# 중앙집중식 무선랜 환경에서의 효율적인 핸드오프를 지원하는 티켓 기반의 인증 메커니즘

우병덕*, 박창섭*
*단국대학교 전자계산학과
e-mail : sayttre@dankook.ac.kr

# A Ticket-based Authentication mechanism Suitable for Efficient Handoff in the Centralized WLAN Environment

Byung-Duk Woo*, Chang-Seop Park*
*Dept. of Computer Science, Dan-Kook 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 Ticket 이라는 새로운 인증 기법을 도입하여 고속의 로밍을 지원하는 핸드오프 메커니즘을 소개한다.

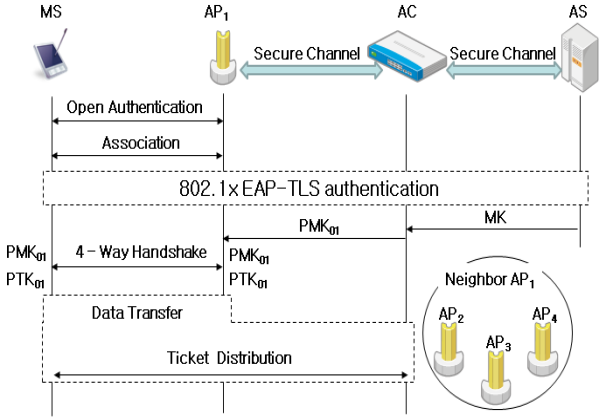
## 1. 서론

최근 들어 최고 320Mbps 의 속도를 지원하는 IEEE 802.11n 표준의 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 나 MoIP 와 같은 실시간 멀티미디어 서비스의 이용을 가능하게 했다. 그러나 IEEE 802.11i 보안표준에서 명시하고 있는 802.1x 인증과정은 끊김 없는 실시간 멀티미디어 서비스를 제공하기에는 핸드오프지연시간이 너무 길다. 본 논문은 802.11 무선랜 환경에서 고속의 핸드오프를 지원하기 위한 Ticket 기반의 핸드오프 메커니즘을 소개한다.

## 2. 관련연구

무선랜 표준화 초기 단계에서부터 계속되던 인증과 무선구간 데이터 보안에 대한 연구는 IEEE 802.11i 의 보안표준을 통해 무선랜에서의 데이터 프라이버시 기능을 더욱 강화하였다.[1][2] 그러나 IEEE 802.11i 의 필수구현 항목인 IEEE 802.1x 인증과정은 MS(Mobile Station)의 핸드오프 시 마다 다수의 메시지교환을 수반하는 EAP-TLS 인증과정을 이용하여 MS 와 AP(Access Point)간 상호인증을 수행하기 때문에 이 과정 중 발생하는 핸드오프 지연시간은 무선랜에서 끊김 없는 실시간 멀티미디어 서비스를 제공하는데 커다란 문제점으로 남아있다.[3][5] 이를 해결하기 위해 IEEE 802.11i 의 Pre-Authentication 방식과 Key Caching 방식, IEEE 802.11f 의 IAPP(Inter Access Point Protocol)[4] 표준안의 제정 등 다양한 무선랜 표준들이 제안되었고 PKD(Proactive Key Distribution)방식등과 같은 선 인증 기법에 대한 연구가 계속되고 있지만 다음과 같은 문제점을 여전히 내포하고 있다. 802.11i 에서 제안하고 있는 Pre-Authentication 의 경우 현재 접속된 AP 를 통해 향후 핸드오프 할 AP 들과 사전인증을 하는 과정에서 인증서버에 많은 부하를 발생시키고 사전인증이 실패 했을 경우 또 다시 802.1x 절차를 거쳐야 하는 문제가 있으며, 802.11f 의 IAPP 는 AP 간 2 계층 전달 정보 및 AP 의 Security Context 정보를 공유함으로써 MS 의 신속한 이동을 지원하지만 AP 상호간 보안상의 독립성을 보장해 주지 못한다는 문제점을 내포하고 있다. 또한 PKD 방식의 경우 NG(Neighbor Graph)라 불리는 향후 접속을 시도 할 가능성이 있는 후보 AP 들을 선정하여 MS 의 인증정보를 선 분배시키는 방식으로 빠른 핸드오프를 지원하지만 NG 영역 이외의 AP 로 MS 가 핸드오프를 할 경우 또 다시 802.1x 인증절차를 수행해야 하고 한 홉 거리 내에서 핸드오프가 발생하더라도 목적지 AP 를 제외한 나머지 AP 들은 불필요한 키를 저장해야 하고 인증서버 또한 불필요한 키를 계산한다는 문제점을 내포하고 있다. 이러한 문제점들을 해결하기 위해 본 논문은 중앙집중식 무선랜 환경에서 AC 를 이용하는 티켓기반의 인증 메커니즘을 제안한다. AC 가 인증 및 접근제어에 관한 기능을 처리하여 인증서버의 부담을 낮추고, 티켓 이라는 새로운 개념을 도입하여 인증관련 정보를 MS 로 전달함으로써 기존 선 인증 방식에서 발생하는 문제점들을 해결하고자 한다. 또한 PMK 도출 알고리즘을 개선함으로써 안전하면서도 빠른 핸드오프를 지원 하는 메커니즘을 제안한다.

