情報保護學會論文誌
第19卷 第6號, 2009. 12

고속의 802.11 핸드오프를 지원하는 CAPWAP 아키텍처를 이용한 티켓 기반의 인증 메커니즘*

박 창 섭,† 우 병 덕‡
단국대학교

A Ticket-based Authentication Mechanism Suitable for Fast 802.11 Handoff which use CAPWAP Architecture*

Chang-seop Park,† Byung-duk Woo‡
Dankook University

요 약

최근 IEEE 802.11n 표준의 상용화와 함께 무선랜 환경에서 실시간 멀티미디어 서비스를 이용하려는 수요가 증가하고 있다. 그러나 IEEE 802.11i 보안표준에서 정의한 IEEE 802.1x 인증과정은 끊김 없는 실시간 멀티미디어 서비스를 제공하기에는 핸드오프 지연시간이 너무 길다. 본 논문은 고속의 핸드오프를 지원하기 위해 CAPWAP (Control And Provisioning Wireless Access Point) 아키텍처를 이용한 티켓 기반의 핸드오프 메커니즘을 소개한다.

ABSTRACT

Recently, there is an increase in demand of real-time multimedia service in the WLAN environment, with a commercialization of IEEE 802.11n standard. However, the 802.1x authentication protocol is too slow to provide seamless real-time multimedia service, which defined in an IEEE 802.11i security standard. In this paper, a Ticket-based authentication mechanism in the CAPWAP(Control And Provisioning Wireless Access Point) architecture is introduced to support for the fast handoff.

Keywords: IEEE 802.11i, WLAN, Fast handover, CAPWAP, 4-Way handshake

I. 서 론

1999년 IEEE 802.11b 표준의 승인 이후부터 현재의 IEEE 802.11n에 이르기까지 무선랜의 기술적 발전은 계속되고 있다. 무선랜은 네트워크 환경 구축 및 변경이 유선랜 환경에 비해 용이하다는 장점은 있으나 낮은 전송 속도 때문에 도입 초기 사용자들의 관심이 크지는 않았다. 그러나 최근 들어 최고 320Mbps의 속도를 지원하는 IEEE 802.11n표준의 등장으로 인해 기업의 사무실, 대학 캠퍼스, 산업용 창고 등 다양한 분야에서 광범위하게 IEEE 802.11 기반의 무선랜 사용이 증가하고 있다. 또한 유선랜 환경에 뒤지지 않는 전송속도는 무선랜을 통한 VoIP(Voice over Internet Protocol)나 MoIP(Multimedia over Internet Protocol)와 같은 실시간 멀티미디어 서비스의 이용을 가능하게 했다.

이처럼 다양한 분야에서 무선랜을 이용하여 실시간 멀티미디어 서비스를 이용하려는 사용자들의 움직임이 활발한 가운데, 무선랜에서 안전하고 빠른 핸드오

접수일(2009년 8월 13일), 수정일(2009년 10월 13일),
게재확정일(2009년 10월 26일)
* 본 논문은 2008년도 단국대학교 대학원 연구보조장학금 지원으로 연구되었음.
† 주저자, csp0@dankook.ac.kr
‡ 교신저자, sayttre@dankook.ac.kr

프(Handoff)는 끊김 없는 실시간 멀티미디어 서비스 제공을 위해 가장 중요하게 고려해야 할 부분으로 대두되고 있다. 무선랜 표준화 초기 단계에서부터 계속되던 인증과 무선구간 데이터 보안에 대한 연구는 IEEE 802.11i의 보안표준을 통해 무선랜에서의 데이터 프라이버시 기능을 더욱 강화하였다[1,2]. 그러나 IEEE 802.11i의 필수구현 항목인 IEEE 802.1x EAP-TLS인증과정은 MS(Mobile Station)의 핸드오프 시 마다 다수의 메시지교환을 수반하는 EAP-TLS인증과정을 이용하여 MS와 AP(Access Point)간 상호인증을 수행하기 때문에 이 과정 중 발생하는 핸드오프 지연시간은 무선랜에서 끊김 없는 실시간 멀티미디어 서비스를 제공하는데 커다란 문제점으로 남아있다[3]. 이를 해결하기 위해 IEEE 802.11f의 IAPP(Inter Access Point Protocol)[4], IEEE 802.11i의 선 인증 방식과 키 캐싱 방식, IEEE 802.11r[5] 표준안의 제정 등 다양한 무선랜 표준들이 제안되었고 PKD(Proactive Key Distribution)방식등과 같은 선 인증 기법에 대한 연구가 계속되고 있다. 그러나 이들 표준에서 제안하고 있는 방식이나 다양한 선 인증 기법들은 선 인증 과정에서 인증 서버의 로드를 증가시키고 제약적인 범위에서만 선 인증이 가능하다는 문제점을 남기고 있다.

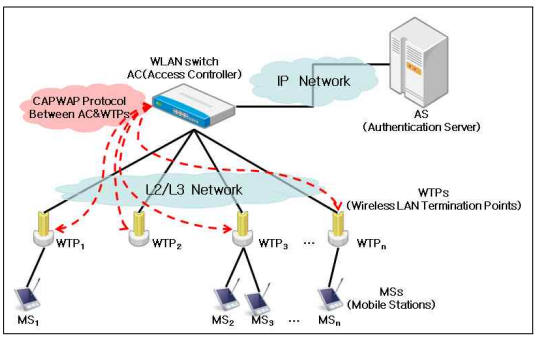
본 논문에서는 안전하고 빠른 핸드오프를 지원하고 불필요한 메시지 전달을 최소화 하여 인증서버의 로드를 감소시키기 위해 무선랜 구성요소에 AC(Access Controller)를 추가한 CAPWAP 아키텍처를 이용한 티켓기반의 인증 메커니즘을 제안한다. CAPWAP 아키텍처를 그대로 이용할 경우 AC또한 전통적인 무선랜 환경의 AS(Authentication Server)처럼 핸드오프과정 중 인증에 따른 로드가 집중될 수 있기 때문에 본 논문에서는 CAPWAP 아키텍처에서 AC에 집중되는 인증 및 접근제어의 기능 중 세션 키 도출 과정을 AP로 분산시켜 AC의 로드를 감소시킨다[6].

본 논문은 다음과 같은 구성으로 제안하고자 하는 메커니즘을 설명한다. 2장에서는 본 논문에서 제안하는 메커니즘의 기본 네트워크 환경인 CAPWAP 아키텍처에 대해 설명한다. 3장에서는 본 논문에서 제안하고 있는 메커니즘과 비교분석의 대상이 되는 사전 키 분배 기반의 인증 메커니즘 (Proactive Key Distribution)에 대해 설명한다. 4장에서는 본 논문이 제안하는 CAPWAP 아키텍처에서 AC(Access Controller)를 이용하는 티켓기반의 인증 메커니즘을 설명한다. 2장 및 3장과 4장에서 언급하는 핸드오프는 MS가 동일한 ESS(Extended Service Set)에 소속된 2개의 상이한 BSS(Basic Service Set)간을 로밍(Roaming)할 경우에 수행되는 2-계층에서의 핸드오프를 지칭한다. 5장은 3장에서 설명한 사전 키 분배 기반의 인증 메커니즘과 본 논문에서 제안하고 있는 티켓기반의 인증 메커니즘의 성능을 Random Waypoint 기반의 시뮬레이션 프로그램을 통해 비교분석 한다. 5장의 성능 비교분석 후 6장을 통해 본 논문의 결론을 맺는다.

