Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.25, NO.6, Dec. 2015 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2015.25.6.1515

신속한 초기 링크 셋업 과정을 위한 WLAN 보안 접속 프로토콜*

김 민 희,† 박 창 섭‡
단국대학교

WLAN Security Access Protocol for Rapid Initial Link Setup Process*

Min-Hee Kim,† Chang-Seop Park‡
Dankook University

요 약

다양한 모바일 기기가 등장하면서 WLAN(Wireless Local Area Network)을 통하여 네트워크 서비스를 받는 경우가 많아졌다. 그러나 제한된 ESS(Extended Service Set) 영역에 한꺼번에 급격히 많은 수의 모바일 기기가 네트워크 접속을 시도할 경우, 현재 WLAN 보안 표준인 802.11i의 초기 링크 셋업 과정은 네트워크 연결 지연 문제를 발생시킨다. 본 논문에서는 802.11i 기반의 ESS 영역에서 신속하고 간단한 초기 링크 셋업 과정을 수행하는 WLAN 접속 프로토콜을 제안한다.

ABSTRACT

It has been prevalent to be serviced through WLAN(Wireless Local Area Network) as a variety of mobile devices have been introduced. If the number of mobile devices increases rapidly for the network access in a limited range of ESS(Extended Service Set), a lengthy connection delays are induced due to the initial link setup process of the IEEE 802.11i which is WLAN security standard. In this paper, we propose a new initial link setup protocol which can be executed in the ESS area of WLAN.

Keywords: IEEE 802.11i, WLAN, 4-way Handshake, Initial Link Setup Process

I. 서 론

모바일 기기의 사용 증가에 따라 WLAN (Wireless Local Area Network)을 통한 네트워크 접속이 급증하게 되었다. WLAN이 제공하는 서비스의 사용자가 증가함에 따라, 다양한 보안 위협으로부터 WLAN을 보호하기 위한 WEP(Wired Equivalency Privacy) 기반의 IEEE 802.11b가 1999년에 도입되었다[1][2]. 그러나 WEP 암호 기법은 암호화와 인증 방법이 보안상 취약하다고 판명되어 신뢰성을 잃어버리게 되었고[3], 이를 보완하기 위하여 2004년에 보다 안전한 RSN(Robust Secure Network) 기반의 IEEE 802.11i[4]를 국제 WLAN 보안 표준으로 제정하였다.

IEEE 802.11i가 도입됨에 따라 기존에 존재하던 WLAN 보안 이슈들이 많이 해결되었다. 802.11i에서는 802.1x 포트 기반 네트워크 접근 제어를 채택하여 WLAN에 연결하기 위한 기기의 인증 메커니즘을 제공하였고, 동적인 WEP 키 관리가 가능해졌으며, 또한 AP(Access Point)와 모바일 기기간의 보안을 강화하였다.

Received(11. 12. 2015), Modified(12. 07. 2015), Accepted(12. 08. 2015)
* 본 연구는 2015년도 정부(교육과학기술부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행되었음.(NRF-2014R1A1A2055074)
* 본 연구는 미래창조과학부 및 한국인터넷진흥원의 "2015년도 정보보호 석사과정 지원사업"의 연구결과로 수행되었음.
† 주저자, minhee4788@nate.com
‡ 교신저자, csp0@dankook.ac.kr(Corresponding author)

그러나 모바일 기기 사용자들이 폭발적으로 늘어나고, 모바일 기기에서 WLAN의 활용 범위가 이전보다 훨씬 넓어짐에 따라 IEEE 802.11i 보안 표준에 몇 가지 문제가 발생하기 시작하였다. IEEE 802.11i에서는 모바일 기기(Station)들이 특정 ESS(Extended Service Set) 영역에 들어오면 STA들은 AP에 연결하기 위하여 초기 링크 셋업 과정을 수행한다[5]. 이러한 과정은 제한된 ESS 영역 안에서 적은 수의 STA이 AP와의 연결을 시도할 때에는 수행과정에 전혀 무리가 없다. 그러나 급격히 많은 수의 STA이 들어와 AP에 연결을 한꺼번에 시도하려 할 때는 IEEE 802.11i의 초기 링크 셋업 과정이 지연되기 때문에 연결 과정에 많은 시간을 소비하게 되어 STA들이 안전한 보안을 유지하면서도 신속한 서비스를 제공받지 못하는 경우가 발생할 수 있다[6].

이러한 802.11i의 문제를 해결하기 위하여 최근에는 802.11ai 기술이 논의되고 있다[7][8]. 802.11ai는 기존의 보안 인증에 필요한 시간을 10분의 1로 단축하는 것을 핵심으로 하여 802.11i의 초기 링크 셋업 과정의 지연을 효과적으로 줄이고자 하는 기술이다. 802.11ai의 활용 사례들을 살펴보면 다음과 같다. 우선, 출퇴근 시간 때 지하철역과 같은 인구 밀집 지역에서는 스펙트럼 양, 네트워크의 수, 모바일 기기 수가 급격히 증가하게 된다. 이와 더불어 시그널링의 오버헤드가 발생하게 되고 불필요한 정보의 교환이 일어남에 따라 제공되는 서비스 질이 떨어지게 된다. 그리고 단 시간 안에 매우 많은 수의 차량이 제한된 지역에 집중적으로 몰리게 되면 엄청난 양의 정보들이 업로딩 또는 다운로딩 되는 현상이 발생한다. 또한 기타 사례로는 전자 지불 시스템을 이용할 때, 여행자들이 여행지 관련 정보를 검색할 때, 차량들이 인터넷에 접속 또는 긴급 서비스 이용할 때, 환승구간, 역 로비, 동적인 교통체계 등이 있다.

