DOI: 10.3745/KIPSTC.2009.16-C.3.317

IEEE 802.11i 4-way 핸드쉐이크 프로토콜의 안전성과 신뢰성

박 창 섭[†] · 우 병 덕[††]

요 약

본 논문은 IEEE 802.11i의 4-way 핸드쉐이크 프로토콜을 안전성과 신뢰성의 측면에서 분석한다. 분석을 통해 MIC 오류와 같은 특정한 상황에서 4-way 핸드쉐이크가 정상적으로 수행되지 못하는 것을 보여주고 문제 해결을 위한 수정방안을 제안한다. 또한 4-way 핸드쉐이크 프로토콜보다 안전하고 효율적인 2-way 핸드쉐이크 프로토콜을 제안한다.

키워드 : 무선랜, 핸드오프

Security and Reliability of the 4-way Handshake Protocol in IEEE 802.11i

Chang-Seop Park[†] · Byung-Duk Woo[††]

ABSTRACT

In this paper, a 4-way Handshake protocol in the IEEE 802.11i is analyzed in terms of both security and reliability. It is shown that the 4-way Handshake protocol breaks down under some conditions due to a MIC (message integrity code) failure, and a solution to fix it is proposed. It is also proposed that a new 2-way Handshake protocol which is more secure and efficient than the 4-way Handshake protocol.

Keywords : IEEE 802.11i, WLAN, Handoff, 4-way Handshake

1. 서 론

IEEE 802.11[1]에 기반을 두는 무선랜은 표준화 이후 10년 동안 안전성과 속도의 측면에서 비약적인 발전을 가져왔다. 특히 무선랜의 보안 관련 문제들을 해결하기 위해 TKIP, CCMP와 같은 강화된 암호 알고리즘과 AKM (Authentication and Key Management) 프로토콜을 새로운 보안 아키텍처인 802.11i[2]의 "RSN(Robust Security Network)"을 통해 소개하였다. 최근 들어 무선랜 환경에서 VoIP (Voice over Internet Protocol)나 MoIP(Multimedia over internet protocol)와 같은 실시간 멀티미디어 서비스 이용에 대한 사용자의 관심이 증가하는 가운데 802.11을 기반으로 하는 무선랜에서 안전하고 빠른 핸드오프 메커니즘은 중요한 문제로 부각되고 있다. MS(Mobile Station)의 이동 시 끊김 없는 서비스를 제공하기 위해 핸드오프 지연시간은 최소화 되어야 한다. 802.11 표준에서는 고속의 핸드오프를 지원하기 위해 802.11f[3]와 802.11i를 통해 고속 핸드오프 메커니즘을 규정하고 있지만 이것은 무선랜에서 VoIP나 MoIP와 같은 실시간 멀티미디어 서비스를 지원하기에는 아직 수정되고 보완되어야 할 부분이 많다. 802.11r[4]에서는 QoS (Quality of Service)에 대한 요구들을 만족 시키는 안전하고 빠른 핸드오프 과정을 표준화 하고 있다.

본 논문은 MS(Mobile Station)와 AP(Access Point)사이의 상호인증 및 세션키 도출을 위해 802.11i에서 제안한 4-way 핸드쉐이크 프로토콜에 대해 분석한다. MS가 AP에 최초 접속을 시도 할 때 또는 MS가 새로운 AP 영역으로 로밍 할 때 4-way 핸드쉐이크 프로토콜은 수행 된다. 그런데 최근 들어 4-way 핸드쉐이크 프로토콜의 불안 요소들이 발견 되고 있고 그것에 대한 한 가지 예가 DoS(Denial-Of Service) 공격에 노출되어 있다는 것이다. 또한 우리는 4-way 핸드쉐이크 프로토콜의 분석을 통해 MIC(Message Integrity Check) 오류로 인해 4-way 핸드쉐이크 프로토콜의 과정이 비정상적으로 종료 될 수 있음을 보인다. 이러한

※ 본 연구는 2008학년도 단국대학교 대학연구비의 지원으로 연구되었음
† 정 회 원 : 단국대학교 전자컴퓨터학부 교수
†† 준 회 원 : 단국대학교 전자계산학 석사과정
논문접수 : 2008년 12월 2일
수 정 일 : 1차 2009년 1월 13일, 2차 2009년 2월 10일
심사완료 : 2009년 2월 18일

문제점들을 해결하기 위해 본 논문에서는 4-way 핸드쉐이크 프로토콜보다 안전하고 효율적인 2-way 핸드쉐이크 프로토콜을 제안한다.

본 논문은 다음과 같은 순서로 진행된다. 2장에서 4-way 핸드쉐이크의 보안상 문제점을 소개한다. 3장에서는 특정 상황에서 4-way 핸드쉐이크 프로토콜이 비정상적으로 동작할 수 있음을 분석 한 후 문제 해결 방안을 제안한다. 4장을 통해 4-way 핸드쉐이크 프로토콜을 대체할 2-way 핸드쉐이크 프로토콜을 소개한다. 마지막으로 5장에서 결론을 맺을 것이다.

