논문 2006-43TC-11-16

IEEE 802.11i 환경에서 신속하고 보안성 있는 핸드오프 메커니즘

(Fast and Secure Handoff Mechanism for IEEE 802.11i System)

박 재 성*, 임 유 진**

(Jaesung Park and Yujin Lim)

요 약

IEEE 802.11i 표준은 802.11 WLAN(wireless LAN) 환경에서 보안성있는 핸드오프 제공을 위하여 FA(Full Authentication)과 PA(Preauthentication)을 정의하였다. 그러나 FA는 핸드오프 사용자들에게 끊김없는(seamless) 서비스를 제공하기에는 너무 느리며, PA 방식은 사용자 밀도가 높은 WLAN 환경에서는 사용자의 캐쉬 엔트리가 핸드오프가 실제로 발생되기도 전에 다른 핸드오프 사용자의 엔트리에 의해 삭제될 수 있기 때문에 적합하지 않다. 본 논문에서는 핸드오프 과정에서의 인증과 키 관리에 소요되는 지연시간을 최소화하기 위한 신속하고 보안성있는 핸드오프 방법을 제안한다. 제안기법은 핸드오프가 발생하면 해당 사용자와 이전 AP(Access Point)사이에 구축되었던 보안 정보를 이전 AP에서 새로이 이동한 AP로 전달하여 인증 지연을 줄이며 핸드오프 세션이 종료될 때 까지 동일한 세션 키를 재활용하여 세션 키 생성 지연을 줄인다. 세션 키의 신규성(freshness)는 핸드오프 세션이 종료된 후에 세션 키를 새롭게 할당됨으로써 유지된다. 본 논문에서 제안하는 메커니즘은 AP가 RSNA(Robust Security Network Association) 설정 이전에 핸드오프 사용자를 인증하게 함으로서 802.1X 인증의 보안 수준을 유지하면서도 핸드오프 지연시간을 최소화시키다.

Abstract

IEEE 802.11i standard specifies full authentication and preauthentication for secure handoff in 802.11 wireless LAN (WLAN). However, the full authentication is too slow to provide seamless services for handoff users, and preauthentication may fail in highly populated WLAN where it is highly probable that the cache entry of a preauthenticated user is evicted by other users before handoff. In this paper, we propose a fast and secure handoff scheme by reducing authentication and key management delay in the handoff process. When a user handoffs, security context established between the user and the previous access point (AP) is forwarded from the previous AP to the current AP, and the session key is reused before the handoff session terminates. The freshness of session key is maintained by regenerating session keys after handoff session is terminated. The proposed scheme can achieve considerable reduction in handoff delay with providing the same security level as 802.1X authentication by letting an AP authenticate a handoff user before making an robust security network association (RSNA) with it.

Keywords: IEEE 802.11i, Fast Authentication, Handoff, Security Context Transfer.

I. 서 론

WLAN(wireless LAN)은 사용자들에게 자유롭고 경제적인 인터넷 접속 환경을 제공해 줌으로서 오늘날 널리 활용되고 있다. 사용자가 통화중에 핸드오프를 발생시키는 셀룰라 네트워크 환경과는 달리, WLAN 사용자는 AP(Access Point)의 서비스 영역 내에서만 이용중인 서비스의 연속성을 보장받는다. 다시 말해서, 현재의 WLAN은 끊김없는(seamless) 핸드오프를 지원하지 않기 때문에 사용자들은 네트워크 사용 중에 현재 접속되어 있는 AP 영역 밖으로 이동할 수 없다. 그러나 무선 네트워크를 사용하는 사용자가 증가함에 따라 이동 중

* 정회원, 수원대학교 IT대학 인터넷정보공학과
(The University of Suwon, IT College, Department of Internet Information Engineering)
** 정회원, 수원대학교 IT대학 정보미디어학과
(The University of Suwon, IT College, Department of Information Media)
접수일자: 2006년10월10일, 수정완료일: 2006년11월18일

에도 끊김없는 통신서비스를 요구하게 되었고 이에 따라 신속한 핸드오프의 제공은 WLAN 환경에서 연구되어져야할 중요한 이슈 중 하나로 부각되었다.

무선 라디오를 통해 데이터가 전송되는 WLAN 환경에서 성공적인 핸드오프 제공을 위해서는 보안성 유지가 필수요소라 할 수 있다. WLAN에서의 보안성 유지를 위하여 IEEE 802.11i 표준이 정의되었다[1]. IEEE 802.11i 표준은 MN(Mobile Node)의 핸드오프를 측정(probing), 재접속(reassociation), 인증, 키 생성의 4단계로 구분하였다. 측정단계는 MN이 향후 접속 가능한 AP를 검색하는 단계이다. MN이 새로운 AP로 핸드오프를 결정하면, MN은 해당 AP와 재접속 절차를 거쳐야 한다. 이후 MN은 802.11i에 정의된 단계에 따라 재인증 절차를 거친 후 마지막으로 MN과 네트워크 사이에 새로운 세션 키가 생성되게 된다. 그러나 802.11i 인증 절차는 MN과 AS(Authentication Server) 사이에 몇 번의 메시지 교환을 요구한다. 일반적으로 AS는 AP에 비해 멀리 떨어져 위치한다. 또한 새로운 세션 키 생성을 위하여 AP와 MN사이에 메시지 교환도 요구된다. 그러므로, 인증과 키 생성을 위한 지연시간은 신속한 핸드오프를 수행하기 위한 큰 걸림돌이 된다.