본 논문에서는 802.11ai 환경[9]을 기반으로 하여 IEEE 802.11i의 초기 링크 셋업 과정의 지연을 감소시키는 것에 초점을 두었다. 따라서 STA이 특정 ESS 영역에 들어올 경우, STA가 AP와 연결하기 위하여 전송되는 총 메시지 수를 효과적으로 줄여 신속한 초기 링크 셋업 과정이 이루어지는 프로토콜을 제안한다. 본 논문의 구성은 다음과 같다. 제 2장에서는 모바일 기기가 WLAN 환경에서 네트워크 접속하는 과정에 관한 기존 연구들을 알아본다. 제 3장은 제안 기법으로 2장에서 살펴본 기존 연구를 바탕으로 하여 더욱 간단한 초기 링크 셋업 과정의 ESS 영역 접속 프로토콜을 설계한다. 제 4장에서는 3장에서 제안한 프로토콜의 안전성에 관하여 분석을 한다. 제 5장에서는 네트워크 시뮬레이터인 NS2를 사용하여 본 논문에서 제안한 프로토콜의 성능 분석을 한 후, 6장을 통해 본 논문의 결론을 맺는다.

II. 관련 연구

2.1 IEEE 802.11i

현재 STA이 802.11i 기반의 특정 ESS로 들어와 네트워크 접속을 시도할 경우에 대부분 IEEE 802.11i의 보안정책에 따라 서비스가 제공되고 있다. 802.11i의 초기 링크 셋업 과정이 이루어지는 환경은 각각 STA, AP, AS(Authentication Server) 이렇게 3개의 개체로 구성이 된다. 802.11i에서 STA 인증은 PSK(Pre-Shared Key) 기반 인증 방법과 Fig. 1과 같이 인증서 기반의 인증 방법이 존재한다. 본 논문의 설명 과정에서 사용하는 표기법들은 Table 1을 따른다.

우선, AP Discovery 단계에서는 네트워크에 접속하고자 하는 STA이 주변의 연결 가능한 AP들에게 브로드캐스트로 *Probe Request* 메시지를 보내 RSN 지원 여부 탐색을 한다. Authentication과 Association 단계에서는 STA이 연결을 원하는 AP와의 Open Authentication 과정을 수행하고 *Association Request/Response* 메시지를 주고받

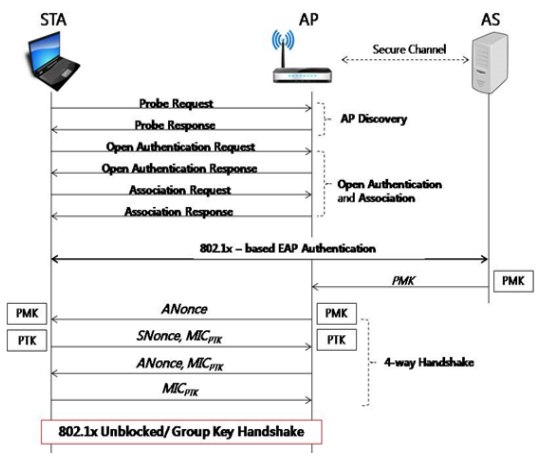


Fig. 1. Protocol of IEEE 802.11i

Table 1. Notations used in this paper

Notation	Description
SNonce, ANonce	Random number, generated by STA and AP, respectively
PSK	Pre-Shared Key
PMK	Pairwise Master Key
PTK	Pairwise Transient Key
STA, AP, AS	ID(Identity) of STA, AP, AS
RSN	RSN Information Element
$h(.)$, $f(.)$	Hash Functions
$prf(.)$	Pseudo Random Function
t	Counter
MIC_{PTK}	Message Integrity Check for all the preceding fields using PTK

는다. EAP(Extensible Authentication Protocol) Authentication 단계에서는 STA와 AS가 상호인증을 하고, 인증에 성공하면 AS가 해당 AP에게 *PMK*를 전달한다. 이때, *PMK*는 해당 세션에서 사용하고자 하는 세션 키인 *PTK*를 생성하기 위한 목적으로 사용되는 키이다. 4-way Handshake 단계에서는 STA와 AP가 각각 생성한 난수 *SNonce*와 *ANonce*를 교환하여 상호인증을 한다. 그리고 *SNonce*, *ANonce*, *PMK* 및 각각의 식별자 값에 802.11i 고유의 prf함수를 적용하여 *PTK*를 생성한다. 그리고 *PTK*를 기반으로 일방향 해쉬 함수를 적용하여 MIC_{PTK}를 도출해낸 후, 각각 MIC_{PTK}를 전송하고 이 값을 검증 한다. 이 과정을 통해 *PTK*에 관한 키 확인 및 메시지 무결성 검증 과정을 수행한다. 이러한 4-way Handshake에 관하여 안전성도 분석 되었다[10].