2. 4-way 핸드쉐이크 프로토콜의 보안 취약점

네트워크를 이용하려는 MS는 적절한 AP를 찾기 위해 영역내의 모든 채널을 검사한다. 모든 채널을 검사한 후 사용가능한 AP를 선택하여 접속하고 네트워크 사용 허가를 받기 위해 인증 작업을 진행 한다. MS와 AP 사이에는 안전한 채널이 존재하지 않기 때문에 MS와 AP 사이의 상호인증은 AS(Authentication Server)를 통해 간접적으로 수행된다. 이때 AP와 AS 그리고 AS와 MS 사이에는 이미 안전한 채널이 존재한다는 것을 가정하고 수행된다.

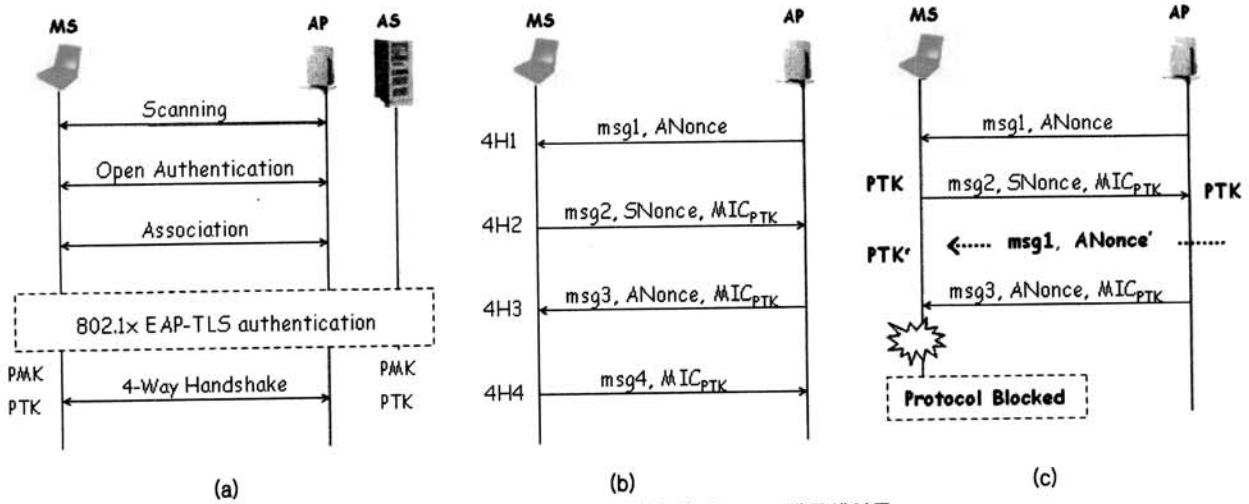
상호인증을 위해 MS는 AS와 802.1x[5] 기반의 EAP-TLS 인증 작업을 수행하여 상호간의 공통 키 PMK(Pairwise Master Key)를 생성한다. 그 후 AS는 안전한 채널을 통해 AP에게 PMK를 전달한다. AP가 PMK를 전달 받으면 PMK를 기반으로 4-way 핸드쉐이크 프로토콜을 진행하여 세션키 PTK(Pairwise Transient Key)를 도출하고 MS와 AP 사이의 상호인증 작업을 진행 한다. MS와 AP 사이의 상호인증 및 세션키 도출 과정을 진행하기 전에 결합(Association) 요청/응답 메시지를 먼저 교환하여 AP에 MS를 등록한다. 802.11i에서는 IEEE 802.11의 이전 표준과의 호환성을 유지하기 위해 개방형 인증(Open Authentication)을 허용하고 있다. 그러나 여기서 개방형 인증은 큰 의미가 없다.

(그림 1)의 4-way 핸드쉐이크 프로토콜은 MS와 AP가 서로 동일한 PMK를 가지고 있음을 검증하고 이들 사이에 교환되게 될 데이터 프레임을 보호하기 위한 세션키 PTK를 생성하는 것을 보여 주고 있다. PTK는 다음과 같이 계산된다.

$$PTK = prf(PMK, SNonce, ANonce, AP, MS)$$

여기서 prf는 키 생성 함수이고 ANonce와 SNonce는 AP와 MS로부터 각각 선택된 난수 값이다. MS와 AP는 각각의 802.11 MAC 주소로 표시된다. MIC_{PTK}는 전송되는 모든 필드의 값을 PTK를 사용하여 계산한 MIC(Message Integrity Code) 값을 나타낸다. 예를 들어 메시지에 field1과 field2 그리고 MIC_{PTK}가 포함되어 있다면 이 메시지에 포함된 MIC_{PTK}는 field1과 field2 그리고 PTK를 이용하여 계산된다. 4-way 핸드쉐이크에 대한 안전성 분석을 위해 EAPOL-Key 프레임에 존재하는 여러 필드들 중 4-way 핸드쉐이크에 대해 설명하기 위한 필수 필드를 제외한 나머지 필드에 대해서는 고려하지 않는다. 그래서 우리는 msg1, msg2, msg3, msg4와 같이 불필요한 필드를 제외한 표기법을 사용하여 4-way 핸드쉐이크 진행을 설명한다.