인증에 따른 지연시간 문제를 해결하기 위하여, 802.11i 표준에는 PA(Preauthentication)이 추가로 포함되어 있다[1]. PA은 MN이 실질적으로 핸드오프하기 전에 향후 핸드오프의 가능성이 있는 AP들(이후 향후 서비스 AP로 지칭)과 사전에 인증절차를 거침으로써 인증 지연시간을 줄이는 방법이다. 그러나 어떻게 향후 서비스 AP들을 선정할 것인가는 802.11i 표준에 포함되어 있지 않으며, 이와 관련된 몇몇 제안이 나와있는 상태이다. FHR(Frequent Handoff Region) 방식은 MN의 장기(long-term) 이동 내역을 기반으로 향후 서비스 AP들을 선정한다[2]. 이 외에 이웃 그래프(neighbor graph)를 사용하여 향후 서비스 AP를 결정하는 방식도 제안되어 있다[3]. 이 방식은 향후 서비스 AP가 전체 AP의 작은 일부분만을 차지한다는 것에 주목하였다. 그러나 이러한 proactive 방식들은 신중하게 설계되지 않으면 재인증 오버헤드가 발생할 수 있다. 예를 들어, MN_i와 향후 서비스 AP사이의 보안 정보는 MN_i가 해당 AP로 실제로 핸드오프하기 전에 다른 MN의 정보들로 갱신될 가능성이 있으며, 이러한 가능성은 핫스폿(hot spot)지역의 WLAN과 같이 AP의 서비스 영역 내의 MN의 밀도가 높고 MN의 이동성이 높은 경우 더욱 높다. MN가 핸드오프 될 때 이동 AP에 해당 MN에 대한 보안 정보가 없는 경우, FA(Full Authentication) 과정을 거쳐야 하므로 끊김없는 핸드오프 지원은 불가능하게 된다. 또한 proactive 방식은 AS에 과중한 관리 오버헤드를 부과하며, AP들에게는 많은 시그널링 메시지의 교환을 요구함으로써 확장성이 떨어진다.

본 논문에서는 reactive 방식을 기반으로 핸드오프 지연을 최소화하면서도 인증과 세션 키의 신규성(freshness)과 보안성 측면에서 IEEE 802.11i 표준 수준을 제공하는 메커니즘을 제안한다. 본 논문은 인증 지연과 핸드오프 후 키 생성 지연시간을 최소화하는데 초점을 맞추며, 제안 메커니즘 구현을 위하여 802.11i 표준을 확장함으로서 기존 표준과의 호환성을 유지하고자 하였다. AP가 보안성있는 재접속을 요구하는 MN을 AS의 도움없이 인증하기 위하여 IEEE 802.11 *RR (reassociation request) MAC management* 프레임 내에 두 개의 필드를 추가하였고, *capability information* 필드에 한 비트를 정의하였다. MN이 AP_i에서 AP_j로 핸드오프하는 경우, AP_i에 설정된 MN의 보안 정보는 AP_j에게로 넘겨지며, AP_j는 이러한 보안정보와 *RR* 프레임을 사용하여 재접속을 요구하는 MN을 인증할 수 있다. 또한 핸드오프 세션이 종료되기 전에는 기존의 세션 키를 재사용한다. 그러나 일단 핸드오프 세션이 종료되면 새로운 세션 키를 생성하기 때문에 키의 신규성을 유지할 수 있다. Proactive 방법과는 달리 본 논문에서 제안한 방법은 MN의 밀도나 이동 패턴 등의 환경 요소와는 무관하게 동작하므로 AS에 과중한 관리 오버헤드를 부과하지 않는다.

논문의 구성은 다음과 같다. Ⅱ장에서는 보안성 제공을 위한 하부구조 기반 WLAN(infrastructure-based WLAN)과 IEEE 802.11i에서의 FA과 키 관리 방법에 대해서 설명한다. Ⅲ장에서는 본 논문에서 제안하는 신속하고 보안성있는 핸드오프 메커니즘에 대해서 설명하고, Ⅳ장에서 기존의 proactive 방법과의 성능 분석을 수행한다. 마지막으로 Ⅴ장에서 결론을 맺는다.

Ⅱ. IEEE 802.11i 기반 보안성있는 WLAN

본 장에서는 일반적인 WLAN 구조와 보안성있는 WLAN 지원을 위한 IEEE 802.11i 표준을 설명한다. 이 과정에서 현 표준으로는 신속한 핸드오프를 지원할 수 없다는 문제점을 제기하고, proactive 기법의 방법의 장단점을 분석한다.

1. 보안성 있는 WLAN

IEEE 802.11i 표준은 보안성있는 WLAN을 모든 MN과 AP들 사이에 RSNA(Robust Security Network Association)을 설정하는 RSN(Robust Security Network)으로 정의하였다. RSN은 하부구조 기반 또는 애드혹 방법으로 구축할 수 있다. 본 논문에서는 이들 중 하부구조 기반 RSN에 초점을 맞춘다. RSNA는 MN과 AS가 상호 인증 과정을 거친 후, AP가 무선 링크를 통하여 전송될 데이터를 암호화하기위한 키를 생성했을 때 설정된다. IEEE 802.11i는 개방 시스템 인증이나 공유 키 인증과 같은 개체 인증에 대하여 향상된 IEEE 802.1X기반 인증 방식을 명시하였다. 또한 WEP(Wired Equipment Privacy)에 대하여 향상된 키 생성 및 관리, 암호화 기법을 포함하고 있다. 표준에서는 MN이 접속(associate)하는 AS와 AP에 대한 신뢰성을 가정하였고, AS와 AP 사이에도 신뢰성 있는 관계가 유지된다고 가정하였다. 본 논문에서는 또한 일반적으로 하나의 조직에 의해 소유되고 관리되는 WLAN에는 인증되지 않은 AP를 적발하기 위한 네트워크 관리 도구가 제공되므로 AP들 간의 신뢰성 있는 관계를 가정하였다[8].