II. CAPWAP 무선랜 아키텍처

CAPWAP(Control And Provisioning Wireless Access Point) 아키텍처는 IETF(internet Engineering Task Force)에서 발표한 무선랜 표준으로써 엔터프라이즈(Enterprise) 무선랜 환경을 지원하기 위한 프로토콜이다[6]. IEEE 802.11에서 명시하고 있는 전통적인 무선랜 환경은 AS(Authentication Server), AP(Access Point), MS(Mobile Station) 총 3개의 컴포넌트로 구성된다. 이때 AP는 물리 계층(Physical Layer)과 MAC계층(Medium Access Control Layer)으로 구성된다. CAPWAP 아키텍처는 전통적인 무선랜 환경의 FAT-AP의 기능을 물리계층과 MAC계층의 두 가지로 분리하여 WTP(Wireless LAN Termination Point)와 AC(Access Controller)라는 새로운 물리적 구성 요소를 추가 하였다. CAPWAP 무선랜 아키텍처는 [그림 1]과 같다.

WTP는 기존 FAT-AP의 MAC계층의 기능 중 일부분과 물리계층의 기능을 THIN-AP로 구현한 일종의 무선 안테나로 IEEE 802.11 물리계층 기능을 담당하는 장치이다. AC는 기존 FAT-AP의 MAC계층

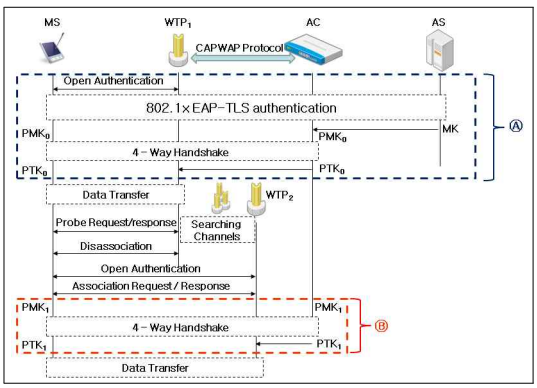


[그림 1] CAPWAP 무선랜 아키텍처

기능을 중앙에서 통합 관리하기 위해 엔터프라이즈 무선랜 환경에서 도입한 물리적 구성 요소로서 엔터프라이즈 무선랜을 구성하고 있는 모든 AP의 MAC기능은 AC를 통해 중앙에서 직접 관리한다. 이렇게 기능을 양분화 한 뒤 WTP는 무선네트워크에서 데이터 전송과 수신을 담당하는 무선안테나 역할을 하고 AC는 IEEE 802.11의 인증 및 접근제어 부분을 담당한다. 이와 같은 기능의 양분화는 Client(MS)가 최초 인증과정을 거친 후 무선네트워크 서비스를 이용하다가 새로운 WTP로 로밍 할 때 802.1x EAP-TLS인증과정 없이 새로운 WTP에 접속하여 서비스를 계속 이용할 수 있도록 하여 고속의 핸드오프를 지원한다[7].

본 논문에서 제안하는 티켓 기반의 인증 메커니즘의 경우 CAPWAP 무선랜 아키텍처에서 AC를 이용하여 티켓을 생성하고 분배하여 고속의 핸드오프를 지원한다. 이와 관련하여 CAPWAP 무선랜 아키텍처에서 WTP와 AC사이에 사용되는 CAPWAP 프로토콜은 본 논문에서 제시하는 메커니즘과는 직접적인 연관이 없고 단지 티켓을 전송하는 역할만 지니기 때문에 CAPWAP 프로토콜에 대한 자세한 설명은 생략하고 제안 메커니즘은 WTP와 AC사이에 안전한 채널이 존재함을 가정하고 설명한다.

[그림 2]의 Ⓐ는 CAPWAP 아키텍처에서 MS의 최초 인증과정을 통한 세션 키 도출 과정을 보여주고 있다. CAPWAP 아키텍처에서 AC는 인증자(Authenticator)로 사용된다. 최초 인증과정 동안 MS와 AS는 WTP_1과 AC를 매개체로 이용하여 IEEE 802.11i에서 명시하고 있는 802.1x EAP-TLS인증과정을 통해 PMK_0(Pairwise Master Key)을 도출한다. 이렇게 도출된 PMK_0는 AS에서 AC로 전달되고 AC



[그림 2] CAPWAP 무선랜 아키텍처에서 MS의 최초 인증 및 세션 키 도출 과정

는 WTP_1을 매개체로 MS와 4-Way Handshake과정을 진행하여 PTK_0(Pairwise Transient Key)를 생성한다. PTK_0생성 후 AC는 CAPWAP 프로토콜을 이용하여 PTK_0를 WTP_1으로 전송한다. 세션 키 도출의 모든 과정이 완료 된 후 MS는 WTP_1을 이용하여 무선네트워크 서비스를 이용하기 시작한다.

MS가 새로운 WTP로 핸드오프 하는 과정은 [그림 2]의 Ⓑ와 같다. WTP_1로부터 무선네트워크 서비스를 제공받던 MS는 새로운 WTP로 로밍하기 위해 Probe Request/Response 과정을 통해 이용 가능한 WTP_2를 발견한다. MS는 WTP_2와 사용할 세션 키를 새롭게 도출해야 하는데 이때 CAPWAP 아키텍처에서는 802.1x EAP-TLS인증과정 없이 AC가 PMK를 도출하여 AC와 MS사이의 4-Way Handshake 과정을 바로 진행한다. 이때 AC가 PMK를 도출하는 방법은 크게 두 가지 방식으로 나뉜다. 첫 번째 방법은 최초 인증 시 도출했던 PMK_0를 재사용하는 방법이다. [그림 2]의 하단 부분을 보면 Probe Request/Response 과정을 통해 이용 가능한 WTP_2를 발견한 MS는 현재 접속하고 있는 WTP_1과의 접속을 Disassociation과정을 통해 해지하고 WTP_2로 Association Request 메시지를 보낸다. MS로부터 Association Request 메시지를 전달받은 WTP_2는 해당 MS와 최초 인증 때 사용했던 PMK_0를 이용하여 WTP_2를 경유해서 MS와 4-Way Handshake과정을 바로 실행하고 이를 통해 새로운 세션 키 PTK_1을 도출한다. 두 번째 방법은 기존에 사용했던 PMK_0를 기반으로 PMK_1을 생성하여 사용하는 것이다. 첫 번째 방식과 동일하게 WTP_2를 발견한 MS는 현재 접속하고 있는 WTP_1과의 접속을 Disassociation과정을 통해 해지하고 WTP_2로 Association Request 메시지를 보낸다. MS로부터 Association Request 메시지를 전달받은 WTP_2 는 다음과 같은 식 (1) PMK도출 알고리즘을 이용하여 PMK_1 을 도출한다.

