모바일 네트워크에서 로밍을 위한 계층적 인증 방법

정회원 홍 기 훈*, 정 수 환**°

A Fast Authentication based on Hierarchical Key Structure for Roaming Mobile Nodes Between Domains

Kihun Hong*, Souhwan Jung**° *Regular Members*

요 약

이 논문에서는 모바일 네트워크에서 이동 노드의 로밍을 위한 해시 기반의 인증 방법을 제안한다. IEEE 802.11과 802.16 기반의 인증 방법은 많은 지연 시간과 계산 과부하로 인하여 핸드오버와 로밍의 인증방법으로 적용하기 부적절하다. 따라서 다양한 방법들이 제안되었지만, 기존의 방법들은 인증의 보안을 약화시키거나 이동 시마다 홈 인증 서버에 과도한 인증 부담을 부여한다. 이 논문에서는 계층적 인증키 관리 구조를 통해 홈 인증 서버의 관리 부담 감소와 핸드오버를 위한 인증 방법의 보안 강화에 초점을 맞추고 있다. 제안하는 방법은 인증키에 해시 키 체인을 적용하여 계층적으로 관리함으로써 홈 인증 서버의 관리 부담을 로컬 인증 서버와 엑세스 포인트로 분산시키고 각 인증 서버와 엑세스 포인트간에 인증키를 독립화하여 보안을 강화한다.

Key Words : Mobile networks, Authentication, Handover, Roaming

ABSTRACT

This paper proposes a fast authentication scheme based on hierarchical key structure (HiFA) for roaming mobile nodes in both intra-domain and inter-domain. The full authentication procedure standardized in IEEE 802.11 and 802.16 is difficult to be applied to a handover since it needs a heavy operation and long delay time during a handover. Though a number of schemes were proposed to solve the problem, the existing schemes might degrade the security of authentication or impose heavy administrative burden on the home authentication server. The main contribution of this paper is to reduce the communication and computation overhead of the home authentication server without degrading the security strength of the fast roaming authentication using hierarchical authentication key structure. The proposed scheme in this paper decentralizes the administrative burden of the home authentication server to other network entities such as a local authentication server or access point and supports the security separation of the authentication key among local authentication servers using hash key chain.

Ⅰ. 서 론

인터넷 접속 환경이 무선 형태로 바뀌고 인터넷 환경은 이동 네트워크 형태로 급속히 변화함에 따라 이동 접속 및 끊김 없는 접속 서비스에 대한 많은 연구가 진행되고 있다. IEEE 802.11[1] 표준은 무선 접속뿐만 아니라 여러 엑세스 포인트 (AP)를 통한 접속 노드의 이동성도 지원한다. 그러나 이동 노드의 핸드오버는 probe, decision, re-authentication, re-association과 같은 많은 작업을 수행하기 때

※ 본 연구는 숭실대학교 교내연구비 지원으로 수행되었습니다.
* 미 캘리포니아 주립대 (데이비스) 컴퓨터학과 (khhong@ucdavis.edu)
** 숭실대학교 정보통신전자공학부 (souhwanj@ssu.ac.kr) (°: 교신저자)
논문번호 : KICS2006-03-108, 접수일자 : 2006년 3월 3일, 최종논문접수일자 : 2006년 12월 7일