핸드오프하는 MN은 새로운 AP와 RSNA를 설정해야만 한다. 이는 MN이 AS에 의해 다시 인증되어야 하고 새로운 보안 키가 생성되야 함을 의미한다. 상호 인증을 위하여 MN와 AS 사이에 EAP (Extensible Authentication Protocol)이 사용된다. EAP는 MN이 EAP-TLS[4], EAP-MD5, EAP-AKA와 같은 인증방법 중 하나를 선택할 수 있도록 허락하지만 일반적으로 EAP-TLS가 사용된다. 무선 링크 상에서 MN과 AP사이에 교환되는 EAP-TLS 메시지는 EAPoL(EAP over LAN) 프로토콜에 의해 전송된다. IEEE 802.11i는 AP와 AS사이에 보안 메시지 전송을 위한 프로토콜을 정의하고 있지 않다. 그러나 RADIUS (Remote Authentication Dial-In User Service)는 사실상의 표준으로 받아들여지고 있다. 상호 인증이 완료되면, 데이터 암호화를 위한 세션 키가 IEEE 802.1X 프로토콜의 4-way handshake 과정을 통해 생성된다.

EAP-TLS는 challenge-response 타입의 강력한 인증 및 암호화 방법을 제공한다. EAP-TLS 인증에서 MN과 AS는 공통의 CA(Certification Authority)로부터 인증서를 발급받아야 한다. 그림 1은 인증과 4-way handshake 과정에서의 메시지 흐름을 보인 것이다. 인증 절차는 MN의 신원정보를 AS에게 전송함으로서 시작되며, MN은 AS의 인증서를 확인함으로서 AS를 인증한다. 성공적인 인증 절차가 끝나면, MN는 무작위로 선택한 PS(Premaster Secret)를 AS의 공개 키로 암호화한 후 AS에게 전송한다 (Client-Key-Exchange 메시지). AS는 MN의 인증서를 받아 해당 MN을 인증한다. MN과 AS사이의 PS를 기반으로 MK(Master Key)가 생성된다. 생성된 MK는 수식 1과 같은 PRF(Pseudo Random Function)을 통하여 PMK(Pairwise Master Key)로 만들어진다.

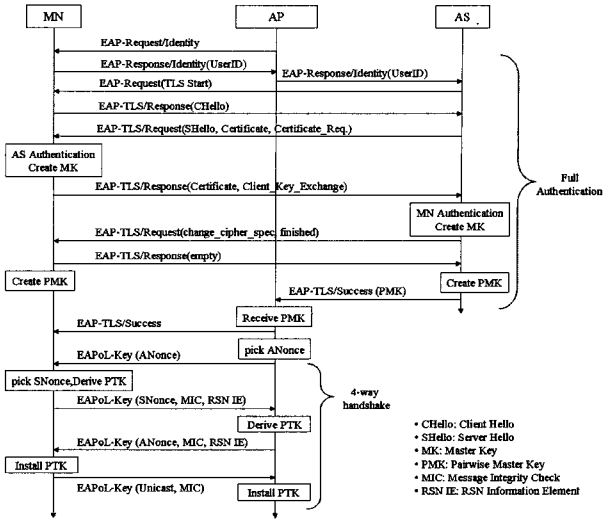


그림 1. Full Authentication과 4-way handshake 절차.
Fig. 1. Full authentication and 4-way handshake procedure.

$$PMK = PRF(MK, CHello \| SHello) \quad (1)$$

$CHello$와 $SHello$는 MN과 AS에 의하여 각각 무작위로 선택된 숫자 (Nonce)이다. AS는 MN이 RSNA를 설정하기를 원하는 AP에게 생성된 PMK를 전송한다. 따라서 성공적인 상호 인증과정이 끝나면, MN과 AS는 MK를, MN, AS, AP는 PMK를 공유하게 된다. PMK는 MN과 AP사이에 교환되는 데이터 암호화를 위해 사용되는 PTK(Pairwise Transient Key)의 생성의 기반이 된다. EAPoL 메시지를 통한 4-way handshake는 MN과 AP의 생존(liveness)을 확인하고 PTK의 신규성을 보장한다. MN과 AP는 4-way handshake의 초기 두개의 EAPoL-Key 메시지를 통하여 각자 무작위로 선택한 nonce (AP의 ANonce, MN의 SNonce)를 교환하며, PMK와 MN/AP의 MAC 주소, ANonce, SNonce를 기반으로 다음과 같이 PTK가 생성된다.

$$PTK = PRF(PMK, MN_{MAC} \| AP_{MAC} \| ANonce \| SNonce) \quad (2)$$

세 번째 EAPoL-Key 메시지를 통하여 MN과 AP가 동기를 맞추게 되고, 마지막 메시지가 전송됨으로서 키의 설정과 4-way handshake가 완료되게 된다.