$$PMK_n = TLS-PRF(MK,\ PMK_{n-1}\ AP\_MAC,\ STA\_MAC) \quad (1)$$

위 식과 같이 AC는 PMK_1을 생성하기 위해 최초 인증 시 도출 한 PMK_0을 이용하여 새로운 PMK_1을 생성한다. PMK_1을 생성한 AC는 곧바로 MS와 4-Way Handshake과정을 실행하고 이를 통해 새로운 세션 키 PTK_1을 도출한다. 이렇게 생성된 세션 키 PTK_1은 CAPWAP 프로토콜을 이용하여 AC에서

WTP_2로 전달되고 MS는 WTP_2를 이용하여 계속해서 무선네트워크 서비스를 제공받게 되다. 본 논문에서는 CAPWAP 아키텍처를 설명하는데 있어서 두 번째 방식에 기준을 두었다. 이는 PMK의 Freshness를 보장하면서도 빠른 핸드오프를 지원할 수 있는 방식이기 때문이다. 두 가지 방법모두 전통적인 무선랜 환경에서 요구하는 802.1x EAP-TLS인증과정 없이 PMK를 도출하기 때문에 핸드오프지연시간을 단축시킬 수 있다.

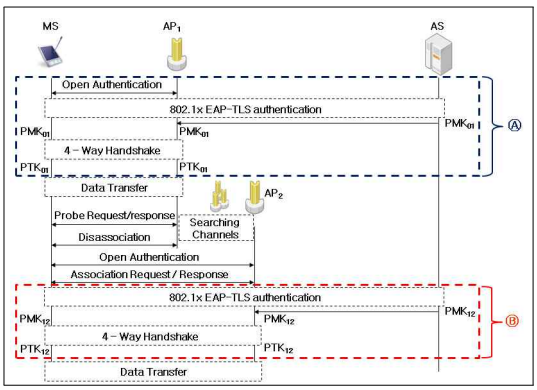
CAPWAP 무선랜 아키텍처를 이용할 경우 전통적인 무선랜 환경보다 고속의 핸드오프를 보장 받을 수는 있지만 AC에 집중되는 인증 및 접근제어에 관한 부하는 전통적인 무선랜 환경의 AS에 집중 되었던 부하와 다를 바 없다. 이는 최초 인증 과정을 제외하고 로밍과정 중 발생하는 모든 인증 및 세션 키 도출 과정에 AC가 관여하기 때문이다. 본 논문에서는 이러한 문제점을 해결하기 위해 CAPWAP 무선랜 아키텍처에서 AC의 기능 중 세션 키 도출에 관한 부분은 WTP에게 전담시킴으로써 AC의 부하를 감소시킨다.

III. 사전 키 분배 기반의 인증 메커니즘 (Proactive Key Distribution)

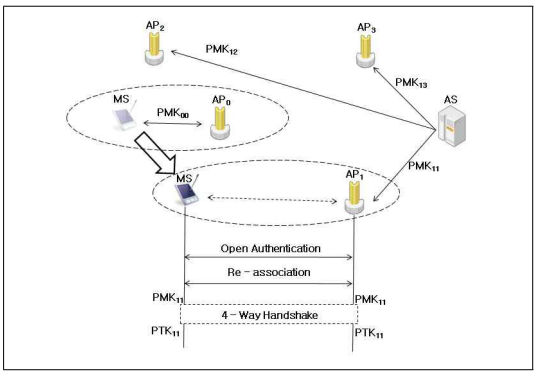
PKD(Proactive Key Distribution)방식은 NG(Neighbor Graph)라 불리는 향후 접속을 시도할 가능성이 있는 후보 AP들과 인증 작업을 사전에 수행하여 핸드오프 지연시간을 단축시키는 선 인증기법 중 하나이다[8,9]. 전통적인 IEEE 802.11 무선랜 환경의 경우 MS가 새로운 AP로 로밍 할 때 IEEE 802.11i 보안 정책에 따라 802.1x EAP-TLS인증과정을 수행하고 4-Way Handshake를 통해 새로운 AP와 사용 할 세션 키 PTK를 도출해 낸다. [그림 3]은 전통적인 무선랜 환경에서 MS가 AP_1을 통해 최초 인증을 진행 한 후 서비스를 이용하는 시점부터 새로운 AP_2로 핸드오프 하는 과정을 보여주고 있다. MS가 AP_1을 이용하여 무선랜 서비스를 이용하기 위해서는 [그림 3]의 Ⓐ와 같이 802.1x EAP-TLS인증과정을 통해 PMK_{01}을 도출한 후 4-Way Handshake를 통해 PTK_{01}를 생성한다.

PTK_{01}을 이용하여 무선랜 서비스를 이용하던 MS는 Probe Request / Response 과정을 통해 AP_2를 향후 핸드오프 할 AP(Target AP)로 선정 한 후 [그림 3]의 Ⓑ와 같이 핸드오프를 진행 한다[10]. 이때 또 다시 수행되는 802.1x EAP-TLS인증과정에서 발생하는 핸드오프 지연시간은 끊김 없는 무선랜 서비스를 제공하는데 큰 문제점이 되고 있다. 이러한 문제점을 해결하기 위해 제안된 PKD방식은 NG라 불리는 향후 접속을 시도할 가능성이 있는 후보 AP들을 선정하여 MS의 인증정보를 선 분배시키는 방식으로 NG 영역 내의 AP들은 한 MS의 사전인증을 위해 분배된 키를 서로 다른 형태로 보유하고 있다. [그림 4]는 NG를 이용한 PKD 방식에서 MS의 핸드오프 시 발생하는 선 인증과정을 보여 주고 있다. MS는 무선랜 서비스를 이용하기 위해 AP_0로 최초 접속을 시도할 때 802.1x EAP-TLS인증과정을 통해 PMK_{00}를 도출한 후 이것을 이용하여 PTK_{00}를 생성하여 무선랜 서비스를 이용하게 된다.

PTK_{00}도출 후 AS는 AP_0의 NG 정보를 이용하여 MS가 다른 AP로 핸드오프 하기 전에 AP_0의 NG 내에 있는 AP들([그림 4]의 AP_1,AP_2,AP_3)에게 MS와 공유할 PMK_{ij}(i: MS의 association 순서, j: A



[그림 3] IEEE 802.11 무선랜 표준에 명시된 MS의 최초 인증 및 핸드오프과정



[그림 4] PKD 방식에서 제안하는 선 인증 과정

P번호), 즉 PMK_{11},PMK_{12},PMK_{13}를 계산 후 전달한다. 추후 MS가 AP_0의 NG 내에 있는 AP_1의 영역으로 로밍 할 경우 이미 AS로부터 전달 받은 PMK_{11}이 있기 때문에 802.1x EAP-TLS인증과정을 거치지 않고 바로 4-Way Handshake를 통해 PTK_{11}을 도출 할 수 있다. 하지만 사용자의 인증정보를 한 홉 단위 거리의 AP들에 대해서만 분배되어 NG 영역 이외의 AP로 MS가 핸드오프를 할 경우, 또 다시 802.1x EAP-TLS인증과정을 진행 하게 되어 고속의 핸드오프를 지원 할 수 없으며, 핸드오프 시 Target AP를 제외한 NG 리스트에 있던 AP들은 불필요한 키를 저장해야 하며 서버 또한 불필요한 키를 계산하고 AP들에게 전송하게 되어 서버의 부하를 가중 시키는 문제점이 있다.