## 3. 제안 핸드오프 메커니즘




(그림 1) 제안 메커니즘의 최초 인증 및 세션 키 도출과정과 Ticket 생성 및 분배과정

본 논문에서 제안하고 있는 티켓기반의 인증 메커니즘은 전통적인 무선랜 환경을 구축하는 MS, AP, AS 이외에 새로운 물리적 구성요소인 AC 를 추가한 중앙집중식 무선랜 환경을 기반으로 한다. AC 는 인증 및 접근제어와 관련된 기능을 담당함으로써 인증서버의 부담을 감소시키는 역할을 한다. 또한 인증 관련 정보를 MS 로 전달하기 위해 본 논문에서 제안하고 있는 티켓을 생성하여 AP 를 통해 MS 로 전달하는 기능도 AC 가 전담한다. 티켓은 NG 를 이용하여 미리 계산된 PMK 를 AC 와 해당 티켓을 받게 되는 AP 들 사이에 공유된 대칭형 암호를 이용하여 암호화한 결과로써 MS 가 새로운 AP 로 핸드오프 할 때 대상이 되는 AP(Target AP)로 미리 계산된 PMK 를 안전하게 전달하는데 사용되는 새로운 개념이다. 본 논문에서 제안하고 있는 PMK 도출 알고리즘과 티켓 생성 알고리즘은 다음과 같다.

$PMK_{0j}=prf(MK,client.random,server.random)$ (1)

$PMK_{ij}=prf(MK,MS,AP_j,PMK_{(i-1)j})$ (2)

$Ticket_j=[MS,PMK_{ij},Lifetime]K_j$ (3)