2. Proactive 인증

앞서 설명한 바와 같이 FA과 4-way handshake는 길게는 수초가 소요되는 MN, AP, AS간 많은 메시지 교환을 요구하기 때문에 신속한 핸드오프를 제공할 수 없다. 이러한 문제를 해결하기 위하여 PA가 IEEE 802.11i에 포함되었다. PA는 MN이 실제로 핸드오프하기 전에 향후 서비스 AP들과 인증 절차를 수행함으로서 핸드오프 지연을 줄이는 방법이다. 그림 2는 PA의 메시지 흐름을 나타낸 것이다.

그러나 802.11i는 어떻게 향후 서비스 AP를 선정할 것인가는 언급하지 않았다. 이와 관련된 몇몇 제안은 다음과 같다. Pack[2]는 향후 서비스 AP 선정을 위하여 FHR(Frequent Handoff Region)을 제안하였다. MN의 FHR은 MN의 장기(long-term) 이동 내역을 기반으로 계산된다. 중앙의 AS는 각 MN의 AP 이동 주기를 기록한다. 다시 말해서, AS는 각 MN당 n x n 행렬을 유지한다. 이때 n은 WLAN에 포설된 AP의 개수이며 N_{ij}는 AP_i에서 AP_j로 발생한 MN의 핸드오프 비율의 역수이다. MN이 AP_i와 연결중인 상태라면, 해당 MN은 FHR의 다른 AP들과도 인증 절차를 거치게 된다. 이와는 다르게 향후 서비스 AP 선정을 위하여 이웃 그래프(Neighbor graph)를 사용하는 방법도 제안되었다[3]. 이 방법은 향후 서비스 AP는 전체 AP에 비해 작은 일부분임에 주목하였다. 이웃 그래프는 각 AP에서 분산 방식으로 또는 AS에 중앙방식으로 구축될 수 있으나 빠른 수렴 시간으로 인해 중앙방식이 주로 사용된다. 일단 이웃 그래프가 구축되면, AS는 MN의 보안 정보와 키 관련 정보를 이웃 그래프 내의 AP들에게 전송한다.

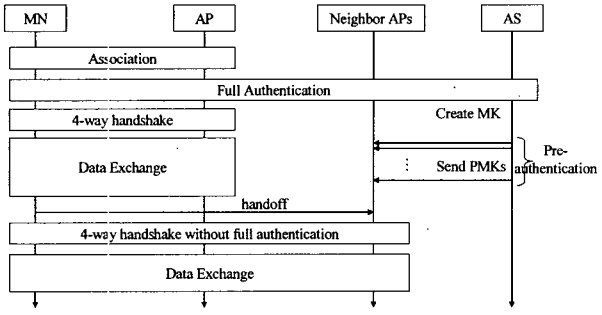


그림 2. Freauthentication 메시지 흐름.
Fig. 2. Freauthentication procedure.

따라서 MN이 이웃 그래프 내의 한 AP로 이동할 때, 인증절차로 인한 지연시간이 발생하지 않는다.

그러나 이러한 proactive 방식은 다음과 같은 단점을 가진다. 먼저 성능 요소로 예측 메커니즘뿐만 아니라 네트워크 환경이 함께 고려되어야 한다. 예를 들어, 향후 서비스 AP가 유지하고 있는 MN_i의 보안 정보는 MN_i가 실제 해당 AP로 핸드오프하기 전에 다른 MN의 보안 정보들로 갱신될 수 있다. 이러한 시나리오는 핫스폿 지역의 WLAN 시스템과 같이 AP내의 MN 밀도가 높고 MN의 이동성이 높은 환경에서 자주 발생할 수 있다. MN이 핸드오프 할 때, 새로이 이동한 AP에 해당 MN의 보안 정보가 존재하지 않는 경우에는 FA 절차를 거쳐야 하기 때문에 신속한 핸드오프 제공은 힘들어진다. 둘째로, proactive 방식은 중앙 AS가 상태 정보를 유지해야 하며 AS와 AP들 사이에 많은 시그널링 오버헤드를 야기하므로 확장성 측면에서 문제가 있다.

III. 신속하고 보안성 있는 핸드오프

이 장에서는 본 논문에서 제안하는 신속하고 보안성 있는 핸드오프 메커니즘에 대해서 설명한다. 제안 기법의 설계를 위해 IEEE 802.11i 표준과의 상호 호환성을 우선적으로 고려하여 802.11i 표준을 확장하였다. 제안된 메커니즘은 AS의 참여 없이 과거 AP가 사용하던 MN의 보안 정보를 MN이 새로이 접속한 AP가 MN을 인증할 때도 그대로 사용한다. 또한 MN과 과거 AP가 사용하던 PTK를 새로운 AP에서 재사용함으로써 4-way handshake 절차로 인한 지연시간을 줄인다. 그러나 PTK 기간이 만료되었거나 핸드오프 세션이 종료한 경우에는 새로운 AP와 MN사이에 새 PTK가 생성되기 때문에 세션 키의 신규성을 보장할 수 있다.