Ⅳ. 티켓 기반의 인증 메커니즘

본 논문은 CAPWAP 아키텍처에서 MS의 핸드오프 시 무선랜 보안 표준인 802.11i에 명시되어 있는 MS와 AP간 상호인증 및 PMK도출 프로토콜을 개선하여 고속의 핸드오프를 제공하는 메커니즘을 제안한다.

4.1 설계 원리

IEEE 802.11 무선랜에서는 MS가 새로운 AP로 핸드오프 할 때 802.1x EAP-TLS인증과정을 통해 PMK를 도출하고 802.11i보안 표준에 명시되어 있는 것처럼 4-Way Handshake를 통해 새로운 세션키 PTK를 분배한다. 이때 MS와 AP를 경유한 AS사이의 상호인증 및 PMK도출을 위한 802.1x EAP-TLS인증과정에서 발생하는 지연시간은 끊김 없는 실시간 멀티미디어 서비스를 제공하는데 커다란 문제점으로 남아있다. 이를 개선하기 위해 다양한 재인증 기법들이 연구되었다. 802.11i에서 제안하고 있는 선 인증 방식은 MS가 현재 접속된 AP를 통해 향후 핸드오프 할 AP들에 대한 사전인증을 시도하는 방식으로 사전인증을 통해 생성된 PMK와 MS와의 관계는 PMKID(PMK Identity)로 식별이 가능하다. 그러나 선 인증 방식은 현재 접속해 있는 AP를 통해 향후 접속 가능한 AP들과 모두 사전인증을 하기 때문에 Target AP를 제외한 사전인증이 진행된 AP들의 PMK를 계산하고 전송하는 과정에서 인증서버에 부하를 가중시킨다. 또한 사전인증이 진행된 AP외에 다른 AP로 MS가 핸드오프 할 경우 802.1x EAP-TLS인증과정을 다시 수행해야 하고 이는 상당한 핸드오프 지연시간을 발생시킨다는 문제점을 가지고 있다.

802.11f에서 제안하고 있는 IAPP는 AP간 2계층 전달 정보 및 AP의 Security Context 정보를 공유함으로써 MS의 신속한 이동을 지원할 수 있는 프로토콜로 MS와 둘 이상의 AP, DS(Distribution System), 인증서버로 구성된 환경에서 동작한다. 이처럼 서로 다른 AP간의 정보교환을 통한 방식은 단말의 Context 정보를 교환함으로써 핸드오프 시 인증에 걸리는 지연시간을 줄일 수 있다는 장점이 있지만 AP상호간 보안상의 독립성을 보장해 주지 못하기 때문에 특정 AP 한곳의 Security Context정보가 노출될 경우 IAPP를 통해 연결된 주변 AP들 또한 연쇄적으로 공격받을 수 있다는 문제점을 내포하고 있다.

3장에서 설명한 PKD방식은 NG를 이용하여 MS의 인증정보를 선 분배시키는 방식을 제안하고 있다. PKD 방식은 현재 접속되어 있는 AP의 NG영역 내의 AP들이 MS의 사전인증을 위해 분배된 키를 서로 다른 형태로 보유하고 있으므로 동일한 인증정보를 가지는 위험성을 제거하였다. 이때 PKD방식에서는 서로 다른 키를 생성하기 위하여 하기의 PMK도출 알고리즘을 사용한다.

$$PMK_0 = TLS-PRF(MK, clientHello.random, serverHello.random) \quad (2)$$

$$PMK_n = TLS-PRF(MK, PMK_{n-1}, AP\_MAC, STA\_MAC) \quad (3)$$

MS가 무선네트워크 서비스를 최초 이용하는 시점에 접속한 AP와 802.1x EAP-TLS인증과정을 통해 PMK를 생성할 때는 식 (2)를 사용하여 PMK_0를 생성한다. 이는 전통적인 IEEE 802.11에서 명시하고 있는 PMK도출 알고리즘과 동일하다. 그러나 MS의 최초 무선네트워크 접속이후 현재 접속한 AP의 NG를 이용하여 향후 핸드오프 할 가능성이 있는 AP들에게 사전인증을 위해 PMK를 분배할 때는 식 (3)의 알고리즘을 이용하여 802.1x EAP-TLS인증과정 없이 신속하게 PMK를 계산해 낸다. 이처럼 PKD방식은 사전인증과정에 NG와 개선된 PMK도출 알고리즘을 사용함으로써 PMK의 Key Freshness를 유지하면서도 신속한 핸드오프를 지원한다. 하지만 PKD방식

또한 3장에서 설명한 것과 같이 MS의 로밍 시 Target AP를 제외한 NG 리스트에 있던 AP들은 불필요한 키를 저장해야 하며 서버 또한 불필요한 키를 계산하고 AP들에게 전송하게 되어 서버의 부하를 가중 시키는 문제점이 있다. 이처럼 현재까지 연구된 대표적인 재인증 및 고속의 핸드오프를 지원하기 위한 프로토콜들이 제안하는 메커니즘과 이들 메커니즘들이 내포하고 있는 문제점들을 분석해보면 안전하고 빠른 핸드오프를 지원하기위한 기본적인 요구사항을 다음과 같이 도출 할 수 있다. 첫째 사전인증을 위한 키 계산 및 전송과정을 최소화 하여 인증서버의 부하를 낮춰야 한다. 둘째 IAPP프로토콜과 같이 AP상호간 보안 독립성을 유지하지 못할 경우 특정 AP의 PMK 노출로 인한 연쇄적인 공격이 발생 할 수 있다. 이를 방지하기 위해 AP상호간 보안 독립성을 유지시켜야 한다. 셋째 MS와 AP사이의 인증 및 데이터 전송 중 사용할 키의 Key Freshness를 유지해야 한다.

본 논문은 위의 3가지 기본적인 요구사항에 초점을 맞추어 고속의 핸드오프를 지원하기 위해 CAPWAP 아키텍처에서 AC를 이용하는 티켓기반의 인증 메커니즘을 제안한다. CAPWAP 아키텍처의 물리적 구성요소인 AC가 인증 및 접근제어에 관한 기능을 처리하여 인증서버의 부담을 낮추고, 티켓 이라는 새로운 개념을 도입하여 인증관련 정보를 MS로 전달함으로써 기존 선 인증 방식에서 발생하는 문제점들을 해결하고자 한다. 또한 PMK도출 알고리즘을 PKD방식에서 제안하고 있는 식 (2)와 식(3)의 방식을 따름으로써 안전하면서도 빠른 핸드오프를 지원 하는 메커니즘을 제안한다.