이와 같이 IEEE 802.11i의 초기 링크 셋업 과정에서는 다수의 메시지를 주고 받게 된다. 모바일 기기의 발달과 더불어 WLAN 활용 범위가 점점 더 넓어지는 최근의 동향에서 이러한 802.11i의 초기 링크 셋업 과정은 적합하지 않다. 제한된 ESS 영역에 한꺼번에 수많은 STA이 들어올 경우 네트워크 연결 지연을 유발하여 서비스 제공에 문제가 발생한다.

2.2 FLAP

802.11i 초기 링크 셋업 과정의 문제점을 해결하고자 FLAP(An Efficient WLAN Initial Access Authentication Protocol)이 제안되었다[11]. FLAP에서는 STA이 특정 ESS 영역에 접속할 때 초기 링크 셋업 과정에서 교환되는 메시지의 개수를 감소시킨 프로토콜을 제안하였다. FLAP의 특징은 첫째, 802.11i 프로토콜에서 의미 있는 역할을 하지 않는 *Open Authentication* 메시지를 활용하여 4-way Handshake 기능을 구현하였다. 둘째, PSK 기반의 인증 방법을 채택하여 많은 메시지 교환이 필요한 EAP Authentication 과정을 대체하였다. FLAP은 위의 두 가지 과정을 통해 STA이 ESS 영역에 접속할 때 필요한 총 메시지의 개수를 감소시키게 된다.

Fig. 2와 같이 FLAP은 AP Discovery 단계, Authentication 단계, Association 단계로 진행된다. 그리고 STA과 AS 사이에는 안전한 방법으로 PSK가 미리 공유되어있다고 가정하는 PSK 기반의 인증방식을 채택하였다.

FLAP 진행 과정에서 사용하는 식은 다음과 같다.

$$PMK = h(PSK, \text{“PMK”}, STA, AS, t) \quad (1)$$

$$PTK = prf(PMK, STA, AP, SNonce, ANonce) \quad (2)$$

$$F = f(PSK, SNonce, STA, AS, t) \quad (3)$$

$$E = f(PSK, SNonce, AS, STA, t) \quad (4)$$

우선, AP Discovery 단계에서 STA은 연결 가능한 AP들에게 브로드캐스트로 *Probe Request* 메시지를 보내면 AP들은 AS의 식별자와 보안 옵션이 탑재된 *Probe Response* 메시지를 유니캐스트로 해

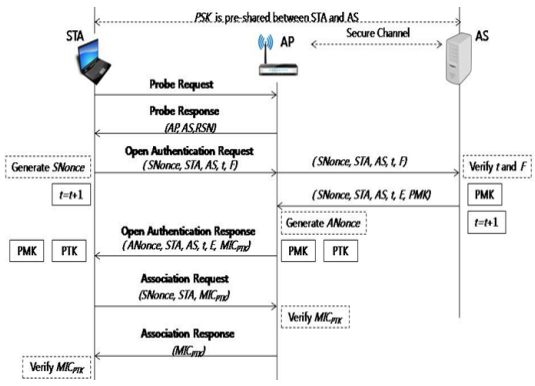


Fig. 2. Protocol of FLAP

당 STA에게 보낸다.

Authentication 단계에서는 STA은 *SNonce*를 생성하여 *t*값과 *F*값과 함께 AP에게 전송한다. 이때, AP는 AS에게 값을 전달해주는 역할만 하고 있기 때문에 AP의 부담을 줄여주고 있고 또한 *F*값을 통해 AS는 STA을 인증할 수 있다. AS는 *t*값과 *F*값을 검증한 후 *PMK*를 생성하고 *E*값을 계산하여 AP에게 전달한다. *SNonce*를 전달받은 AP는 *PTK*를 계산하고, *ANonce*를 생성하여 *E*값과 함께 STA에게 전송한다. *F*값과 마찬가지로 *E*값을 통해 STA은 AS를 인증하게 된다.

Assocation 단계에서 *ANonce*를 전달받은 STA은 *PTK*를 생성하고 *PTK*에 대한 키 확인을 하기위하여 MIC_{PTK}를 AP에게 전송한다. AP는 MIC_{PTK}를 검증하고 검증에 성공하면 AP가 생성한 *PTK*에 대한 MIC_{PTK}를 보낸다. STA이 받은 MIC_{PTK}에 대한 검증이 성공적으로 이루어지면 해당 AP와의 연결이 이루어진다.

이 논문에서 제안하는 프로토콜은 6개의 메시지만으로도 초기 링크 셋업과정을 수행하여 IEEE 802.11i의 프로토콜보다 현저하게 적은 수의 메시지로 특정 ESS 영역에 접속 할 수 있다. 그렇게 되면 인구밀집 지역 등의 상황에서도 STA은 신속하게 네트워크에 연결될 수 있으며 또한 802.11i와 같은 보안 수준의 서비스를 제공받을 수 있다.

III. 제안 기법

3.1 설계원리

본 논문에서 제안하고자 하는 프로토콜은 FLAP을 기반으로 하여 802.11i와 같은 보안 안전성을 제공하면서도 더욱 효과적이고 간단한 초기 링크 셋업 과정을 설계하였다.