1. MAC Management 프레임 확장

본 논문에서는 그림 3과 같이 IEEE 802.11i 표준의 *RR MAC management* 프레임의 *frame body* 필드와 *capability information* 필드를 확장하였다. 신속하고 보안성있는 핸드오프 지원 여부를 타나내기 위하여 MN은 *RR* 프레임 내의 *capability information* 필드의 FSH(Fast and Secure Handoff) 비트를 설정한다. 또한 *become* 메시지, *probe* 메시지, *association* 메시지에서도 FSH 비트는 MN과 AP의 신속하고 보안성있는 핸드오프 지원 여부를 나타낸다. MN은 *RR* 프레임의 *frame body*에 MN이 핸드오프할 AP가 PTK를 생성하

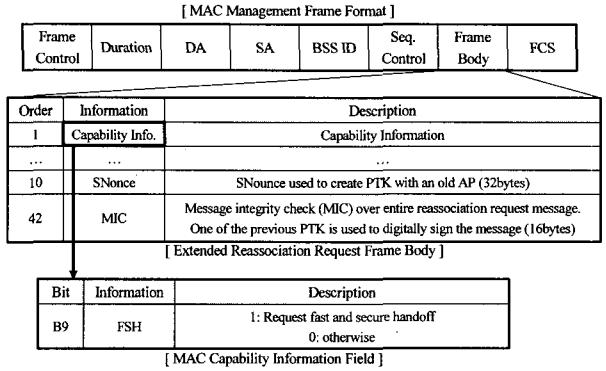


그림 3. 확장된 MAC management 프레임
Fig. 3. Extended MAC management frame.

기 위한 SNonce를 포함시킨다. 또한 MN은 AP가 *RR* 프레임의 무결성(integrity)을 확인할 수 있도록 MIC(Message Integrity Check)를 추가한다.

2. 신속한 재인증과 세션 키 관리

그림 4는 본 논문에서 제안한 메커니즘의 메시지 흐름을 보인 것이다. MN이 한 AP에서 다른 AP로 핸드오프하는 경우, MN은 새로운 AP에게 *RR* 프레임을 전송한다. 새 AP는 과거 AP로부터 MN의 보안 정보(PMK, SNonce, ANonce, 과거 AP의 MAC 주소, Cipher Suite 등)를 전달받는다. 이때 AP사이의 보안 정보 교환을 위하여 IAPP(Inter-Access Point Protocol)가 사용된다. IAPP는 다른 사업자 AP들 간의 통신을 위하여 고안된 프로토콜이다[5]. 본 논문에서는 네트워크 초기에 AP사이 보안성 있는 접속이 미리 설정되었다고 가정하였다. *RR* 프레임의 MIC는 MN과 과거 AP사이에 사용되었던 PTK에 의하여 암호화되기 때문에, 같은 PTK와 cipher suite를 가지는 새 AP만이 보안 정보로부터 MIC를 복호화할 수 있다. 메시지 무결성 검사가 끝나면, 새 AP는 *RR* 프레임의 Snonce와 과거 AP로부터 받은 보안 정보 내의 SNonce 값을 비교하여 MN을 인증한다.

인증 절차가 완료되면, MN과 새 AP는 과거의 PTK를 재사용함으로써 4-way handshake로 인한 지연시간을 줄일 수 있다. 802.11i는 핸드오프를 네트워크 초기 접속과 같은 선상에서 바라보았으나, 본 논문에서는 MN이 새 AP와의 인증 후 이전에 사용하던 세션 키를 그대로 사용하게 함으로서 핸드오프를 초기 네트워크 접속과는 다른, 진행 중인 세션의 연속선상에서 바라보았다. 그러나 이러한 세션 키의 재사용이 세션 키의 신규성이나 통신 객체의 생존성(liveness)에 악영향을 미

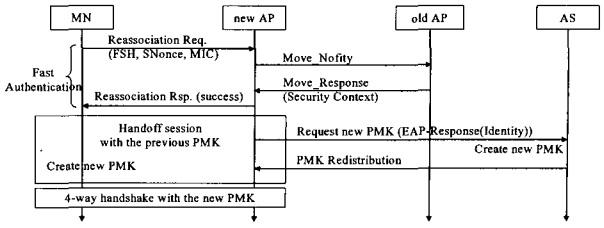


그림 4. 신속하고 보안성있는 핸드오프.
Fig. 4. Fast and secure handoff procedure.

치지 않게 하기 위해서, 각 세션이 종료될 때 세션 키는 새로이 생성된다. 다음은 MK와 과거 AP/새 AP의 MAC 주소를 기반으로 새로운 PMK를 생성하는 함수이다.

$$nPMK = PRF(MK, oldPMK \| MN_{MAC} \| oldAP_{MAC} \| \neq wAP_{MAC}) \quad (3)$$

MK는 MN이 초기 네트워크 접속 시 FA 과정을 통해 AS와 공유된다. *oldPMK*는 MK와 MN/AS 사이에 생성된 무작위 수 (CHello, SHello)를 기반으로 생성되며, 이는 MN과 AS, AP사이에 공유된다. 핸드오프 세션이 종료되거나 PTK 기간이 만료될 때는 4-way handshake를 통하여 새로운 PTK가 생성되므로, 세션 키의 신규성과 통신 객체의 생존성 또한 보장된다.

Ⅳ. 성능 분석

이 장에서는 본 논문에서 제시한 메커니즘의 성능을 핸드오프 지연과 MN의 최대 이동 속도 측면에서 분석한다. PA와의 성능 비교를 위하여 RSNA (인증 지연과 4-way handshake 지연의 합) 지연 시간을 비교하였다. 또한 AP들 간 지연시간을 기반으로 MN의 최대 속도 범위를 분석하였다.