4.2 제안 메커니즘

본 논문에서 제안하고 있는 티켓기반의 인증 메커니즘은 전통적인 무선랜 환경을 구축하는 MS, AP, AS 이외에 새로운 물리적 구성요소인 AC를 추가한 CAPWAP 아키텍처를 기반으로 한다. AC는 인증 및 접근제어와 관련된 기능을 담당함으로써 인증서버의 부담을 감소시키는 역할을 한다. 또한 인증 관련 정보를 MS로 전달하기 위해 본 논문에서 제안하고 있는 티켓을 생성하여 AP를 통해 MS로 전달하는 기능도 AC가 전담한다. 티켓은 NG를 이용하여 미리 계산된 PMK를 AC와 해당 티켓을 받게 되는 AP들 사이에 공유된 대칭형 암호를 이용하여 암호화한 결과로써 MS가 새로운 WTP로 핸드오프 할 때 대상이 되는 WTP(Target WTP)로 미리 계산된 PMK를 안전하게 전달하는데 사용되는 새로운 개념이다. 본 논문에서 제안하고 있는 PMK 도출 알고리즘과 티켓 생성 알고리즘은 다음과 같다.

$$PMK_{0j=prf(MK}, client.random, server.random) \quad (4)$$

$$PMK_{ij} = prf(MK,\ MS,\ WTPj, PMK_{(i-1)j}) \quad (5)$$

$$Ticket_j = [MS,\ PMK_{ij},\ Lifetime]K_j \quad (6)$$

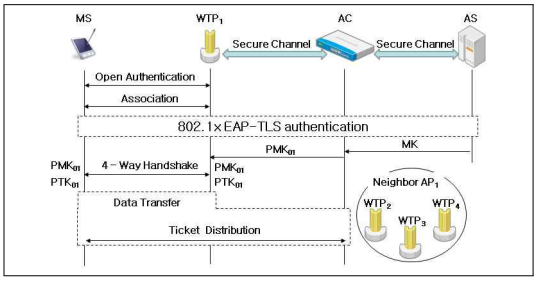
[표 1] 기호 설명

PMK_{0j}	MS의 최초 association시 생성되는 PMK로써 0은 최초 인증 시 생성된 PMK임을 나타낸다. j는 WTP번호로써 WTP의 고유 식별 번호로 사용된다.
PMK_{ij}	인증과정에서 생성되는 PMK로써 i는 Re-association 횟수를 나타낸다. j는 WTP번호로써 WTP의 고유 식별 번호로 사용된다.
prf	Pseudo random function의 약어
MK	MS의 최초 association시 AS(인증서버)에서 생성하는 pre-Master Key로써 PMK계산을 위해 사용되는 키이다.
$Ticket_j$	MS와 WTP가 공유할 PMK를 WTP와 AC가 공유한 대칭키로 암호화한 결과 j는 WTP번호로써 WTP의 고유 식별 번호로 사용된다.
Lifetime	Ticket을 구성하는 속성으로써 Ticket의 유효기간을 표시한다.
K_j	$Ticket_j$를 생성할 때 사용하는 대칭 키로써 j는 WTP의 고유 식별 번호로 사용된다.

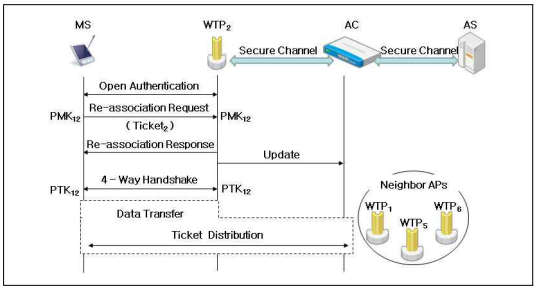
[그림 5]는 본 논문에서 제안하고 있는 프로토콜 중 MS가 IEEE 802.11 무선랜 서비스를 최초 이용할 때 발생되는 상호인증 및 세션 키 도출 과정, 세션 키 도출 후 티켓 분배 과정을 보여주고 있다. 본 논문에서 제안하고 있는 프로토콜은 WTP와 AC, AC와 AS사이에는 안전한 채널이 존재한다고 가정한다. MS는 WTP_1과 최초 접속 작업 후 AS와 802.1x EAP-TLS인증과정을 진행 하고 이를 통해 상호인증 및 MK(pre-Master Key)를 도출한다.

MK는 안전한 채널을 통해 AC로 전달되고 MK를 전달 받은 AC는 식 (4)를 이용하여 하기와 같이 PMK_{01}을 도출한다.

$$PMK_{01} = prf(MK,\ clientHello.random,\ serverHello.random)$$



[그림 5] 제안 메커니즘의 최초 인증 및 세션 키 도출과정과 Ticket 생성 및 분배과정



[그림 6] 제안 메커니즘의 핸드오프과정

AC는 PMK_{01}을 안전한 채널을 이용하여 WTP_1로 전달하고 PMK_{01}을 전달받은 WTP_1은 PMK를 이용하여 MS와 4-Way Handshake 과정을 진행한다. 정상적으로 4-Way Handshake 과정을 마치면 MS와 WTP_1사이에 새로운 세션 키인 PTK_{01}이 생성되고 이를 이용하여 MS는 WTP_1을 통해 안전한 무선랜 서비스를 이용할 수 있다. PTK_{01}생성 후 데이터 전송(Data Transfer)과정이 이루어지는 동안에 AC는 WTP_1의 NG정보를 이용하여 MS가 향후 핸드오프 할 가능성이 있는 WTP들이 사용할 PMK를 미리 계산한다. [그림 5]에서 WTP_1의 NG는 WTP_2,WTP_3,WTP_4이다. AC는 식 (5)를 이용하여 MS의 핸드오프 시 WTP_1의 이웃 WTP들이 사용할 PMK를 계산한다. 이에 대한 결과는 하기와 같이 PMK_{12}, PMK_{13}, PMK_{14}이다.

$$PMK_{12} = prf(MK, MS, WTP_2, PMK_{01})$$
$$PMK_{13} = prf(MK, MS, WTP_3, PMK_{01})$$
$$PMK_{14} = prf(MK, MS, WTP_4, PMK_{01})$$

WTP_1의 이웃 WTP들에 대한 PMK 계산 작업이 완료되면 AC는 식 (6)을 이용하여 하기와 같이 티켓을 생성한다.

$$Ticket_2 = [MS, PMK_{12}, Lifetime]K_2$$
$$Ticket_3 = [MS, PMK_{13}, Lifetime]K_3$$
$$Ticket_4 = [MS, PMK_{14}, Lifetime]K_4$$

티켓은 MS의 MAC주소와 NG를 이용하여 미리 계산된 PMK, 해당 티켓의 유효기간을 나타내는 Lifetime을 AC와 WTP들 사이에 공유된 대칭키 K를 이용하여 암호화한 결과이다. 이렇게 생성된 티켓은 하나의 데이터 프레임(Data Frame)으로 구성되어 안전한 채널을 통해 AC에서 WTP_1을 경유하여 MS로 전달한다. 티켓 생성과 전달에 관한 일련의 과정은 MS와 WTP_1사이의 데이터 전송과정 중 진행된다. WTP_1을 이용하여 무선네트워크 서비스를 이용하던 MS가 주변의 다른 WTP로 로밍 할 경우 티켓을 이용하여 핸드오프 지연시간을 최소화 할 수 있다. [그림 6]은 MS가 WTP_1에서 WTP_2로 로밍 할 경우 본 논문에서 제안하고자 하는 핸드오프 과정을 보여주고 있다.