4-way 핸드쉐이크 프로토콜은 다음과 같이 진행된다. AP가 먼저 MS로 ANonce와 msg1을 생성하여 보내면 MS는 SNonce를 생성한 후 PTK를 계산한다. MS는 PTK 계산 후 4H2 메시지를 보호하기 위해 MIC_{PTK}를 포함한 4H2 메시지를 AP로 전달한다. 4H2 메시지를 통해 SNonce를 획득한 AP는 PTK를 계산할 수 있고 계산된 PTK를 이용하여 MIC_{PTK}를 검증 할 수 있다. 검증 작업이 성공적으로 끝나면 AP는 MS와 동일한 PMK를 가지고 있음을 확인 할 수 있다. 4H3에 있는 MIC_{PTK}의 성공적인 확인을 통해 MS 또한 AP와 동일한 PTK를 가지고 있음을 확인할 수 있다. 이를 통해 궁극적으로, MS와 AP 사이의 상호간 인증이 정상적으로 수행되었음을 증명할 수 있다. 4H4 메시지는 MS가 AP로 부터 전송받는 데이터 프레임을 PTK를 이용하여 정상적으로 처리할 준비가 되었음을 의미한다.



(그림 1) MS와 AP간의 결합 및 4-way 핸드쉐이크

선행된 연구결과처럼 4-way 핸드쉐이크 프로토콜은 DoS 공격 [6-8]에 노출된다. 4-way 핸드쉐이크 프로토콜에서 암호화에 의해 보호받지 못하는 4H1 메시지가 가장 기본적인 취약점이다. 이를 이용하여 공격자는 상이한 ANonce' 를 포함하고 있는 위조된 4H1 메시지를 MS에게 보낼 수 있다. 공격자로부터 전달된 위조된 4H1 메시지를 받은 MS는 아래의 식처럼 새로운 PTK'을 계산한다.

$$PTK' = prf(\ PMK,\ SNonce,\ ANonce',\ AP,\ MS)$$

이것은 MS와 AP사이의 PTK 동기화가 깨졌다는 것을 의미한다. (그림 1)-(c)에서 보이는 것과 같이 PTK에 의해 계산된 MIC를 포함한 4H3 메시지는 MS측에 의해 단순히 폐기 되며 수차례에 걸친 4H3 메시지 재전송 후 4-way 핸드쉐이크 프로토콜이 완료 되지 못하고 중단된다.

3. 4-way 핸드쉐이크 프로토콜의 신뢰성 문제

3.1 4-way 핸드쉐이크 프로토콜의 FCS 오류 및 MIC 오류

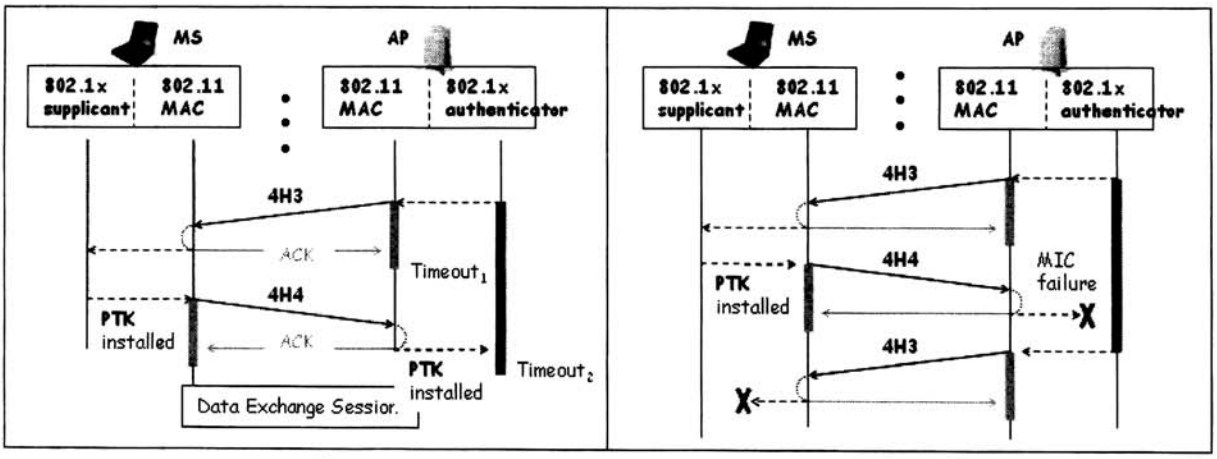
4-way 핸드쉐이크 프로토콜을 구성하는 메시지를 처리하는 과정에서 FCS(Frame Check Sequence) 오류와 MIC (Message Integrity Code) 오류가 발생할 수 있다. MIC 오류는 해당 메시지에 대한 인증이 실패하였음을 의미한다. 또한 MS나 AP측의 처리과정에서 내부적인 오류로 인해 MIC 오류가 발생 할 수 있다. 우리는 지금부터 4-way 핸드쉐이크 프로토콜의 마지막 두 메시지인 4H3, 4H4 메시지에 관심을 두고 살펴볼 것이다. 4H4 메시지는 암호학적인 측면에서의 역할은 없고 단지 MS가 4H3 메시지를 정상적으로 수신했다는 응답 메시지로서의 역할을 수행한다. 즉, 4H4 메시지는 MS가 정상적으로 PTK를 설치하였고 이제 암호화된 데이터 프레임을 보낼 수도 있고 받을 수도 있다는 것을 AP에게 알리는 목적으로 사용된다. 핸드쉐이크 프로토콜을 신뢰성 관점에서 분석하기 위해 우리는 AP를 IEEE 802.1x Authenticator와 802.11 MAC으로 분리하고, MS 또한 802.1x Supplicant와 802.11 MAC으로 분리하여 다룬다. 지금부터 프레임이라는 용어는 메시지와 혼용해서 사용된다.