문에 지연 시간을 가지게 된다. 반면에 인터넷 서비스는 기존의 텍스트 기반이 아닌 멀티미디어 환경으로 바뀌고 있기 때문에 오디오나 비디오 기반의 실시간 서비스들은 이러한 지연 시간으로 인하여 서비스의 질이 떨어진다. 이 논문에서는 이동 노드의 핸드오버에 의해 발생하는 지연 시간을 감소시키는 방법에 대해 언급할 것이다. 이동 노드가 처음 네트워크에 접속하게 되면 IEEE 802.11의 EAP(Extensible Authentication Protocol)/TLS(Transport Layer Security)[3]기반의 인증 방법을 수행하게 되는데 이 절차는 1초 이상의 지연 시간을 가지게 되므로 이 방법을 핸드오버의 인증에 적용하기 어렵다. 이러한 지연 시간 문제를 해결하기 위해 pre-authentication 기반의 security context 전달 방법[6]과 proactive key distribution 방법[5]이 제안되었다. Pre-authentication 인증 방법들은 이동 노드가 접속 포인트를 바꾸기 전에 인증을 미리 수행하므로 비슷한 인증 지연 시간을 가지게 된다. IEEE 802.11i의 pre-authentication 방법은 TLS 연결 과정을 통해 과도한 통신 과부하 및 지연 시간을 가지게 된다. Security context 전달 방법은 현재의 AP에서 사용한 키를 해시한 후 IAPP(Inter-Access Point Protocol)[2]를 이용하여 안전하게 이웃 AP들에게 키를 전달한다. 그러나 이러한 종류의 해결 방법들은 핸드오버 이후에도 여전히 이전 AP가 인증키를 알고 있는 보안적 문제가 존재한다. 마지막으로 proactive key distribution 방법은 이웃 그래프를 이용하여 인증 서버가 새로운 PMK(Pair-wise Master Key)를 현재 서비스 중인 AP의 이웃 AP들에게 모바일 노드의 이동전에 한 홉 먼저 키를 분배하는 방법이다. 그러나 이러한 방법은 홈 인증 서버가 이웃 그래프와 키의 생성 및 전달 등 모든 인증 처리의 관리 부담을 책임져야 하므로 홈 인증 서버의 과부하가 심하다. 따라서 이 논문에서는 홈 인증 서버의 관리 과부하가 적으며 보안적 문제가 없는 핸드오버를 위한 인증 방법에 초점을 맞추고자 한다.

이 논문에서 제안하는 계층적 인증 관리 방법인 HiFA(a hierarchical fast authentication scheme for roaming mobile nodes between domains)의 핵심 아이디어는 홈 인증 서버와 모바일 노드 사이에 해시 체인을 이용하여 추가적인 메시지 교환없이 인증키를 갱신하는 것이다. 홈 인증 서버에서 생성된 LMK(Local Master Key)는 모바일 노드가 이동하는 각 도메인의 로컬 인증 서버에 주어지며, 각 로컬 인증 서버는 새로운 PMK를 이 LMK와 이전 PMK로부터 생성한다. 해시 체인의 초기값을 가지고 있는 모바일 노드와 홈 인증 서버는 상호간에 메시지 교환없이 해시 체인을 이용하여 새로운 LMK를 만들 수 있다. 해시 체인으로부터 도출된 키는 로컬 인증 서버간 인증키의 보안적 강도를 강화하고 홈 인증 서버의 관리 부담을 로컬 인증 서버들에게 분산한다.

이 논문은 Ⅱ장에서 모바일 네트워크의 인증 환경과 문제점을 언급하고 관련 연구들을 살펴본다. Ⅲ장에서는 제안하는 인증 방법의 초기 인증 절차와 핸드오버 인증 절차에 대해 설명하고 Ⅳ장에서 제안하는 방법의 보안적 문제를 분석한다. Ⅴ장에서 제안하는 방법과 기존 방법들의 계산 및 통신 과부하를 비교하고 Ⅵ장에서 결론을 맺는다.

Ⅱ. 기존 연구들

인증 관점에서 모바일 네트워크 요소는 모바일 노드(MN)와 엑세스 포인트(AP) 그리고 엑세스 라우터(AR)와 현재 모바일 노드가 위치하고 있는 도메인의 로컬 인증 서버(LAS), 홈 인증 서버(HAS) 등으로 구분할 수 있다. 모바일 노드는 네트워크에 접속하기 위해서 홈 인증 서버를 거쳐 초기 인증을 받아야 한다. 그러나 EAP/TLS와 AAA(Authorization, Authentication and Accounting)로 구성된 초기 인증은 많은 네트워크 자원을 소비하고 지연 시간을 요구하기 때문에 모바일 노드의 이동으로 발생하는 핸드오버의 인증 방법으로 적당하지 않다. 모바일 노드가 현재의 AP에서 새로운 AP로 이동시에 모바일 노드는 새로운 AP를 통해 재인증 받아야 하고 이것은 지연 시간을 필요로 한다. 만일 모바일 노드가 VoIP와 같은 실시간 서비스를 제공하면서 이동한다면 사용자는 서비스 질의 저하를 경험하게 될 것이다. 따라서 핸드오버를 위한 빠른 인증 방법이 요구된다. 이를 위해 초기 연구에서는 핸드오버 중에 인증을 수행하는 방법들이 제안되었지만 이것은 최소한이라도 지연 시간을 요구하므로 최근에는 이동전에 인증을 수행하는 pre-authentication 기반의 방법들이 많이 연구되고 있다.