WTP_2를 Target WTP로 선정 한 MS는 Re-association 과정을 통해 $Ticket_2$를 WTP_2로 전달한다. WTP_2는 $Ticket_2$를 생성한 AC와 사전에 공유된 대칭키 K를 이용하여 $Ticket_2$를 복호화 하고 복호화된 내용을 이용하여 MS와의 상호인증 작업을 진행한다. 이때 $Ticket_2$를 복호화한 결과 중 MS의 MAC주소를 이용하여 Re-association을 요청한 MS에 대한 인증 작업을 진행하고 Lifetime을 이용하여 해당 $Ticket_2$의 유효성을 판단한다. WTP_2가 정상적으로 티켓의 내부 속성을 이용하여 티켓의 유효성 및 MS에 대한 인증을 완료 하였다면 WTP_2는 $Ticket_2$에 담긴 PMK_{12}를 이용하여 802.1x EAP-TLS인증과정 없이 바로 4-Way Handshake를 진행함으로써 MS와 WTP_2사이에 사용할 세션 키 PTK_{12}를 도출 할 수 있다. PTK_{12}도출 후 MS와 WTP_2사이의 데이터 전송과정 중 AC는 WTP_2의 NG를 이용하여 다음 핸드오프 때 사용할 티켓을 생성한다. 위와 같이 티켓을 이용하여 고속의 핸드오프를 진행하는 가운데 티켓 전송 과정 중 악의적인 공격자에게 티켓이 노출되어 해당 티켓의 재전송 공격이 발생될 가능성이 있다. 그러나 제안 메커니즘이 가지고 있는 기본적인 특성을 종합해 보면 티켓 재전송 공격은 제안 메커니즘에서 어떠한 피해도 발생 시킬 수 없다. 제안 메커니즘이 가지고 있는 기본적 특성은 다음과 같다.

AC가 현재 MS가 접속해 있는 WTP의 NG정보를 이용하여 생성한 티켓들은 WTP와 MS사이의 데이

터 전송 과정에 하나의 데이터 프레임으로 전송된다. 이때 데이터 프레임은 현제 접속되어 있는 WTP와 MS사이의 세션 키로 보호받고 있기 때문에 공격자가 티켓을 중간에 가로챘다 하더라도 티켓 내부의 내용이 노출 될 수 없다. 또한 MS가 로밍을 시도할 때 Target WTP로 전송하는 티켓의 경우 AC와 WTP 사이에 사전에 공유된 대칭키로 암호화 되어 있기 때문에 해당 티켓 메시지 또한 공격자가 중간에 가로챘다 하더라도 티켓 내부의 내용이 노출 될 수 없다. 티켓 내부의 내용이 노출 될 수 없기 때문에 공격자는 가로챈 티켓을 변형 없이 WTP로 재전송할 수밖에 없다. 이렇게 공격자로부터 재전송된 티켓을 전달 받은 WTP는 티켓을 전달 받은 후 이를 사전에 공유된 대칭키를 이용하여 복호화 하고 PTK도출을 위한 4-Way Handshake과정에 돌입한다.

이때 티켓을 전달 받은 WTP가 티켓을 복호화 한 후 해당 티켓에 포함되어 있는 MS의 MAC주소를 이용하여 해당 티켓을 생성한 MS와 4-Way Handshake를 시도하기 위해 4-Way Handshake의 첫 번째 메시지를 MS로 전송할 것이다. 4-Way Handshake의 첫 번째 메시지를 전달받은 MS가 해당 메시지를 전송한 WTP와 이미 세션 키를 도출하여 무선랜 서비스를 제공받고 있었다면 해당 MS는 802.11i에 명시되어 있는 것처럼 4-Way Handshake를 계속 진행하여 새로운 세션 키를 도출 할 것이다. 이는 4-Way Handshake를 통해 도출되는 세션 키의 경우 MS와 WTP사이에서 서로 다른 난수를 발생하여 생성하기 때문에 티켓 내부의 속성 중 PMK가 변질되지 않았다면 티켓 재전송으로 인해 4-Way Handshake가 다시 발생해도 Key Freshness을 유지하면서 정상적으로 세션 키를 도출하여 802.11무선랜 서비스를 계속 유지시킬 수 있으며 이때 발생하는 4-Way Handshake과정은 끊김 없는 무선랜 서비스를 제공하는데 전혀 문제가 없는 진행시간을 가진다.

실제로 전통적인 802.11무선랜 표준에서도 세션 키의 Lifetime이 종료되었을 경우 MS와 WTP사이에 무선랜 서비스가 이루어지고 있는 상황 속에서도 4-Way Handshake과정을 통한 새로운 세션 키 도출 작업을 진행한다고 명시되어있다. 또한 티켓 내부의 Lifetime을 이용하여 티켓의 재전송 공격을 방어할 수 있다. 재전송 공격을 통해 티켓을 전달받은 WTP는 티켓을 복호화 한 후 해당 티켓의 유효성 여부를 판단할 때 티켓의 Lifetime을 확인하여 Lifetime이 초과된 티켓의 경우 유효하지 않은 티켓으로 간주하여 해당 티켓을 폐기한다. 이처럼 본 논문에서 제안하고 있는 티켓기반의 인증 메커니즘은 MS와 WTP사이의 데이터 전송 과정 중 티켓이 전달된다는 특성과 전통적인 802.11 무선랜 표준에서 명시하고 있는 4-Way Handshake의 특성 및 티켓 내부의 Lifetime항목을 이용하여 공격자로부터 티켓의 재전송 공격을 방어할 수 있다.

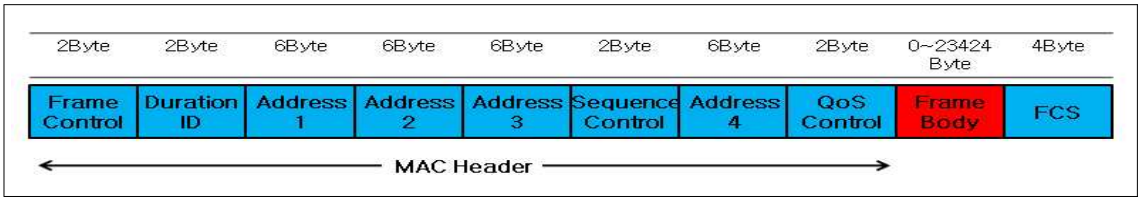
V. 비교분석

우리는 4장을 통해 본 논문이 제안하고 있는 CAPWAP 아키텍처에서 티켓을 이용한 인증기법에 대해 살펴보았다. 5장에서는 기존에 연구된 선 인증기법 중 가장 대표적인 NG를 이용한 PKD 방식과 본 논문에서 제안하고 있는 티켓기반의 인증방식의 성능을 비교분석 한다. 성능의 비교 분석을 위해 Random Waypoint Model을 기반으로 하는 어플리케이션(Application)을 이용하며 비교분석은 MS의 로밍 과정에서 발생하는 네트워크 부하에 초점을 맞추어 AC와 AS가 전송하는 인증 관련 메시지의 개수와 메시지 전송에 따른 전체 데이터 프레임 사이즈를 비교한다.