1. 이동 모델

MN의 이동성 표현을 위하여 CRT(cell residence time)를 도입하였다. CRT란 MN이 한 셀에 진입하여 해당 셀을 벗어날 때까지의 시간을 말한다. MN이 새로운 셀에 진입할 때는 그 이동 방향을 바꾼다고 가정하고, 핸드오프 발생 시 현재 MN의 이동 방향과 새로운 이동 방향 사이의 각도를 θ로 나타내면, MN이 이동 방향의 큰 변화 없이 AP 영역 내를 이동할 때의 CRT(t_{cr})

은 다음 식 4와 같이 나타낼 수 있다.

$$t_{cr} = \frac{2R \cdot \sin(\theta)}{v} \quad (4)$$

R은 셀 반경을, v는 MN의 이동 속도를 나타낸다. MN이 자신의 이동 방향을 $[0,\pi]$ 내에서 결정한다면 평균 CRT는 $\mu = \frac{4R}{\pi v}$이다. 본 논문에서 사용한 이동 모델은 신속하고 보안성있는 핸드오프를 제공하기 위한 MN의 최대 속도를 분석하기 위한 것이므로 (IV.3절) 셀 내에서의 MN의 움직임은 고려하지 않았다. 제시한 모델은 MN이 이동방향의 큰 변화 없이 움직이는 경우 [9]에서 제시한 평균 CRT(식 5)와 같다.

$$\frac{\pi R}{2E[v]} \quad (5)$$

MN의 CRT는 이동 방향이나 이동 속도의 함수가 아니라 실측값의 통계적 분석에 의해 감마 함수로 직접 모델링이 가능하다[6]. 즉, CRT의 PDF(probability density function)은 다음과 같다.

$$f(t_{cr}) = \frac{1}{b^a T(a)} t^{a-1} e^{\frac{-t}{b}} \quad (6)$$

a는 형상(shape) 파라미터이고, b는 척도(scale) 파라미터, $T()$는 감마함수이다. 이러한 파라미터들은 이동 방향, 속도, 그리고 방향이나 속도의 변화정도와 같은 MN의 이동 패턴에 의해 결정되며, 시뮬레이션에 의한 모델 파라미터 조정 예가 제공되어 있다[6]. 파라미터들의 다양한 값들에 따라 CRT와 CRT에 대한 분산 값을 조정할 수 있다.

수식 5와 수식 6에 따른 CRT의 차는 0.0015% 이내로[6], 수식 6과 본 논문에서 사용하는 모델의 차는 아주 미미하다고 할 수 있다.

2. RSNA 지연시간

MN과 AP, AP와 AS, AP와 AP사이의 지연을 각각 t_a, t_d, t_{ap}라 지칭한다. t_a는 무선 링크에 대하여 서로 경쟁하는 MN들 사이의 802.11 MAC(Medium Access Control) 프로토콜에 의하여 결정된다. 따라서 제어 관리 채널(controlled management channel)이 사용되지 않는 경우의 t_a 값의 분산은 아주 커지게 된다. 반대로 t_d와 t_{ap}는 전송 지연시간의 영향을 받는다. 유선망에서의 지연 시간은 안정된 값을 가지며, 주로 홉 수에 의해 영향을 받는다. 그러나 WLAN에서는 인접한 AP들이 2계층 스위치나 액세스 라우터에 의하여 연결되기 때문에 AP들은 보통 1-2홉 정도 떨어져 있다. AS는 네트워크의 중심부에 위치하므로 t_d는 t_{ap}에 비하여 훨씬 큰 값을 가진다. 그림 1에서의 FA의 RSNA 지연시간은 $13t_a + 8t_d$이다.

PA의 경우, MN이 핸드오프하는 AP에 해당 MN의 보안 정보가 이미 있다면 인증절차를 거치지 않아도 되지만, 보안 정보가 없는 경우에는 FA 절차를 거쳐야 한다. PA 방법에서 핸드오프할 AP가 유지하고 있는 MN의 캐쉬 엔트리는, 해당 MN이 실제 핸드오프를 하기 전에 다른 MN의 캐쉬 엔트리에 의해 삭제될 수 있다. 한 AP의 셀 내에 존재하는 MN의 개수가 ρ, AP의 캐쉬 크기가 N_c, L이 셀의 크기일 때, fluid flow model[7]에 의한 셀 경계를 넘어가는 MN의 aggregate rate는 다음과 같다.

$$C = \frac{\rho v L}{\pi} \quad (7)$$

MN이 향후 서비스 AP중 하나로 핸드오프했을 때 해당 AP의 캐쉬에 MN의 보안 정보가 없을 확률은 다음과 같다.

$$p_m = P_r\left(\frac{\rho v L}{\pi} t_{cr} > N_c\right) = 1 - \int_0^{\frac{\pi N_c}{\rho v L}} f(t_{cr}) dt_{cr} \quad (8)$$

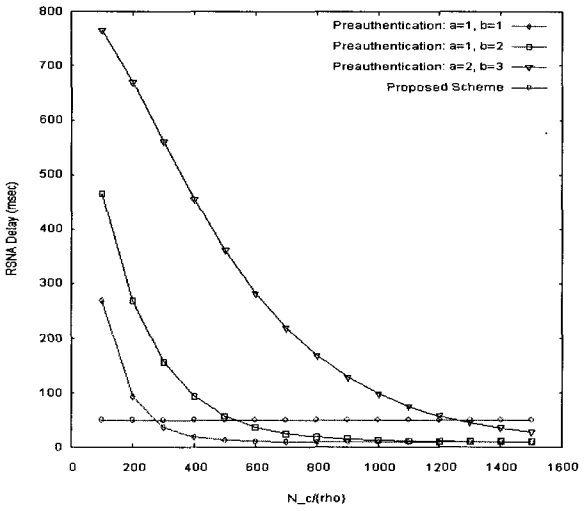
따라서 PA의 RSNA 지연시간은 다음과 같다.