IEEE 802.11i에 정의되어 있는 pre-authentication 방법[1]은 모바일 노드가 IEEE 802.1x EAPOL-start 메시지를 현재의 AP를 경유하여 이동할 AP로 보냄으로써 인증을 시작한다. 인증 서버는 모바일 노드를 인증한 후에 PMK를 이동할 AP로 보내게 된다. 그러나 이 방법은 모바일 노드와 인증 서버 사이에

TLS 세션을 사용하므로 많은 메시지 교환과 지연 시간이 요구된다.

Predictive authentication 방법[4]은 사용자의 이동 패턴과 AP들의 위치를 기반으로 이웃 AP들의 집합인 FHR (Frequent Handoff Region)을 구성하여 FHR안에 있는 AP들에게 모바일 노드를 미리 인증시킨다. 인증 서버는 모바일 노드의 인증 요청에 대해 인증키를 포함한 다수의 응답 메시지를 FHR에 포함된 AP들에게 보내줌으로써 한번에 인증을 수행한다. 그러나 이 방법은 FHR이외의 지역으로 초기 인증없이 핸드오버를 위한 연속적인 인증 방법을 제공하지 못하고, 같은 인증키를 여러 AP들에게 분배하므로 키 노출에 의해 모든 AP의 키가 노출되는 보안적 문제를 해결하지 못한다.

Proactive key distribution 인증 방법[5]은 인증 절차의 지연 시간을 줄이기 위해 모바일 노드의 이동에 앞서 인증키를 미리 이웃 AP들에게 분배한다. 인증 서버는 이웃 그래프를 이용하여 현재 AP의 이웃 AP들에 대한 정보를 가지고 있으며 현재의 PMK와 이웃 AP의 MAC 주소 그리고 모바일 노드의 MAC 주소를 이용하여 새로운 PMK를 만들어 각 이웃 AP들에게 전달한다. 이것은 인증의 지연을 줄이기 위해 효율적인 방법이지만 이웃 그래프의 계산과 키 전달, 암호화, PMK 생성 등 대부분의 인증 수행을 인증 서버가 수행하여야 하므로 인증 관리 부담이 집중되는 단점이 있다.

Wang에 의해 제안된 난수 교환을 이용한 인증 방법은 현재의 AP가 자신만이 알고 있는 난수와 exclusive OR된 키를 모바일 노드와 이동할 AP에게 전달한다. 그리고 키를 받은 두 노드는 난수를 서로 교환하고 이 난수와 이전 AP로부터 받은 키를 이용하여 새로운 PMK를 생성한다. 이것은 간단하고 인증 서버를 거치지 않는 효율적인 방법이지만 이전 AP가 공격당하여 exclusive OR된 키가 노출되면 모바일 노드와 이동할 AP간에 평문으로 교환된 난수를 쉽게 얻을 수 있기 때문에 보안적인 문제점을 가진다. Context 전달 방법도 같은 문제점을 가지게 된다. 지금까지 기존 인증 방법들을 살펴보고 그것들의 문제점을 분석해 보았다. 따라서 인증 처리의 부담이 분산되고 보안적 문제점이 존재하지 않는 핸드오버를 위한 안전하고 빠른 인증 방법이 요구된다.