(그림 1)은 본 논문에서 제안하고 있는 프로토콜 중 MS 가 IEEE 802.11 무선랜 서비스를 이용할 때 발생되는 상호인증 및 세션 키 도출 과정, 세션 키 도출 후 티켓 분배 과정을 보여주고 있다. 본 논문에서 제안하고 있는 프로토콜은 AP 와 AC, AC 와 AS 사이에는 안전한 채널이 존재한다고 가정한다. MS 는 $AP_1$ 과 최초 접속 작업 후 AS 와 802.1x 인증과정을 진행하고 이를 통해 상호인증 및 MK(pre-Master Key)를 도출한다. MK 는 안전한 채널을 통해 AC 로 전달되고 MK 를 전달 받은 AC 는 식(1)을 이용하여 $PMK_{01}$ 을 도출한다. AC 는 $PMK_{01}$ 을 안전한 채널을 이용하여 $AP_1$ 로 전달하고 $PMK_{01}$ 을 전달받은 $AP_1$ 은 PMK 를 이용하여 MS 와 4-Way Handshake 과정을 진행한다. 정상적으로 4-Way Handshake 과정을 마치면 MS 와 $AP_1$ 사이에 새로운 세션 키인 $PTK_{01}$ 이 생성되고 이를 이용하여 MS 는 $AP_1$ 을 통해 안전한 무선랜 서비스를 이용할 수 있다. $PTK_{01}$ 생성 후 데이터 전송(Data Transfer)과정이 이루어지는 동안에 AC 는 $AP_1$ 의 NG 정보를 이용하여 MS 가 향후 핸드오프 할 가능성이 있는 AP 들이 사용할 PMK 를 미리 계산한다. (그림 1)에서 $AP_1$ 의 NG 는 $AP_2$, $AP_3$, $AP_4$ 이다. AC 는 식(2)를 이용하여 MS 의 핸드오프 시 $AP_1$ 의 이웃 AP 들이 사용할 PMK 를 계산한다. 이에 대한 결과는 $PMK_{12}$, $PMK_{13}$, $PMK_{14}$ 이다. $AP_1$ 의 이웃 AP 들에 대한 PMK 계산 작업이 완료되면 AC 는 식(3)을 이용하여 $Ticket_2$, $Ticket_3$, $Ticket_4$ 를 생성한다. 티켓은 MS 의 MAC 주소와 NG 를 이용하여 미리 계산된 PMK, 해당 티켓의 유효기간을 나타내는 Lifetime 을 AC 와 AP 들 사이에 공유된 대칭 키 K 를 이용하여 암호화한 결과이다. 이렇게 생성된 티켓은 하나의 데이터 프레임으로 구성되어 안전한 채널을 통해 AC 에서 $AP_1$ 을 경유하여 MS 로 전달한다. 티켓 생성과 전달에 관한 일련의 과정은 MS 와 $AP_1$ 사이의 데이터 전송과정 중 진행된다. MS 가 $AP_1$ 의 NG 에 소속된 AP 로 로밍 할 경우 해당 Target AP 와 일치하는 티켓을 Target AP 로 전달하고 해당 티켓을 전달받은 Target AP 는 AC 와 사전에 공유된 대칭 키 K 를 이용하여 티켓을 복호화 하고 복호화된 내용을 이용하여 802.1x 인증절차 없이 MS 와 고속의 상호인증 작업을 통해 빠른 핸드오프를 진행 할 수 있다.

## 4. 결론

본 논문은 고속의 802.11 핸드오프를 지원하기 위해 중앙집중식 무선랜 환경을 바탕으로 티켓기반의 인증기법을 제안하였다. 전통적인 무선랜 구조에서 AC 를 추가하여 인증서버의 부하를 감소시켰으며 핸드오프 과정 중 Target AP 와 MS 사이에서 새롭게 계산되어야 하는 PMK 는 AC 에서 NG 를 이용하여 미리 계산한 후 이에 대한 결과를 티켓으로 암호와 하여 MS 로 전달하고 MS 는 해당 티켓을 사용하여 고속의 핸드오프를 진행 할 수 있다. 향후 연구해야 할 과제는 본 논문에서 제안하는 인증방식과 기존 인증방식과의 성능 비교 분석 및 안전성 분석을 통해 제안 메커니즘이 최적의 핸드오프를 지원한다는 것을 증명하는 것이다.

## 참고문헌

[1] IEEE, "Wireless LAN Medium Access Control and Physical Layer specifications", IEEE Standard 802.11, June. 2007.

[2] IEEE, "Medium Access Control Security Enhancements, Amendment 6 to IEEE Standard for Information", 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, 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 802.11 Operation", IEEE Standard 802.11f, July. 2003.

[5] Mishra. A, Min Ho Shin, Petroni. N.L. Jr, Clancy. T.C and Arbaugh. W.A, "Proactive key distribution using neighbor graphs", IEEE Wireless Communications, Vol 11, Issue 1, pp.26-36, Feb. 2004oger S. Pressman. “Software Engineering, A