$$P_d = (1 - p_m) 4t_a + p_m (13t_a + 8t_d) \quad (9)$$

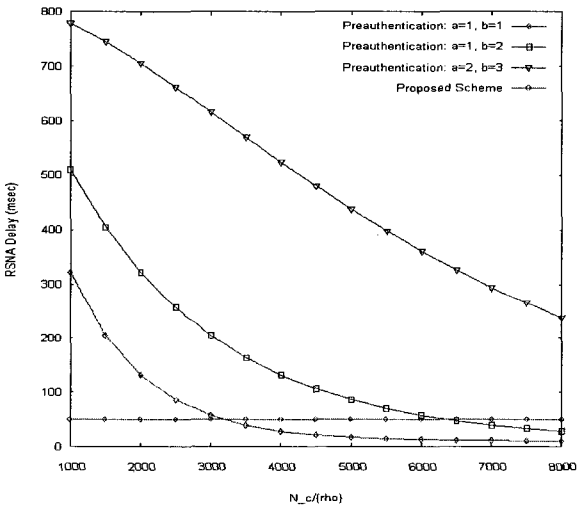
그림 4로부터, 본 논문에서 제안한 메커니즘의 RSNA 지연시간은 t_{ap}에 의해 결정된다. 이는 4-way handshake 절차를 거치지 않기 때문이며, 결과적으로 RSNA 지연시간은 다음과 같다.

$$R_d = 2t_{ap} \quad (10)$$

11Mbps 802.11b 무선 링크 환경에서, t_a=2.5ms, t_d=97.2ms, t_{ap}=23.7ms로 가정할 수 있다. 그림 5는 셀 반경이 100m일때, 다양한 MN의 셀 체류시간에 따른 RSNA 지연시간을 비교한 것이다. 각각의 그림 5-(a)와 5-(b)는 MN의 평균속도가 5km/h와 60km/h일 때를 나타내며, x축은 AP 반경 내 MN 밀도에 대한 AP 캐쉬 크기를 나타낸 것이다. 앞서 언급한 바와 같이 PA의 지연시간은 AP 캐쉬 크기, 핸드오프 MN의 CRT, 다른 MN들의 이동 속도에 의해 결정되므로, 다른 MN들이



(a) 평균 속도 = 5km/h.
(a) average velocity = 5km/h.



(b) 평균 속도 = 60km/h
(b) average velocity = 60km/h

그림 5. RSNA 지연시간 비교.
Fig. 5. RSNA delay comparison.

빠르게 이동할수록 AP는 더 큰 캐쉬를 유지해야 한다. 또한 CRT가 커질수록 (예를 들어 a=1, b=1에서 a=2, b=3으로 커질수록) 커지는 편차 값을 보완하기 위해서는 더 큰 캐쉬가 요구되며, 이는 WLAN 시스템 구축 비용을 높이는 결과를 초래한다. 반대로 본 논문에서 제안한 메커니즘의 RSNA 지연시간은 셀 내 MN의 밀도와 다른 MN들의 이동 속도, 핸드오프 MN의 CRT과 상관없으며, 제안된 방법의 RSNA 지연시간은 AP사이의 지연시간에 의해서만 영향을 받으며 이는 WLAN 설치 단계에서 조절이 가능하다.

3. MN의 최대 속도

본 논문에서 제안한 방법은 과거 AP가 향후 서비스 AP에게 MN의 보안 정보를 전달하는 reactive 방식의 메커니즘이다. 따라서 보안 정보를 가져오는데 소요되는 지연시간은 MN의 CRT보다 작아야 한다. 수식 4와 10으로부터 MN의 이동 속도 상한은 다음과 같이 계산될 수 있다.

$$v \leq \frac{R \bullet \sin(\theta)}{t_{ap}} \tag{11}$$

그림 6은 t_{ap}와 θ가 주어졌을 때 MN의 최대 속도를 보인 것이다. 패킷 간 지연시간이 150ms이내여야 하는 멀티미디어 스트리밍 서비스와 같이 시간제한을 가지는 응용에 대한 끊김없는 핸드오프를 지원하기 위해서는 RSNA 지연시간이 50ms이내 여야 한다. MN이 핸드오프 할 때 그 이동 방향을 바꾸지 않는 경우 (즉, $\theta = 0^\circ$), 제안된 방법은 최대 14.4km/h의 속도로 움직이는 MN을 지원할 수 있다. MN이 핸드오프 할 때 방향을 갑자기 바꾸는 경우에는 (예를 들어, $\theta = 85^\circ$), MN의 최대 속도는 t_{ap}가 25ms일 때 1.25km/h이며, t_{ap}가 3ms일 때는 10.5km/h이다. 빌딩 내 AP간 연결을 위하여 고속 이더넷(fast ethernet)이 주로 사용되므로 1500바이트 크기의 보안 정보를 전달하는데 소요되는 시간은 3ms정도 이다. 따라서 제안된 방법은 핫스폿 지역에서의 실내 WLAN 환경에 적합하다. 또한 메트로 이더넷(metro ethernet)이나 vDSL 등이 사용되는 광대역 MAN(Metropolitan Area Networks) 환경에서도 제