첫째, FLAP에서는 AS가 STA을 인증한 후 AP가 생성한 *ANonce*를 *Open Authentication Response* 메시지에 탑재하여 STA에게 보낸다. 제안 프로토콜에서는 이 과정 대신 초반에 주변 AP들이 *ANonce*를 생성하여 *Probe Response* 메시지를 해당 STA에게 전송할 때 탑재하여 보내는 방식을 채택하였다. 이러한 방식으로 프로토콜이 진행되면 이전의 FLAP에서 주고받는 총 메시지의 수보다 적은 메시지의 수로 ESS 영역에 접속할 수 있다. 기존의 방식보다 간단한 메시지를 주고받으면서도 훨씬 신속한 초기 링크 셋업 과정을 수행할 수 있게 된다.

둘째, FLAP에서 *E*값을 통해 STA이 AS를 인증하게 되는데, 제안 프로토콜에서는 *E*값을 삭제하였다. STA와 AS 사이에 *PSK*가 사전에 미리 공유되는 키이고, *F*값 계산에 *PSK*가 포함된다. 그러므로 AP를 통하여 STA가 *F*값을 AS에게 전송한 후, AS가 *F*값을 검증에 성공하면 *PMK*를 전달받은 AP가 MIC_{PTK}를 STA에게 전송하여 STA이 MIC_{PTK}를 검증하는 과정만으로도 STA과 AS는 상호인증이 가능하다. FLAP에서와는 달리 *E*값을 생략할 수 있는 근거는 *PTK*가 궁극적으로 *PSK*에 기반을 두고 도출되기 때문에 MIC_{PTK}값의 검증이 유효함은 AP에 대한 인증뿐만 아니라, 결국 AS에 대한 인증도 포함하게 된다. *E*값을 삭제함으로써 AS가 *E*값을 계산해야 하는 부담을 줄여줄 수 있다.

3.2 제안 프로토콜

본 논문은 IEEE 802.11i에 명시되어 있는 프레임워크를 개선하여 초기 접속 과정에서 최소한의 메시지 전달을 통한 STA과 AP, AS간의 상호인증 및 세션 키 분배 프로토콜을 제안한다. Fig. 3과 설명 과정에서 사용하는 표기법들은 Table 1을 통해 명시하고 있다.

IEEE 802.11i와 FLAP에서와 마찬가지로 제안 프로토콜에도 AP와 AS 사이에는 안전한 채널(Secure Channel)이 존재한다고 가정한다. 또한 사전에 AS는 등록과정을 통해 STA의 인증 정보를 갖고 있고, 사전 등록과정 후에는 STA과 AS 사이에는 두 개체만 알고 있는 키인 *PSK*가 안전한 방법으로 미리 공유 되어있다고 가정한다. 그리고 *PMK*와 *PTK*, *F*값의 계산식은 FLAP과 동일하다.

• 단계 1: Probe Request 전송

특정 ESS 영역에 STA가 들어오면, STA은 주변 AP들에게 *Probe Request* 메시지를 브로드캐스트한다.

• 단계 2: Probe Response 전송

Probe Request 메시지를 받은 각각의 AP들은 *ANonce* 값을 생성한다. 그리고 *ANonce*를 AS의 식별자와 보안 옵션과 함께 *Probe Response* 메시지에 탑재하여 해당 STA에게 유니캐스트로 전송한다. 이때, AP가 생성한 *ANonce*는 재사용될 수 없는 난수로 재생 공격을 방지할 수 있다. 주변 AP들이 해당 STA에게 *Probe Response* 메시지를 전송

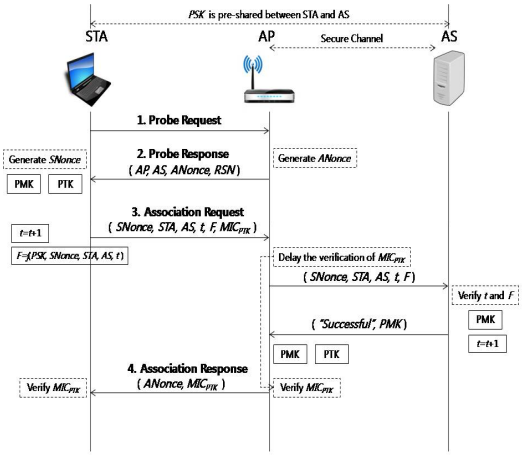


Fig. 3. Proposed Protocol

하면, STA은 그 중 가장 신호가 강한 AP를 선택하는 방식을 채택했다.