4-way 핸드쉐이크 프로토콜의 메시지는 IEEE 802.1x EAPOL-Key 프레임을 통해 전송된다. EAPOL-Key 프레임은 802.11의 3가지 종류의 프레임 형태 중 하나인 데이터 프레임 안에 캡슐화 된다. 데이터 프레임은 ACK 프레임을 동반 한다. ACK 프레임은 데이터 프레임 수신측에서 송신측으로 보내는 메시지로써 전달 받은 데이터 프레임이 FCS 오류 없이 성공적으로 전달되었다는 의미를 내포하고 있다. 802.11의 기본적인 흐름제어 및 에러제어는 정지-대기 (stop-and-wait) 프로토콜을 사용한다. 4H3 (또는 4H4) 프레임은 전송과정에서 분실될 수 있으며 또한 FCS 오류가 발생할 경우 폐기되어진다. 만약 $Timeout_1$ 동안 ACK 프레임이 도착하지 않으면 4H3 (또는 4H4) 프레임은 재전송 된다. Supplicant와 Authenticator 사이에 전달되는 EAPOL-Key 프레임의 확실한 전송을 위해 사용되는 규칙인 $Timeout_1$에 관한 동작은 IEEE 802.11 MAC에 의해 다루어진다. (그림 2)-(a)에서처럼 4H3 메시지는 Supplicant가 받아서 처리한다. 만약 4H3 메시지의 MIC값이 정상적이라면 Supplicant는 PTK를 설치하고 Authenticator에게 4H4 메시지를 전송한다. 이때 4H4 메시지가 FCS 오류나 MIC 오류 없이 Authenticator에게 전달되었다면 Authenticator 또한 PTK를 설치한다.

3.2 MIC 오류에 의한 4-way 핸드쉐이크 프로토콜의 오작동

(그림 2)-(b)에서와 같이 4H4 프레임이 802.11 MAC AP에게 FCS 오류 없이 전달되지만, 4H4 프레임에 MIC 오류가 발생 되었다고 가정해 보자. 위와 같은 상황이 발생하면 802.11 표준에 따르면 4H4 프레임은 단순히 폐기되어지고 $Timeout_2$가 지난 이후에 4H3 프레임이 재전송 된다.

$Timeout_2$는 802.11 MLME(MAC Layer Management Entity) 안에 있는 MIB(Management Information Base) 속



(a) (b)

(그림 2) 4-way 핸드쉐이크 프로토콜의 신뢰성

성 중 "dot11RSNAConfigPairwiseUpdateTimeOut"에 미리 설정되어 있는 값이다. 4H3 프레임의 재전송 동작은 유효한 MIC 값을 가진 4H4 프레임이 전달 될 때 또는 MIB 속성 중 "dot11RSNAConfigPairwiseUpdateCount"에 미리 설정된 재전송 횟수를 넘을 때 까지 계속 진행 된다.

그러나 4H4 메시지의 MIC 오류를 다루는데 있어 802.11 표준은 중요한 결점을 가지고 있다. Supplicant는 4H4 메시지를 전송한 후 PTK를 설치하고 AP로부터 암호화된 데이터 프레임을 받을 것이라고 기대하고 있다. 이때 4H4 메시지가 유효하지 않은 MIC 값을 가지고 있다면 Authenticator는 해당 메시지를 무시하고 폐기할 것이다. 그 후 AP는 처음 보낸 4H3 메시지에 대한 정상적인 응답이 없는 관계로 4H3 메시지를 재전송 하는데 해당 메시지는 AP쪽에서 PTK가 설치되지 않은 관계로 암호화가 되지 않은 상태에서 MS로 전달된다. 재전송된 4H3 메시지는 암호화 되지 않고 전송되었기 때문에 MS는 해당 메시지가 유효하지 않다고 판단 한 후 폐기한다. $Timeout_2$ 이후 AP는 4H3 메시지를 재전송 하겠지만 Supplicant는 계속해서 암호화 되지 않는 4H3 메시지를 무시 할 것이고 이로 인해 4-way 핸드쉐이크 프로토콜은 비정상적으로 종료된다.

문제가 되고 있는 해당 프로토콜을 더 자세히 분석해 보기 위해 (그림 3)에 대해 알아보자. (그림 3)은 전달 받은 MPDU(MAC Protocol Data Unit) 처리에 관한 의사코드로서 IEEE 802.11 표준 Section 8.7.2.3에 명시되어 있다. 위와 같은 케이스에서 MPDU의 프레임 바디는 4-way 핸드쉐이크 메시지를 포함하고 있는 EAPOL-Key 프레임과 일치한다. (그림 3)의 ①에서 보는 것과 같이 MS와 AP가 RSN 보안 연결을 사용하기로 결정하였다면 MIB 속성 중 dot11RSNAEnabled 항목을 TRUE로 설정한다.

MS와 AP가 4-way 핸드쉐이크를 시작할 때 전달 받은 MPDU 처리를 위해 (그림 3)의 ①에서 (그림 3)의 ②로 넘어간다. 802.11 MAC 헤더의 Frame control 필드는 Protected Frame 부필드(subfield)를 포함한다. Protected Frame subfield는 MPDU가 PTK에 의해 암호화 될 경우 1로 설정한다. 4-way 핸드쉐이크 과정에 사용되는 데이터 프레임의 경우 PTK로 암호화 되지 않았기 때문에 Protected Frame 부필드는 4-way 핸드쉐이크 과정 중에는 항상 0으로 설정된다. 전달 받은 데이터 프레임의 Protected Frame 부필드가 0으로 설정 되었을 경우 해당 프레임의 처리를 위해 (그림 3)의 ②에서 (그림 3)의 ③으로 진행된다.