제안메커니즘에서 AC와 WTP사이에 대칭 키를 사용하여 티켓을 복호화 하는데 소요되는 시간은 대칭키의 특성상 약 6μs(microsecond)의 극히 작은 시간이 소요되고, 일반적인 무선네트워크 환경에서 수시로 발생하는 메시지 전송과정이 항상 동일한 시간 안에 이루어 지지 않기 때문에 대칭 키의 복호화에 소요되는 연산시간은 무시할 수 있는 시간이다. 그렇기 때문에 본 논문에서는 PKD방식과 제안메커니즘과의 비교 분석에서 티켓의 복호화과정 중 발생하는 연산시간이 미치는 영향은 비교 분석을 진행하지 않는다. 비교분석 과정에서 표기되는 AP는 본 논문의 기반 환경이 되는 CAPWAP 아키텍처에서 WTP에 해당한다. PKD방식과 본 논문에서 제안하는 방식의 비교설명과정에서 논문의 가독성을 높이기 위해 해당 용어를 AP로 통일하여 사용하였다.

5.1 모의실험

본 논문에서 제안하고 있는 티켓기반의 인증기법과 NG를 이용한 PKD방식을 비교하기 위해 Random Waypoint Model을 기반으로 하는 어플리케이션을 제작하여 가상의 시뮬레이션 환경을 구축하였다. 기본



[그림 7] MAC Frame format

적인 실험 환경은 [표 2]와 같이 설정하였다. IEEE 802.11 무선 네트워크에서 개체 간 데이터를 전송할 때는 [그림 7]과 같이 MAC 프레임을 구성한다. MAC 프레임은 크게 두 가지 부분으로 구분 할 수 있다. [그림 7]에서 보이는 것과 같이 MAC 헤더(Header) 와 FCS는 항상 고정된 부분으로 총 36Byte의 고정된 영역을 사용하고 프레임바디(Frame body)부분은 전달되는 데이터의 크기에 따라 0 ~ 23424byte만큼 가변적으로 할당되어 전체 MAC 프레임을 구성한다.

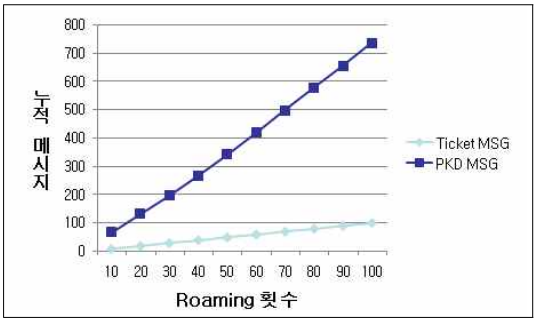
시뮬레이션에서는 하나의 메시지를 전송할 때 [그림 7]과 같이 MAC 프레임의 공통부분은 36byte로 설정한다. 그 외의 프레임바디부분은 [표 2]의 설정에 따라 미리 계산된 PMK는 256bit로 설정하고 티켓은 328bit로 설정하여 실험을 진행 한다.

[표 2] 시뮬레이션 환경 기본 설정

AP개수	100개 (10 * 10)
MS개수	1개
NG형성 방식	1hop 거리 주변 모든 AP
Mobility Model	Random Waypoint Model
Roaming 횟수	100회
PMK Size	256bit
Ticket Size (MS+PMK+Lifetime)	328bit (64 + 256 + 8)
Frame Size	36byte(Common) + Frame body(가변)

[실험 1] Target AP의 NG 개수가 한 홉 거리 내의 모든 AP인 상황에서 PKD 방식과 티켓방식의 인증 메시지 개수 비교

[실험 1]은 Target AP의 한 홉 거리 내의 모든 AP들을 NG로 설정 한 후 [표 2]의 실험환경을 기반으로 MS가 100 회의 로밍을 시도하는 동안 발생하는 인증메시지의 전송개수를 비교하는 실험이다. PKD



[그림 8] [실험 1]의 결과

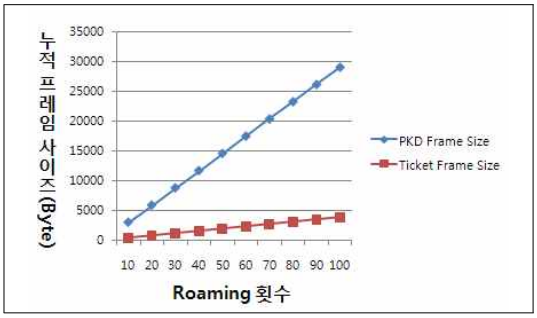
방식의 경우 AS에서 선 인증된 결과를 AP들에게 전송하는 메시지개수를 개수하였고(From AS to APs) 본 논문에서 제안하고 있는 티켓방식에서는 AC에서 MS로 전송하는 인증관련 티켓메시지 개수를 개수하였다(From AC to MS).

[실험 1]의 시뮬레이션 결과는 [그림 8]과 같다. 본 논문에서 제안하고 있는 티켓기반의 인증방식은 로밍이 발생 할 때마다 하나의 인증메시지만을 전송하고 있다. 티켓기반의 인증방식의 경우 NG를 이용하여 미리 계산된 PMK를 티켓으로 변환하고 이를 하나의 데이터 프레임으로 MS로 전달하기 때문에 매회 로밍 시 마다 인증관련 메시지는 한 번 전송된다.

그러나 NG를 이용한 PKD방식의 경우 로밍이 발생 할 때마다 선 인증된 정보를 각 각의 AP들에게 개별적으로 전달함으로써 매회 로밍 시 마다 Target AP의 NG에 소속된 AP의 개수만큼 선 인증 관련메시지를 전송하게 된다.

[실험 2] Target AP의 NG 개수가 한 홉 거리 내의 모든 AP인 상황에서 PKD 방식과 티켓방식의 인증관련 전송메시지의 프레임사이즈(Frame Size)비교

[실험 2]은 Target AP의 한 홉 거리 내의 모든 AP들을 NG로 설정 한 후 [표 2]의 실험환경을 기반



[그림 9] [실험 2]의 결과

으로 100 회의 로밍동안 발생하는 인증관련 전송메시지의 누적 프레임사이즈를 비교하는 실험이다. PKD 방식의 경우 AS에서 선 인증된 결과를 AP들에게 전송하는 선 인증메시지의 프레임사이즈를 개수하였고(From AS to APs) 본 논문에서 제안하고 있는 티켓방식에서는 AC에서 MS로 전송하는 인증관련 티켓 메시지의 프레임사이즈를 개수하였다(From AC to MS).