• 단계 3: Association Request 전송

Probe Response 메시지를 받은 STA은 *PMK*를 계산할 수 있다. *PMK*를 계산할 때 *t*값이 포함되는데, *t*는 초기 값이 1로 설정되어 있고 한 세션이 끝날 때 마다 1씩 증가된다. 그리고 생성한 *PMK*를 이용하여 해당 세션에 사용할 세션 키인 *PTK*를 계산할 수 있다. 또한 STA은 *SNonce*를 생성하고 *F* 값을 계산한다.

$$PMK = h(PSK, \text{“PMK”}, STA, AS, t) \quad (5)$$

$$PTK = prf(PMK, STA, AP, SNonce, ANonce) \quad (6)$$

$$F = f(PSK, SNonce, STA, AS, t) \quad (7)$$

STA은 *SNonce*를 *t*값, *F*값, MIC_{PTK}와 함께 *Association Request* 메시지에 탑재하여 선택한 AP에게 전송한다. 이때, AP는 STA이 생성한 *PTK*에 관한 키 확인을 하기 위한 값인 MIC_{PTK}에 대한 검증을 일시적으로 보류한다. AP가 STA으로부터 받은 값들을 AS에게 전달하면 AS는 *t*를 검증한 후, *F* 값을 계산하여 전달받은 *F*값과 비교하여 *F*값을 검증한다. *t*와 *F*값에 관한 검증이 성공적으로 이루어지면 *PMK*를 계산하여 AP에게 보낸다. AS로부터 *PMK*를 받은 AP는 *PTK*를 계산할 수 있고, 보류되었던 MIC_{PTK} 값을 검증한다. MIC_{PTK} 값의 검증을 통하여 AP는 STA 인증 및 생성된 *PTK*에 대한 키 확인을 할 수 있다.

• 단계 4: Association Response 전송

MIC_{PTK} 값에 대한 검증이 성공적으로 이루어지면, 성공했다는 의미로 *ANonce*와 자신이 생성한 *PTK*에 관한 MIC_{PTK}를 *Association Response* 메시지에 탑재하여 STA에게 전송한다. *Association Response* 메시지를 받은 STA은 메시지에 포함된 MIC_{PTK}를 검증한다. 검증이 완료되면 STA은 해당 AP와 연결이 된다.

IV. 안전성 분석

제 3장에서는 본 논문에서 제안하는 프로토콜의 설계원리와 진행과정에 대해서 소개하였다. 제 4장에서는 제안 프로토콜의 안전성을 분석하고자 한다. 키의 Freshness, 4-way Handshake, PSK기반 인증, 세션 키 확인, Man-In-The-Middle 공격과 Replay 공격에 관하여 분석한다.

4.1 키의 Freshness

제안 프로토콜에서는 *PSK*와 *t*값을 기반으로 *PMK*를 생성한다. 이때 사용되는 *t*는 카운터 값으로 한 세션이 끝날 때 마다 1씩 증가 하고, STA와 AS 사이에서 동기화 되어야 한다. 미리 공유되어 있는 고정된 *PSK*를 기반으로 *PMK*를 생성하는 과정에서 계속 변화되는 *t*값을 같이 해쉬 함수에 넣어줌으로써 키의 Freshness를 보장한다.

4.2 4-way Handshake

IEEE 802.11i에서 STA와 AP간의 상호인증과 키 확인을 하기위해서 4-way Handshake 과정이 이루어진다. 제안 프로토콜에서는 이러한 4-way Handshake 과정을 *Probe Response* 메시지, *Association Request/Response* 메시지를 통해 설계하였다. 그 메시지들에 추가적인 값들을 탑재하여 STA와 AP가 각각 생성한 Nonce 값을 교환하고, 키 확인 값인 MIC_{PTK}를 서로에게 전송하는 과정을 구현함으로써 4-way Handshake와 동등한 기능과 목적을 달성하였다.

FLAP에서도 이와 비슷한 방식으로 4-way Handshake 과정을 프로토콜에 구현하였지만 총 6개의 메시지를 주고 받는다. 반면, 본 논문의 제안 프로토콜에서는 STA과 AP사이에서 단 4개의 메시지의 전송과정만으로도 802.11i의 4-way Handshake 과정 및 사용자 인증과정을 담아내고 있다. 802.11i와 FLAP 보다 적은 수의 메시지로 802.11i의 보안 기능을 구현하였고 초기 링크 셋업 과정의 지연을 줄였다.

4.3 PSK 기반 인증

WLAN 서비스를 이용하고자 할 때, STA 인증 방법은 인증서 기반의 EAP 인증방식과 PSK 기반의 인증방식이 있다. IEEE 802.11i에서는 인증서 기반의 EAP 인증방식은 필수 사항이고 PSK 기반의 인증방식은 선택 사항으로 채택되어 있다. FLAP에서는 PSK 기반의 인증방식을 채택하고 있다.

우선, 인증서 기반의 EAP 인증방식은 STA와 AS가 상호인증을 한 후 AS가 *PMK*를 생성하여 AP에게 전달한다. 이때, Fig. 1에서와 같이 STA와 AS 사이의 인증과정에서 가장 많은 메시지의 교환이 일어난다. 그리고 PSK 기반의 인증방식은 사전에 안전한 방법으로 STA과 AP(혹은 AS)사이에 *PSK*를 공유한 후, 연결을 시도 할 때 *PSK*로부터 *PMK*를 생성하고 4-way Handshake를 수행하여 *PMK*를 확보하였는지를 확인하는 과정을 통해 상호인증을 한다. PSK 기반의 인증방식을 사용하게 되면 사전에 안전한 방법으로 키를 분배해야한다는 점이 있지만 프로토콜 진행과정에서 메시지 개수가 가장 많이 필요한 인증서 기반의 EAP 인증과정을 생략할 수 있다. 인증서 기반에서 가장 널리 사용되고 있는 EAP-TLS 인증방식을 사용했을 경우 대략 22~26개의 메시지 교환이 이루어지는데, PSK 기반의 인증방식을 통해 보다 훨씬 적은 단계만으로도 상호인증과 *PTK* 분배가 가능하다. 본 논문에서는 802.11ai 기반의 환경에 초점을 맞추고 있기 때문에 STA과 AP와의 연결이 보다 신속하게 이루어져야 한다. 따라서 802.11ai 기반의 환경에서는 PSK 인증방식이 보다 적합하다고 할 수 있다. 제안 프로토콜에서 PSK 인증방식을 사용함으로써 802.11ai 환경에 적합한 사용자 인증방식을 적용하여 안전한 보안을 유지하면서도 신속한 초기 링크 셋업과정이 가능하게 하였다.