만약 PTK가 아직 설치되지 않은 수신자의 경우 의사코드의 "Protection for TA is off for Rx" 항목을 나타내며 수신자는 암호화 되지 않는 MPDU를 전달 받을 것으로 기대하고 있다는 의미를 가지고 있다. 그런데 다른 한편으로 "Protection for TA is on for Rx"는 이미 수신자는 PTK를 설치하였기 때문에 암호화 되지 않고 전달되는 MPDU의 경우 수신자가 정상적인 복호화를 하지 못하므로 해당 MPDU는 폐기된다는 것을 의미한다. (그림 2)-(b)가 의미하고 있는 4H3 메시지의 경우 (그림 3)의 ⑤에 해당하는 상황으로 AP가 보낸 4H3 메시지는 이미 PTK를 설치한 MS측에서 정상적으로 복호화 하지 못하므로 MS는 4H3 메시지를 무시하게 된다. 위와 같은 프로토콜의 결점을 수정하기 위해 PTK가 설치되어 있어도 4H3 메시지를 수신할 수 있게 프로토콜을 수정해야 한다.

❸ If (Protection for TA is off for Rx) or (Data frame contains EAPOL-Key frame)

여기서 우리는 일반적인 데이터 프레임과 EAPOL-Key 프레임을 캡슐화한 데이터 프레임을 구별해야 한다. MS의 802.11 MAC은 오직 MAC 헤더와 FCS만 인식할 수 있으므로 802.11 MAC 헤더에 있는 예비의 필드를 사용하여 두 가지 종류의 데이터 프레임 구별에 사용할 수 있다. 즉 MAC 헤더의 Frame control 필드 안에 있는 Type과 Subtype 두 개의 필드를 이용할 수 있다는 것이다. 데이터 프레임의 Type 필드의 값은 "10"이고 Subtype 필드는 데이터 프레임의 기능을 식별하는 데 사용된다. 현재 Subtype 값 중 "1101"은 예약되어있다. (그림 4)에서 나타내고 있는 재전송된 4H3 메시지에 대한 응답인 4H4 메시지의 의사코드는 4H4 메시지가 암호화 되지 않아야 하기 때문에 수정되어야 한다. (그림 4)의 ②는 아래와 같이 수정 되어야 한다.

❷ If (MSDU has an individual RA and Protection for RA is off for Tx) or (Protection for RA is on for Tx and MSDU contains EAPOL-Key frame)

```
        :
① If dot11RSNAEnabled = TRUE then
②    If the Protected Frame subfield of the Frame Control field is zero then
③       If Protection for TA is off for Rx
④          then Receive the unencrypted MPDU without protections
⑤          else discard the frame body without indication to LLC
        :
```

(그림 3) 수신된 MPDU 처리 의사코드

```
:
① If dot11RSNAEnabled = TRUE then
②    If MSDU has an individual RA and Protection for RA is off for Tx then
③       transmit the MSDU without protections
④          else If (MSDU has individual RA and Pairwise key exists for the MPDU's RA) or
           :
```

(그림 4) 전송될 MSDU 처리 의사코드

즉, (그림 3)의 ③과 (그림 4)의 ②를 위와 같이 수정하여 PTK가 이미 설치된 상황(Protection for RA is on for Tx)에서도 암호화 되지 않는 EAPOL-Key 프레임을 전송할 수 있어야 한다.

4. 새로운 2-way 핸드쉐이크 프로토콜의 제안

4-way 핸드쉐이크 프로토콜을 통해 생성된 PTK의 현재성을 보장하기 위해 PTK 생성 시 SNonce와 ANonce 값을 사용한다. MS나 AP 중 한쪽에 의해 PTK 생성이 전적으로 통제될 경우 재생 공격이나 main-in-the-middle 공격과 같은 보안공격이 가능하기 때문에 이를 예방하기 위해 두 개의 독립적인 난수를 사용하여 PTK를 생성한다. 그렇기 때문에 4H1과 4H2 메시지는 PTK생성 시 꼭 필요하다. 그러나 만약 PTK 생성에 필요한 Nonce를 MS와 AP 그 어느 한쪽에 의해서 일방적으로 결정되지 않는 값을 사용한다면 4H1 메시지와 4H2 메시지는 하나의 메시지로 통합될 수 있다. 우리는 MS와 AP 사이에 공유되는 순번(sequence number)을 기반으로 하는 2-way 핸드쉐이크 프로토콜을 제안한다.

