp. 43-50, 2004.

[5] Changhua He, John C. Mitchell. "Security analysis and improvements for IEEE 802.11i," The 12th Annual Network and Distributed System Security Symposium (NDSS'05), pp. 90-110, 2005.

[6] Junbeom Hur, Chanil Park, Young-joo Shin and Hyunsoo Yoon, "An Efficient Proactive Key Distribution Scheme for Fast Handoff in IEEE 802.11 Wireless Networks," ICOIN 2007: pp. 629-638, 2007.

[7] Manivannan N, Neelameham P. "Alternative Pair-wise Key Exchange Protocols(IEEE 802.11i) in Wireless LANs," in Proc, of International Conference on Wireless and Mobile Communications(ICWMC'06), pp. 52-58, 2006.

[8] Jing Liu, Xinming Ye, Jun Zhang and Jun Li "Security Verification of 802.11i 4-Way Handshake Protocol," Communications, 2008. ICC '08. IEEE International Conference on, pp. 1642-1647, 2008.

[9] IEEE 802.11w, Draft Standard, Wireless LAN Medium Access Control(MAC) and Physical Layer (PHY) specifications Amendment 4: Protected Management Frames, IEEE Standard, 2008.

임 정 미

2000년 단국대학교 전자계산학과 졸업 학사
2002년 단국대학교 전자계산학과 석사
2006년 단국대학교 전자계산학과 박사
2004년~현재 단국대학교 교양학부 강의전임

관심분야 : 정보보호, 네트워크 보안