4.4 세션 키 확인

세션 키인 *PTK*의 키 확인을 하기 위해 *Association Request* 메시지를 받은 AP가 MIC_{PTK} 값을 검증해야 한다. 제안 프로토콜에서는, MIC_{PTK} 값에 대한 검증을 잠시 뒤로 미뤄두었다가 AS로부터 *PMK*를 전달받은 후에 앞서 미뤄두었던 검증을 수행하는 과정을 통하여 FLAP 보다 메시지 개수를 줄이면서도 *PTK*의 키 확인 과정이 이루어지게 하였다.

4.5 Man-In-The-Middle 공격과 Replay 공격

Association Response(*ANonce*, MIC_{PTK}) 메시지를 수신한 STA는 MIC_{PTK}에 대한 검증을 통해 AP가 정단한 AP인지 아니면 불법적으로 설치된 AP인지에 대한 확인이 가능하다. MIC_{PTK}의 생성에는 *PTK*가 필요하고, 다시 *PTK* 생성에는 *PMK* 그리고 *PSK*가 기반이 되기 때문에, STA가 접속을 시도하는 AP가 AS와 사전에 안전한 채널이 설정되어 있지 않다면 결국 유효한 MIC_{PTK}를 생성해 낼 수가 없게 된다. 따라서 AP를 경유한 STA와 AS 간의 통신에 있어서 Man-In-The-Middle 공격의 가능성은 존재하지 않는다.

STA와 AS 간에는 *PSK* 이외에도 카운터 값인 t가 공유되어지고 매번 접속시도마다 새로운 t값이 사용된다. 따라서 *Association Request* 및 *Association Response* 메시지에 대한 Replay 공격은 불가능하게 된다. 특히, (식 5)에서와 같이 $PMK = h(PSK, \text{“PMK”}, STA, AS, t)$를 도출하는 데에 있어서 t값이 이미 사용되고 있기에

Table 2. Comparison between each protocol

Protocol / Subsection	802.11i	FLAP	Proposed Protocol
Mutual authentication & Session key generation	O	O	O
Hash Function	X	O	O
STA-AS Authentication	certificate based	2 formula (E, F)	1 formula (F)
Total Stage	11	6	4

Association Response 메시지에 별도로 *t*값을 첨가할 필요는 없게 된다.

안전성 분석을 위한 항목들을 기반으로 하여 Table 2와 같이 기존의 프로토콜들과 본 논문에서 제안한 프로토콜을 항목별로 비교하였다. 본 논문에서 제안한 프로토콜이 기존의 프로토콜들과 비교하였을 때 STA과 AS간의 인증에서 *F*값 한 개만을 사용하면서 총 수행단계도 제일 적은 것을 알 수 있고, 그럼에도 기존의 프로토콜들과 동등한 보안정도를 제공한다는 것을 확인할 수 있다.

V. 성능 분석

제 5장에서는 기존에 제안되었던 FLAP과 본 논문에서 제안한 프로토콜의 성능을 비교 분석한다. 성능 비교 분석을 위해 네트워크 시뮬레이터로 널리 이용되고 있는 NS2를 사용하였으며, Table 3과 같이 시뮬레이션 환경을 설정하였다. 또한 무선 환경 기본 설정 값으로 802.11b의 기본 파라미터를 사용하였다. Fig. 4는 STA의 수가 20개일 때 시뮬레이션 화면을 캡처한 것이다.

첫 번째 실험에서는 STA의 수를 1부터 50까지 늘려가며 ESS 영역안의 모든 STA들이 동시에 스캐닝을 시작하게 한 후 특정 STA이 *Association Response* 메시지를 받은 시간 즉, AP에 연결되기까지의 시간을 측정하였다. Fig. 5의 결과 값은 FLAP은 평균 38.04ms이고 제안 프로토콜은 평균 23.86ms가 나왔다. 그리고 STA의 수가 30개에서 40개로 늘어날 때 급격하게 연결 시간이 늘어나는 것을 볼 수 있다. 이는 STA의 수가 40개로 증가했을

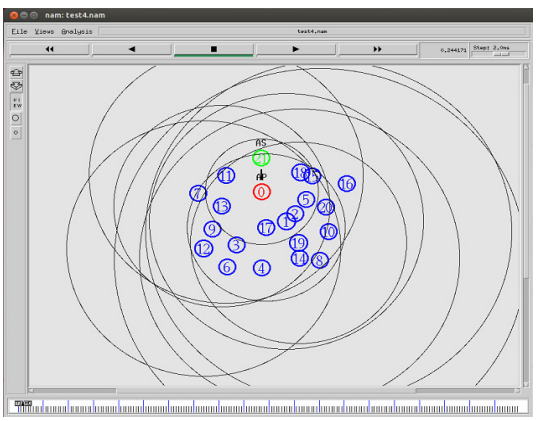


Fig. 4. Simulation capture

Table 3. Simulation environment setting

Item	Value
Number of STAs	1~50
Number of APs	1
Number of ASs	1
Simulation Time	20s
Bandwidth	11M
Area	600m * 600m
Scan Type	Active