4.1 순번 기반의 2-way 핸드쉐이크 프로토콜

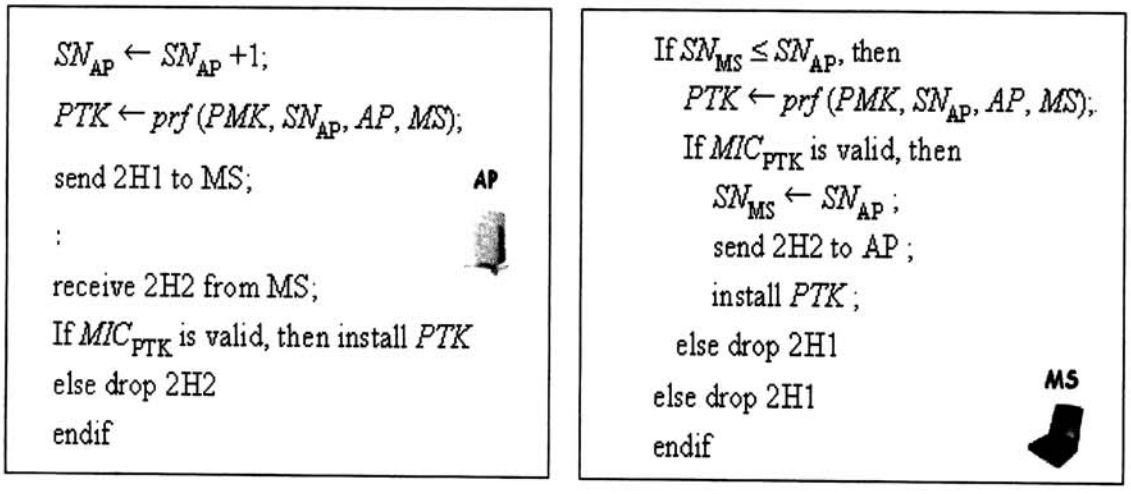
MS와 AS사이의 성공적인 EAP-TLS 기반의 802.1x 인증의 결과로 PMK는 AP(Authenticator)와 MS(Supplicant) 사이에 공유되어지고, PMKSA(PMK Security Association) 또한 양쪽 모두에 생성되어진다. PMKSA는 PMK와 PMKID로 구성되어 있다. 우리의 제안에서 순번 SN_{MS}와 SN_{AP}는 MS와 AP의 PMKSA 안에서 각각 생성되어진다. 그들은 생성될 때 0으로 초기화 된다. 우리는 2H1과 2H2 두 메시지로 구성된 아래와 같은 2-way 핸드쉐이크 프로토콜을 제안한다.

(2H1) MS ← AP : $msg1,\ SN_{AP},\ MIC_{PTK}$
(2H2) MS → AP : $msg2,\ SN_{AP},\ MIC_{PTK}$

(그림 5)의 (a)에서처럼 AP는 SN_{AP}를 1로 증가시킨 후 다음 식을 이용하여 PTK를 계산한다.

$$PTK = prf(PMK,\ SN_{AP},\ AP,\ MS)$$

PTK 계산 후 AP는 2H1 메시지를 MS에게 보낸다. 이때 2H1 메시지는 MIC_{PTK}를 이용하여 보호된다. MS가 2H1 메시지를 받으면 가장 먼저 SN_{AP}가 자신의 SN_{MS} 보다 작은 값이 아닌지를 검사하고 그렇지 않으면 (그림 5)의 (b)처럼 PTK를 계산 한 후 MIC_{PTK}를 검증한다. 이때 PTK의 생성



(a) (b)

(그림 5) 2-way 핸드쉐이크 프로토콜

은 위 식에서 보이는 것처럼 PMK와 MS, AP 양자간의 ID인 MAC주소가 포함되기 때문에 MIC_PTK의 검증이 성공하게 되면, 이는 결국 상대방에 대한 인증과 키 확인이 내재된 명시적 인증이 수행된 결과가 된다. 그렇기 때문에 만약 MIC_{PTK} 검증 작업이 성공적으로 끝난다면 MS는 AP가 자신과 동일한 PTK 및 PMK를 가지고 있음을 확인하게 되며, 결국 AP에 대한 인증작업을 수행한 결과가 된다. 그 후 MS는 SN_{MS}의 값을 SN_{AP}의 값과 동일하게 변경하고 PTK를 설치한다. 그런데 만약 2H1 메시지에 대한 MIC_{PTK} 검증이 실패한다면 MS는 해당 메시지를 무시한다. 또한 SN_{AP}의 값이 SN_{MS}의 값보다 작을 경우 2H1 메시지는 재생된 메시지로 판단되어 이 또한 무시된다. MS가 2H1 메시지에 대한 검증을 성공적으로 종료한 이후에는 계산된 PTK를 기반으로 *msg2*, SN_{AP}에 대한 MIC_{PTK}를 계산하여 2H2 메시지를 AP에게 전송한다.

MS가 보낸 2H2 메시지를 전달 받은 AP는 자신의 PTK를 기반으로 MIC_{PTK}를 검증한다. 만약 이 검증이 성공한다면 AP의 입장에서는 MS가 자신과 동일한 PTK를 가지고 있다는 확신을 가지게 되며 궁극적으로 MS와 동일한 PMK를 가지고 있음을 확인하게 된다. 이는 결국 AP가 MS에 대한 인증을 수행한것과 동일한 효과를 가지게 된다. 이후 AP는 PTK를 설치한다. 만약 2H1 메시지 전송부터 2H2 메시지 전송까지 아무 문제없이 순조롭게 진행 된다면 IEEE 802.1x 포트가 열리고 MS와 AP는 PTK를 이용하여 데이터 프레임을 암호화한 후 프레임을 주고받는다.