모바일 네트워크의 각 개체들은 그 들 간에 채널 보호를 위해 신뢰 관계를 가지게 된다. 그림 1은

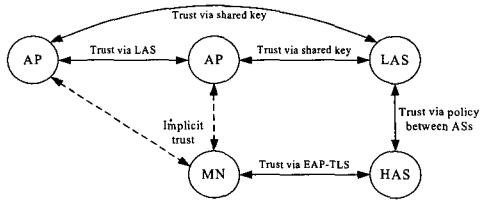

그림 1. 네트워크 개체간의 신뢰관계

모바일 노드와 엑세스 포인트, 모바일 노드가 방문 중인 도메인의 로컬 인증 서버 그리고 홈 인증 서버 등 상호간의 신뢰 관계를 보여주고 있다. AP는 이웃 AP들 간에 서로 신뢰 관계를 가지며 이런 신뢰 관계는 IAPP의 context 보호를 지원하게 된다. Context 전달은 네트워크에서 발생하는 다양한 이벤트와 모바일 노드의 이동성 및 서비스 셋을 관리하며 채널 보호를 위해 AP들 간에 IP 주소와 ID의 맵핑이나 키의 분배 등을 제공하기 위해 RADIUS 기반 구조를 포함한다. AP는 또한 로컬 인증 서버와 공유키를 이용하여 신뢰 관계를 구성한다. 모바일 노드는 홈 인증 서버와 초기 인증에서 수행하는 EAP-TLS를 통한 신뢰 관계를 이용하여 채널을 보호한다. 홈 인증 서버와 로컬 인증 서버는 미리 협의된 로밍 서비스 정책에 의해 신뢰 관계를 가지게 될 것이다. 모바일 노드는 AP와 직접적인 신뢰 관계를 가지지는 않지만 다른 개체들을 통해 신뢰 관계를 생성할 것이다.

Ⅲ. 핸드오버를 위한 계층적 인증키 관리 방법

이 장에서는 제안하는 방법인 HiFA (a hierarchical fast authentication scheme for roaming mobile nodes between domains)의 초기 인증 방법과 핸드오버를 위한 pre-authentication 방법에 대해 상세히 설명할 것이다. 제안하는 방법의 핵심 아이디어는 초기 인증 이후에 모바일 노드가 이동한 도메인내의 로컬 인증 서버에게 홈 인증 서버가 인증키를 전달하고, 로컬 인증 서버는 PMK를 생성하여 각 엑세스 포인트에게 전달하는 것이다. 이러한 방법은 모바일 노드의 이동시 마다 홈 인증 서버까지 경유해야 하는 통신 과부하 및 홈 인증 서버의 관리 부담을 줄일 수 있다.

3.1 초기 인증 절차

모바일 노드가 부팅 시 AP는 모바일 노드에게

네트워크 접속을 위한 인증을 요청하게 되고, 모바일 노드는 EAP-TLS 인증 절차를 거쳐 홈 인증 서버에게 인증 받게 된다. 이 과정을 통해 두 개체는 마스터 키(MK)와 난수(RN)를 공유하게 된다. 홈 인증 서버는 모바일 노드의 ID와 난수 그리고 다음 절에서 설명할 해시 체인을 통해 로컬 마스터 키(LMK_0)를 생성하여 로컬 인증 서버에 보내게 된다. 이후에 로컬 인증 서버는 모바일 노드와 현재의 AP 간 인증 및 채널 보호를 위한 PMK_0를 다음과 같이 생성한다.

$$PMK_0 = prf(LMK_0, RN \mid AP\_MAC \mid MN\_MAC)$$

로컬 인증 서버는 LMK_0와 난수 그리고 AP의 MAC 주소(AP_MAC)와 MN의 MAC 주소(MN_MAC)를 랜덤 함수(prf)을 통해 PMK_0를 생성한 후에 현재의 AP에게 전달한다. 모바일 노드도 자신이 가지고 있는 정보를 기반으로 같은 PMK_0를 생성하며 이렇게 같은 키를 공유하게 된 AP와 MN은 PMK_0로부터 채널 암호키와 MIC(Message Integrity Check) 키 등을 추출하고 암호 알고리즘을 결정한다.

3.2 도메인내 이동을 위한 pre-authentication

초기 인증이 수행된 후에 모바일 노드의 이동에 대비하여 현재의 AP는 이웃 AP들과 핸드오버를 위한 pre-authentication을 수행한다. 현재 서비스 중인 AP는 핸드오버 키(HOK)를 이웃 AP들에게 IAPP의 context transfer를 이용하여 전달한다. 현재 AP는 IAPP를 통해 이웃 AP들을 알 수 있고 보호된 채널을 제공할 수 있으며 핸드오버 키를 다음과 같이 만들 수 있다.

$$HOK_i = prf(PMK_{i-1}, 0)$$

핸드오버 키의 인덱스 i는 모바일 노드의 핸드오버 순서를 의미하며 MN의 핸드오버에 대해 1부터 n까지 연속적으로 사용한다. HOK는 랜덤 함수에 의해 생성되므로 HOK를 이용하여 PMK_{i-1}를 생성할 수 없다. 그림 2는 현재의 AP가 한 홉 거리에 떨어져 있는 이웃 AP들에게 IAPP를 이용하여 HOK를 전달하는 것을 보여준다. 모바일 노드는 이 이웃 AP들 중에 하나의 AP로 이동할 수 있을 것이며 G는 현재 서비스 중인 AP의 이웃 AP들 집합이다.