경우에 이전에 비해 패킷의 충돌이 많이 발생하였고, 패킷의 재전송이 반복적으로 시도되었음을 알 수 있다. 첫 번째 실험의 경우, STA의 수가 늘어나도 제안한 프로토콜에서 AP와의 연결에 걸리는 시간이 FLAP에 비해 평균 약 15ms 정도 적은 것을 알 수 있다. 또한 FLAP과 비교했을 때 본 논문에서 제안한 프로토콜의 측정 시간이 전체적으로 아래쪽에 분포하는 것을 확인 할 수 있다.

두 번째 실험에서는 첫 번째 실험과 마찬가지로 STA의 수를 1부터 50까지 늘렸으며, STA의 스캐닝 시작 시간을 1ms씩 증가시키며 AP와 연결되기까지의 시간을 측정하였다. Fig. 6와 같이 두 번째 실험의 결과는 STA의 수가 40개까지 늘어날 동안에는 연결시간이 점차 지속적으로 증가하다가 STA 수가 50개가 되었을 때는 급격히 시간이 증가하면서 그래프가 대략적으로 지수함수적인 증가의 형태를 나타내었다. 결과 값은 FLAP은 평균 91.19ms이고 제안 프로토콜은 평균 62.10ms로, 두 번째 실험의 경우 본 논문에서 제안한 프로토콜이 기존의 제안된 것보다 AP와의 연결시간이 평균 약 29ms 만큼 단축된 것을 알 수 있다. 또한 첫 번째 실험과 마찬가지로 제안 프로토콜의 측정시간이 FLAP에 비해 전체적으

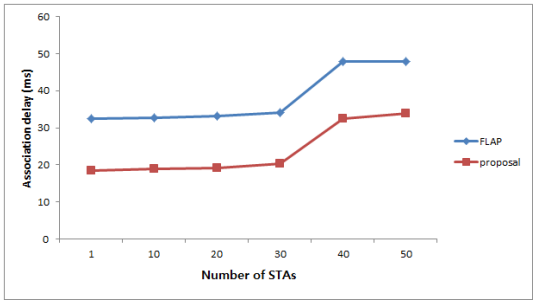


Fig. 5. Association delay simulation result 1 of FLAP and proposed protocol

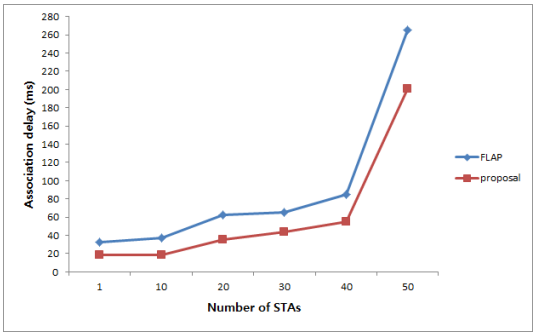


Fig. 6. Association delay simulation result 2 of FLAP and proposed protocol

로 아래쪽에 분포하고 있다.

세 번째 실험에서 STA의 수는 앞의 실험들과 동일하며 STA들이 AP와 연결을 수행하는 과정 위에 CBR(Constant Bit Rate)로 트래픽을 발생시키고 UDP를 통해서 특정 STA에 전달하여 해당 STA에서 받는 패킷의 양을 측정하여 처리율을 계산하였다. CBR 응용은 0.01s 당 1024바이트의 패킷을 생성하도록 설정하였다. Fig. 7과 같이 STA의 수가 10개까지는 FLAP과 제안한 프로토콜이 차이를 보이지 않다가 20개부터 STA 수가 점차 늘어날수록 제안한 프로토콜에 비해 FLAP에서의 처리율이 급격히 떨어지는 것을 볼 수 있다. 처리율은 FLAP이 평균 752436.48bps이고 제안 프로토콜이 평균 795153.31bps로 나타났다. 이는 본 논문에서 제안한 프로토콜에서 STA와 AP 연결 과정을 위해 교환되는 메시지의 수를 줄였기 때문에, 특정 STA이 동일한 시간 동안 지속적으로 생성되는 패킷을 받는 양과 처리율이 기존의 FLAP 보다 높게 유지되는 것임을 알 수 있다.