4.2 보안성 및 신뢰성 분석

4-way 핸드쉐이크 프로토콜의 근본적인 문제점은 4H1 메시지가 전혀 보호되지 않는 상태에서 전송된다는 것이다. 이로 인해 4-way 핸드쉐이크 프로토콜은 DoS 공격에 노출된다. 그러나 본 논문에서 제안하고 있는 2-way 핸드쉐이크 프로토콜은 2H1과 2H2 두 메시지가 PTK에 의해 보호되기 때문에 Dos 공격은 불가능하다.

4-way 핸드쉐이크 프로토콜에 사용되는 두개의 독립적인 난수 SNonce, ANonce와는 달리, 2-way 핸드쉐이크 프로토콜에서는 순번을 통해서 PTK의 현재성과 상호인증이 보장된다. SN_{MS}는 2-way 핸드쉐이크 프로토콜 시작 전후의 SN_{AP}와 동일하다. 따라서 새롭게 2-way 핸드쉐이크 프로토콜이 시작 할 때 마다 새로운 PTK를 보장하기 위해 AP는 SN_{AP}를 1씩 증가시킨다. 한편 FCS 오류와 MIC 오류에 기인하는 재전송을 대비하여 순번은 적절하게 관리되어져야 한다.

MS가 전달 받은 2H1 메시지의 SN_{AP}가 SN_{MS}와 동일한 예외적인 경우가 발생 할 수 있다. 2H1 메시지가 MS의 802.11 MAC에 의해서 성공적으로 받아들여지지 않았다고 가정하자. 거기에는 3가지 경우가 있다. 첫 번째는 MS로 전송되는 도중 메시지가 분실 된 경우이다. 두 번째는 FCS 오류에 의해 폐기된 경우이다. 세 번째는 2H1 메시지를 포함하고 있는 데이터 프레임에 대한 응답인 ACK 프레임이 AP로 전송 도중 분실 된 경우이다. 결국, 2H1 메시지는 $Timeout_1$이 종료된 이후에 MS로 재전송 되어져야 한다. 처음 두 경우에, SN_{MS}는 MS가 후속 작업을 진행 하지 않기 때문에 증가되지 않는다. 그래서 재시도 된 2H1 메시지의 SN_{AP}은 여전히 SN_{MS}보다 크다. 그러나 세 번째 경우에서, 2H1 메시지가 유효한 MIC를 가지고 있었다면 SN_{MS}는 증가된다. 그 이유는 ACK 프레임이 MS의 802.11 MAC에 의해 AP로 전송 되자마자 MS는 2H1 메시지에 대한 후속 작업을 진행하기 때문이다. 그래서 재시도된 2H1 메시지의 SN_{AP}는 SN_{MS}와 동일하게 된다.

마지막 세 번째 경우를 고려하면, 2H1 메시지의 SN_{AP}가 SN_{MS}와 똑같을 경우 해당 메시지가 AP에 의해 재시도된 2H1 메시지인지 또는 공격자에 의해 반복된 2H1 메시지인지를 구별하는 것이 필요하다. 이를 해결하기 위한 하나의 방법은 특정시간 간격 안에 재시도된 2H1 메시지를 정상적인 메시지로 인정하는 것이다. 이러한 목적으로 $Timeout_{SN}$을 SN_{MS}와 관련하여 정의한다. SN_{MS}가 변화 될 때 언제나 $Timeout_{SN}$은 최대값 (예 100ms)으로 재 설정 된다. 만일 MS가 $Timeout_{SN}$이 만료되기 전에 SN_{MS}와 동일한 값의 SN_{AP}를 포함한 2H1 메시지를 받게 되면 해당 메시지는 재시도된 2H1 메시지로 간주되고 정상적으로 처리된다. 공격자가 $Timeout_{SN}$이 만료되기 전에 2H1 메시지를 재전송 할 가능성은 있다. 그러나 공격자가 2-way 핸드쉐이크 프로토콜 과정 중 관찰된 메시지에 기초하여 PTK를 계산하는데 걸리는 시간을 생각한다면 $Timeout_{SN}$ 사이의 공격자의 재생공격은 불가능 하다.

재전송은 MIC 오류의 경우에도 발생할 수 있다. 여기서 우리는 유효하지 않은 MIC를 포함하는 2H1 메시지 그리고 유효하지 않은 MIC를 포함한 2H2 메시지의 두 가지 경우를 고려한다. 첫째로, 만일 전송된 2H1 메시지의 MIC가 유효하지 않다고 판단되면 해당 메시지는 폐기되고 SN_{MS}는 SN_{AP}로 변경되지 않는다. 그 후 (그림 2)에서와 마찬가지로 2H1 메시지는 $Timeout_2$ 만료 후에 MS로 재전송 될 것이다. 두 번째로, 만일 2H1 메시지가 유효한 MIC 값을 가지고 있었다면 MS는 SN_{MS}를 SN_{AP}의 값과 동일하게 변경하고 2H2 메시지를 AP에게 전송한다. 그런데 2H2 메시지가 유효하지 않은 MIC 값을 가지고 있으면 그것은 AP에 의해 폐기되고 $Timeout_2$ 만료 후에 2H1 메시지를 MS에게 재전송한다. 두 경우 모두 재전송된 2H1 메시지를 위한 PTK 계산 시 SN_{AP}는 증가되어진다. 특히, 두 번째 경우는 유효하지 않은 4H4 메시지에 의해 야기되는 4-way 핸드쉐이크 프로토콜의 것과 같다. 즉, MS는 이미 설치된 PTK를 가지고 있기 때문에 암호화 되지 않은 재전송된 2H1 메시지는 정상적으로 처리될 수 없다. 그러나 3장에서 논의된 변경된 의사코드를 사용한다면 이러한 경우 재전송된 2H1 메시지는 2-way 핸드쉐이크 프로토콜의 일부로써 정상적으로 처리될 수 있다.