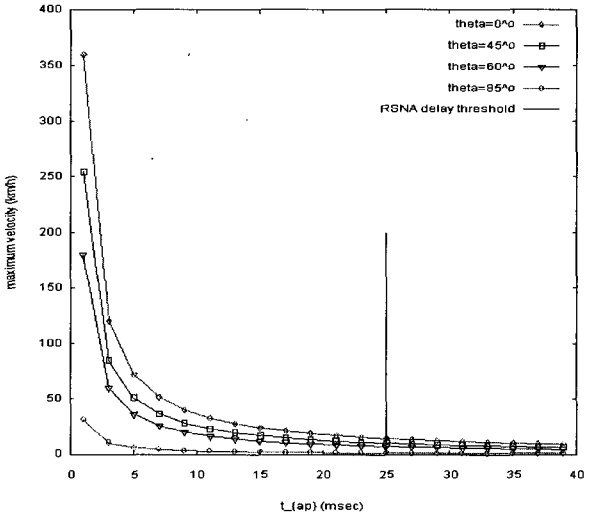


그림 6. MN의 최대 이동 속도
Fig. 6. Maximum velocity of MN supportable.

안된 방법은 실외 광대역 무선 액세스 방법으로서 사용 가능하다.

관리 오버헤드 측면에서 proactive 방법은 n이 MN당 향후 서비스 AP의 개수일 때, AS와 AP는 각 MN당 적어도 $O(n)$의 계산 복잡도 및 저장 공간을 가져야 한다. 반면에 제안된 방법은 AS와 AP가 $O(1)$의 계산 복잡도와 저장 공간 요구를 가지므로 보다 높은 확장성을 가진다.

V. 결 론

본 논문에서는 reactive 방식을 기반으로 WLAN 환경에서 신속하고 보안성있는 핸드오프 메커니즘을 제안하였다. 제안된 방법은 인증 지연시간을 줄이기 위하여 AS대신 AP에서 핸드오프하는 MN을 인증하고 4-way handshake 절차는 핸드오프 세션이 종료되거나 PTK 기간이 만료될 때까지 연기된다. 이러한 과정을 통하여 제안된 방법은 핸드오프 지연시간을 줄이면서도 802.1X 인증 수준의 보안성을 제공할 수 있다. 다른 MN들의 이동성과 핸드오프 MN의 CRT에 의해 RSNA 지연시간이 결정되는 proactive 방식에 비하여, 제안된 방법은 AP와 AS에 과도한 관리 오버헤드를 부과하지 않으면서도 AP사이의 RTT(Round Trip Time)을 기반으로 RSNA 지연시간이 결정되므로 핸드오프 지연시간을 줄일 수 있다.

참 고 문 헌

[1] IEEE Std. 802.11i: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Amendment 6: Medium Access Control (MAC) Security Enhancement, July 2004.

[2] S. Pack and Y. Choi, "Fast Handoff Scheme Based on Mobility Prediction in Public Wireless LAN Systems", Communications IEE Proc, Vol. 151, no 5, pp 248-295, Aug. 2004.

[3] A. Mishra et al, "Proactive Key Distribution Using Neighbor Graphs", IEEE Wireless Communications, Vol 11, no 1, pp26-36, Feb. 2004.

[4] B. Aboba and D. Simon, "PPP EAP TLS Authentication Protocol", RFC 2716, Oct. 1999.

[5] IEEE Std. 802.11f: IEEE Trial-Use Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol Across Distributed Systems Supporting IEEE802.11 Operation, July 2003.

[6] M. M. Zonoozi and P. Dassanayake, "User Mobility Modeling and Characterization of Mobility Patterns", IEEE JSAC, Vol 15, no. 7, pp1239-1252, Sep. 1997.

[7] H. Xie et al, "Dynamic Location Area Management and Performance Analysis" Proc. VTC, pp536-539, May 1993.

[8] J. W. Branch et al, "Autonomic 802.11 Wireless LAN Security Auditing", IEEE Security and Privacy, Vol. 2, no. 3, pp56-65, May 2004.

[9] K. L. Yeung and S. Nanda, "Optimal Mobile-Determined Micro-Macro Cell Selection", Proc. PIMRC, pp294-299, Sep. 1995.

저 자 소 개

박 재 성(정회원)

1995년 연세대학교 전자공학과 학사 졸업.
1997년 연세대학교 전자공학과 석사 졸업.
2001년 연세대학교 전기전자 공학과 박사 졸업.
2001년~2002년 Univ. Minnesota Post Doc.
2002년~2005년 LG전자 선임연구원
2005년~현재 수원대학교 인터넷정보공학과 전임강사
<주관심분야 : 4세대 무선통신망>

임 유 진(정회원)

1995년 숙명여자대학교 전산학과 학사 졸업.
1997년 숙명여자대학교 전산학과 석사 졸업.
2000년 숙명여자대학교 전산학과 박사 졸업.
2000년 서울대학교 박사후연구원.
2000년~2002년 서울시립대학교 연구교수.
2002년~2003년 Univ. of California Los Angeles 박사 후 연구원
2003년~2004년 삼성종합기술원 전문연구원.
2004년~현재 수원대학교 정보미디어학과 전임강사
<주관심분야 : 센서네트워크, 애드혹네트워크>