[실험 2]의 시뮬레이션 결과는 [그림 9]와 같다. 본 논문에서 제안하고 있는 티켓기반의 인증방식은 로밍이 발생 할 때마다 하나의 인증메시지만을 전송하고 있다. [그림 7]에서 보여주는 것과 같이 하나의 MAC 프레임은 항상 포함되어야 하는 정보 36Byte와 가변적으로 변하는 프레임바디 부분으로 구성된다. 이때 프레임바디 부분에는 인증관련 정보가 포함된다. 티켓기반의 인증방식의 경우 NG를 이용하여 미리 계산된 PMK를 티켓으로 변환하고 이를 하나의 메시지로 MS에 전달하기 때문에 매 회 로밍 시 마다 전송되는 프레임의 사이즈는 식 (7)과 같이 산출 할 수 있다.

$$36Byte + (328bit * Target AP의\ NG에\ 소속된\ AP의\ 개수) \quad (7)$$

NG를 이용한 PKD방식의 경우 로밍이 발생 할 때마다 선 인증된 정보를 각 각의 AP들에게 개별적으로 전달함으로써 매회 로밍 시 마다 Target AP의 NG에 소속된 AP의 개수만큼 선 인증 관련 메시지를 전송하게 된다. 이때 매회 로밍 시 마다 전송되는 데이터프레임의 사이즈는 식 (8)과 같이 산출 할 수 있다.

$$(36Byte + 256bit) * Target AP의\ NG에\ 소속된\ AP의\ 개수 \quad (8)$$

식(7)과 식(8)을 통해 알 수 있듯이 본 논문에서 제안하고 있는 티켓방식의 경우 매회 로밍 시 하나의 인증관련 메시지만을 전송함으로 MAC 헤더와 FCS의 불필요한 중복전송을 최소화 하고 있는 반면 PKD 방식의 경우 매회 로밍 시 마다 Target AP의 NG에 소속된 AP들에게 개별적으로 선 인증 관련 메시지를 전송함으로써 각 각의 MAC 프레임마다 공통적으로 삽입되는 36Byte의 불필요한 데이터들을 NG에 소속된 AP의 개수에 비례하는 만큼 전송하고 있다.

[실험 1] 과 [실험 2]의 결과에서 알 수 있듯이 본 논문에서 제안하고 있는 티켓기반의 인증 방식은 MS의 로밍 시 Target AP의 NG개수와는 상관없이 미리 계산된 PMK를 티켓으로 변환하여 하나의 메시지만을 전송한다. 그러나 PKD 방식은 MS의 로밍이 발생하면 Target AP의 NG에 소속된 AP의 개수에 따라 AS에서 전송하는 선 인증 메시지의 개수는 결정된다. 이로 인해 NG를 이용한 PKD방식은 불필요한 데이터의 중복전송을 유발하게 되어 전체 네트워크에 부하를 가중 시킨다.

VI. 결 론

IEEE 802.11b 표준의 승인이후 최근까지 무선랜은 다양한 분야에서 사용되고 있다. 최근에는 IEEE 802.11n 표준의 상용화로 무선랜 환경에서도 유선랜 환경에 버금가는 QoS(Quality of Service)를 제공하고 있고 이로 인해 많은 사용자들이 실시간 멀티미디어 서비스를 무선랜 환경을 통해 이용하려고 한다. 그러나 IEEE 802.11i 보안표준은 강력한 데이터 프라이버시는 제공하고 있지만 핸드오프 지연시간이 너무 길어 끊김 없는 실시간 멀티미디어 서비스를 제공하는데 여전히 큰 문제점으로 남아 있는 실정이다. 이를 해결하기위해 선행 된 많은 연구들과 IEEE 802.11 표준은 고속의 핸드오프를 지원하기는 하나 크고 작은 문제점들을 여전히 내포하고 있다. 본 논문은 이러한 문제점을 해결하기 위해 CAPWAP 아키텍처를 바탕으로 티켓기반의 인증기법을 제안하였다. 전통적인 무선랜 구조에서 AC를 추가하여 인증서버의 부하를 감소시켰으며 CAPWAP 아키텍처에서 명시하고 있는 AC의 기능 중 세션 키 도출과정은 AP에 부여함으로써 AC의 부하 또한 감소시켰다. 핸드오프 과정 중 Target AP와 MS사이에서 새롭게 계산되어야 하는 PMK는 AC에서 NG를 이용하여 미리 계산한 후 이에 대한 결과를 티켓으로 암호와 하여 MS로 전달하고 MS는 해당 티켓을 사용하여 고속의 핸드오프를 진행 할 수 있다.

참 고 문 헌

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

[2] IEEE, “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 Standard 802.11i, July 2004.

[3] IEEE, “IEEE Standards for Local and Metropolitan Area Networks: Port based Network Access Control,” IEEE Standard 802.1x-2004(Revision of IEEE Std 802.1X-2001), June 2001.

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

[5] IEEE, “Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Fast BSS Transition,” IEEE Standard 802.11r, July 2008.

[6] B. O'Hara, P. Calhoun, and J. Kempf, “CAPWAP Problem Statement,” RFC 3990, Feb. 2005.

[7] T. Clancy, “Secure Handover in Enterprise WLANS: CAPWAP, HOKEY, and IEEE 802.11r,” IEEE Wireless Communications, vol. 15, issue. 5, pp. 80-85, Oct. 2008.

[8] A. Mishra, M.H. Shin, and W.A. Arbaugh, “Context caching using neighbor graphs for fast handoffs in a wireless network,” IEEE INFOCOM 2004, vol. 1, p. 361, Mar. 2004.

[9] C.M. Huang and J.W. Li, “An Accelerated IEEE 802.11 Handoff Process Based on the Dynamic Cluster Chain Method,” Computer Communications, vol. 30, issue. 6, pp. 1383-1395, Mar. 2007.

[10] A. Mishra, M.H. Shin, N.L. Petroni, T.C. Clancy, and W.A. Arbaugh, “Proactive key distribution using neighbor graphs,” IEEE Wireless Communications, vol. 11, issue. 1, pp. 26-36, Feb. 2004.

<著 者 紹 介>

박 창 섭 (Chang-Seop Park)
1983년: 연세대학교 경제학과 졸업
1983년: 한국 IBM 근무
1990년: 미국 Lehigh Univ. 전자계산학 박사
1990년 ~ 현재: 단국대학교 전자컴퓨터학부 교수
<관심분야> 네트워크 보안, 암호 프로토콜

우 병 덕 (Byung-Duk Woo)
2006년: 단국대학교 컴퓨터과학과 졸업 학사
2006년: (주)EOTECHNICS 근무
2008년 3월 ~ 현재 : 단국대학교 전자계산학 석사과정
<관심분야> 정보보호, 무선 네트워크 보안