4.3 관련연구

[6, 7]의 연구는 DoS 공격으로부터 4-way 핸드쉐이크 프로토콜을 보호하기 위한 방법을 제안하고 있다. 4-way 핸드쉐이크 프로토콜은 암호화되지 않은 4H1 메시지로 인해 안전성이 결여된다. 이에 대한 문제를 해결하기 위해 첫 번째로 제시되었던 방법은 PMK와 시각표(timestamp)를 이용하여 생성된 임시키로 4H1 메시지를 보호하는 방법이다. 그리고 또 다른 한 가지 방법은 Supplicant 측에서 정상적인 AP에서 받는 메시지나 공격자로부터 받는 메시지나 모두 수용하여 그때마다 동적인 PTK를 계산하는 방식이다.

그러나 위의 두 가지 해결 방안은 여전히 MS와 AP사이의 4개 메시지 교환에 기초하고 있다. 그렇기 때문에 본 논문이 제안하고 있는 2-way 핸드쉐이크 프로토콜은 메시지 개수에 있어서 더 효율적이다. [9]의 연구는 PTK를 도출하기 위해 MS와 AP사이에 교환되어지는 메시지를 감소시키기 위한 방식을 제안하고 있다. 그러나 [9]의 연구에서 제안하는 방식은 4-way 핸드쉐이크 프로토콜과 더불어 802.1x EAP-TLS 프로토콜의 수정을 요구한다. 즉, 4H1과 4H2 메시지 모두 802.1x EAP-TLS 프로토콜 안에서 교환되는 것을 제안하고 있다.하지만, 그것은 여전히 보안 공격에 노출되어 있다. 또한 [6, 7]과 [9]에서 제안하고 있는 방식은 3장에서 논의된 4H4 메시지안의 MIC 오류와 관련된 상황을 다룰 수가 없다.

5. 결 론

우리는 본 논문을 통해 802.11i의 4-way 핸드쉐이크 프로토콜에 대해 안전성과 신뢰성이라는 두 가지 이슈에 대해 분석하였다. 선행된 연구들은 4-way 핸드쉐이크 프로토콜이 DoS 공격과 같은 정상적인 프로토콜 수행을 방해하는 공격에 안전하지 않다는 것을 보여주고 있다. 본 논문에서는 4-way 핸드쉐이크 프로토콜 설계 자체의 결함으로 인해 MIC 오류 발생 시, 정상적으로 프로토콜이 진행 될 수 없다는 것을 보여주고 있으며 이에 대한 해결 방법 또한 제시했다. 최종적으로 우리는 4-way 핸드쉐이크 프로토콜보다 안전하고 효율적인 2-way 핸드쉐이크 프로토콜을 제시하였다.

참 고 문 헌

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

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

[3] IEEE 802.11f, Recommended Practice for Multi -Vendor Access Point Interoperability via an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11 Operation, IEEE Standard, July, 2003.

[4] IEEE 802.11r Draft Standard, Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Fast BSS Transition, IEEE Standard, September, 2007.

[5] IEEE 802.1x, IEEE Standards for Local and Metropolitan Area Networks: Port based Network Access Control, IEEE Standard, June, 2001.

[6] C. He, C. Mitchell, Analysis of the 802.11i 4-Way handshake, in Proceedings of the ACM Workshop on Wireless Security, Philadelphia, Pa, USA, October, 2004, pp.43-0.

[7] C. He, J. C. Mitchell, Security analysis and improvements for IEEE802.11i, in Proceedings of the 12th Annual Network and Distributed System Security Symposium, San Diego, Calif, USA, February, 2005.

[8] F. De Rango, D. C. Lentini, S. Marano, Static and Dynamic 4-Way Handshake Solutions to Avoid Denial of Service Attack in Wi-Fi Protected Access and IEEE 802.11i, EURASIP Journal on Wireless Communications and Networking, vol. 2006, Article ID 47453, 2006, pp.1-9.

[9] J. Hur, C. Park, Y. Shin, H. Yoon, An efficient Proactive Key Distribution Scheme for Fast Handoff in IEEE 802.11 Wireless Networks, ICOIN 2007, Lecture Notes in Computer Science, LNCS Vol.4883, Springer-Verlag, pp.407-418

박 창 섭

e-mail : csp0@dankook.ac.kr

1983년 연세대학교 경제학과 졸업

1983년 한국 IBM 근무

1990년 미국 Lehigh Univ. 전자계산학(박사)

1990년~현 재 단국대학교 전자컴퓨터학부 교수

관심분야 : 네트워크 보안, 암호 프로토콜

우 병 덕

e-mail : sayttre@dankook.ac.kr

2006년 단국대학교 컴퓨터과학과(학사)

2006년 (주)EOTECHNICS 근무

2008년 3월~현 재 단국대학교 전자계산학 석사과정

관심분야 : 정보보호, 무선 네트워크 보안