$$G = \{AP1, AP2, AP3, AP4, AP5\}$$

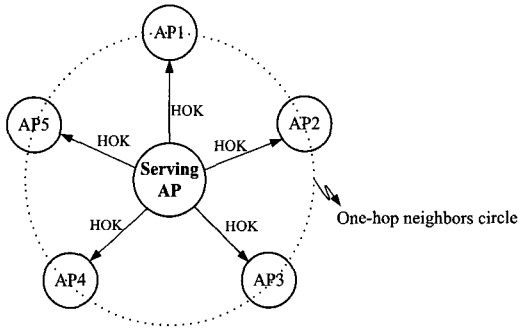

그림 2. 핸드오버 키 분배

핸드오버 키의 분배 이후에 HOK를 받은 각 AP들은 현재 서비스 중인 AP의 ID, MN의 ID, 자신의 ID, MN과 자신의 MAC 주소, HOK, LMK 인덱스, PMK 인덱스 정보 등을 포함한 PMK Request 메시지를 로컬 인증 서버에 보내 PMK를 요청한다. 그림 3은 모바일 노드가 서비스 중인 AP(sAP)에서 같은 로컬 인증 서버에 의해 관리되는 도메인 내의 다른 이웃 AP(nAP)로 이동할 때의 pre-authentication 절차를 묘사하고 있다. 로컬 인증 서버는 PMK를 요청한 AP가 현재 모바일 노드가 있는 지역의 이웃 AP인지를 확인하기 위해 받은 정보 중에 HOK를 확인한다. 로컬 인증 서버는 이미 전에 만들어 놓은 PMK_{i-1}을 알고 있기 때문에 랜덤 함수로 계산하여 HOK를 확인할 수 있다. HOK가 같으면 로컬 인증 서버는 PMK를 계산하여 요청한 AP에게 보내주는데 PMK 계산은 다음과 같다.

$$PMK_i = prf(LMK_0, PMK_{i-1} \mid AP\_MAC \mid MN\_MAC)$$

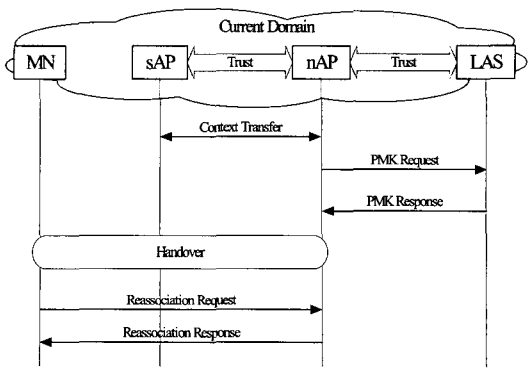

그림 3. MN의 도메인내 이동을 위한 pre-authentication 절차

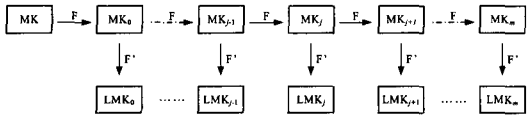

그림 4. MK 해시 체인

PMK Response 메시지를 통해 PMK_i를 받은 AP는 데, 특정 시간 안에 자신에게 이 모바일 노드의 핸드오버가 발생하지 않으면 이 키 정보들은 메모리에서 삭제된다. 만일 모바일 노드가 이 AP에게로 이동하게 되면 모바일 노드는 PMK_i를 자신이 만들 수 있기 때문에 홈 인증 서버를 거친 인증을 수행하지 않고 단순히 이 AP와 PMK_i를 확인하는 절차만을 수행하면 된다.