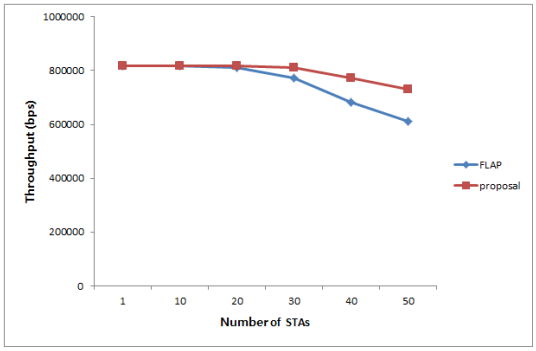


Fig. 7. Throughput comparison between FLAP and proposed protocol

첫 번째 실험과 두 번째 실험을 통하여 스캐닝 시작 시간에 상관없이 본 논문에서 제안한 프로토콜이 기존의 FLAP 보다 STA이 AP에 연결되기까지의 시간이 단축되었다는 것을 알 수 있다. 또한 STA와 AP 사이의 교환하는 메시지의 수가 감소함에 따라 STA의 패킷 처리율이 보다 높게 유지됨을 세 번째 실험을 통해 확인했다.

VI. 결 론

모바일기기의 수요급증과 더불어 WLAN의 활용범위가 넓어짐에 따라 현 표준인 802.11i의 초기 링크 셋업 과정은 네트워크 연결 지연문제를 발생시켰다. 이러한 문제를 해결하고자 많은 연구들이 진행되고 있지만 아직까지 확실한 해결책을 제시하진 못하였다.

본 논문에서는 STA이 802.11i기반의 특정 ESS 영역으로 들어와 AP와 연결 할 경우, 연결 과정에 필요한 메시지의 개수를 기존의 제안된 연구들보다 훨씬 효과적으로 줄인 신속한 초기 링크 셋업 과정 프로토콜을 제안하였다. 본 논문에서 제안한 프로토콜에서는 *Probe Response* 메시지에 AP가 생성한 *ANonce*를 탑재하여 보내는 방식을 채택하여 세션 키 생성 및 인증 과정에 필요한 메시지 개수를 줄였으며, *F*값 한 개로 STA와 AS 상호인증이 가능하게 하였다. 그리고 802.11i의 4-way Handshake의 기능과 목적을 단 4개의 메시지에 담아내고 802.11ai에 적합한 인증방식인 PSK 기반 인증을 채택하여 STA와 AP와의 연결과정을 기존의 표준과 동등한 수준의 보안을 제공하면서도 보다 간단하고 빠르게 하였다.

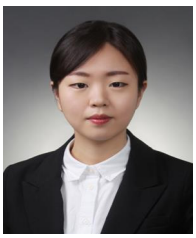
References

[1] IEEE Standard 802.11, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications," IEEE, IEEE std 802.11(Revision of IEEE std 802.11-1999), June. 2007.

[2] IEEE Standard 802.11b, "Higher- Speed Physical Layer Extension in the 2.4 GHz Band, Supplement to IEEE Standard for Information Technology-Telecommunications and Information

Exchange between Systems-Local and Metropolitan Area Networks-Specific Requirements-Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," IEEE, Sep. 1999.
〔3〕 P. C. Mehta, "Wired Equivalent Privacy Vulnerabilities," SANS Institute 2000-2002, Security Essentials Track, Apr. 2001.
〔4〕 IEEE Standard 802.11i, "Medium Access Control (MAC) Security Enhancements, Amendment 6 to IEEE Standard for Information Technology - Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications," IEEE, July. 2004.
〔5〕 Hongquiang Zhai, Yuguang Fang, "Performance Analysis of IEEE 802.11 Mac Protocols in Wireless LANs," Wireless Commun. Mob. Comput, vol. 4, no. 8, pp. 917-931, 2004.
〔6〕 P. Chatzimisios, A. Boucouvalus, and V, Vitsas, "Packet Delay Analysis of the IEEE 802.11 MAC Protocol," Electronics Letter, vol. 39, no. 18, pp. 1358-1359, 2003.
〔7〕 IEEE 802.11ai Draft Standard, "Draft Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications - Amendment - Fast Initial Link Setup," IEEE, Sep. 2014.
〔8〕 Hiroshi Mano, "802.11ai - Improving WLAN System Performance," IEEE 802.11 Documents, Nov. 2013.
〔9〕 Eng Hwee Ong, "Performance Analysis of Fast Initial Link Setup for IEEE 802.11ai WLANs" IEEE Personal Indoor and Mobile Radio Communications (PIMRC), pp. 1279- 1284, Sept. 2012.
〔10〕 C. He, C. Mitchell, "Analysis of the 802.11i 4-way Handshake," in Proc. of the 3rd ACM workshop on Wireless Security (WiSe'04), pp. 43-50, Oct. 2004.
〔11〕 Xinghua Li, Fenye Bao, Jianfeng Ma, "FLAP: An Efficient WLAN Initial Access Authentication Protocol," IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 2, pp. 488-497, Feb. 2014.

〈저자소개〉



김 민 희 (Min-hee Kim) 학생회원
2014년 2월: 단국대학교 컴퓨터과학과 졸업 학사
2014년 3월~현재: 단국대학교 소프트웨어보안 석사 과정
〈관심분야〉 정보보호, 무선 네트워크 보안

박 창 섭 (Chang-seop Park) 종신회원
1983년 2월: 연세대학교 경제학과 졸업
1987년 2월: Lehigh University 컴퓨터과학과 석사
1990년 2월: Lehigh University 컴퓨터과학과 박사
1990년 3월~현재: 단국대학교 소프트웨어학과 교수
〈관심분야〉 정보보호, 네트워크 보안, 무선 인터넷 및 모바일 컴퓨팅 보안