3.3 도메인간 이동을 위한 pre-authentication

모바일 노드는 어떤 장소든지 이동할 수 있기 때문에 현재의 관리 도메인에서 다른 관리 도메인으로의 이동도 고려하여야 한다. 이 경우 새롭게 도착한 도메인의 로컬 인증 서버는 로컬 마스터 키(LMK)를 가지고 있지 않고 이 모바일 노드가 인증된 노드인지를 확인할 수 없기 때문에 홈 인증 서버를 거친 인증이 필요하다. 현재의 로컬 인증 서버가 이웃 도메인의 로컬 인증 서버에게 현재의 로컬 마스터 키(LMK)를 전달할 수도 있지만 같은 키가 여러 도메인에 의해 공유되는 보안상의 문제가 발생하므로 LMK는 각 도메인마다 다른 키이어야 한다. 따라서 이 논문에서는 모바일 노드의 도메인간 이동에 대해 홈 인증 서버가 가지고 있는 마스터키로부터 추출된 새로운 LMK를 새로운 로컬 인증 서버에 할당한다. 이러한 새로운 LMK의 생성은 해시 체인 방법이 사용되며 그림 4에 묘사되어 있다. 초기 인증 과정을 거쳐 마스터키는 모바일 노드와 홈 인증 서버에 공유되어 있으며 이 키를 기반으로 두 개의 서로 다른 랜덤 함수로 각기 LMK를 생성한다. F와 F'는 서로 다른 랜덤 함수이며 LMK의

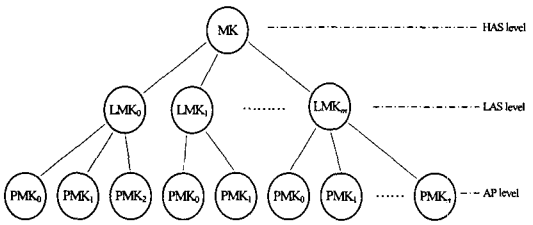

그림 5. 계층적 마스터키 구조

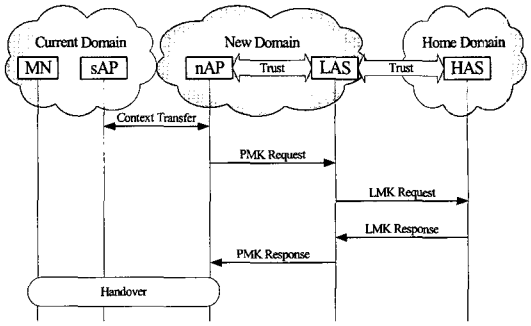

그림 6. MN의 도메인간 이동을 위한 pre-authentication 절차

인덱스 j는 모바일 노드의 도메인간 로밍의 순서를 의미하고 각 로밍에 대해 0부터 m까지 사용한다. 마스터키(MK)는 랜덤 함수의 암호학적 특성에 의해 LMK로부터 생성될 수 없다.

마스터키로부터 추출되는 키들의 전체 구조는 그림 5와 같이 표현할 수 있는데 MK는 인덱스 j에 따라 각 LMK로 나뉘어지고, 각 LMK는 모바일 노드와 각 AP의 MAC 주소와 함께 각 PMK의 추출에 사용된다. 이러한 구조는 홈 인증 서버가 모바일 노드의 도메인내 이동과 도메인간 이동에 대해 초기 인증을 수행하지 않고 인증키를 효율적으로 관리하는데 도움이 된다. 특히, LAS 레벨과 AP 레벨에서 동일 레벨의 키간에 서로 다른 정보로 랜덤 함수를 통해 키를 생성하므로 보안적인 독립을 보장한다. 각 레벨의 인덱스 m과 n은 보안 정책에 의해 정의될 수 있다.

모바일 노드가 현재 도메인의 가장자리에 위치할 때 이웃 AP(nAP)중 하나의 AP는 다른 도메인에 위치할 수 있는데 이 경우의 pre-authentication 절차가 그림 6에 묘사되어 있다. 앞에서 설명한 도메인 내에서 이동시 pre-authentication 절차와 마찬가지로 서비스 중인 AP가 HOK를 context transfer로 전달하면 새로운 도메인에 있는 이웃 AP는 PMK Request 메시지를 통해 PMK를 요청할 것이다. 그러나 새로운 도메인의 로컬 인증 서버는 ID 확인을 통해 이 모바일 노드에 대한 LMK를 가지고 있지 않기 때문에 MN의 ID를 포함한 LMK Request 메시지를 홈 인증 서버에 보내 LMK를 요청한다. 요청 받은 홈 인증 서버는 즉시 앞에서 언급한 해시 체인 생성 방법을 통해 LMK_j를 생성한 후 LMK Response 메시지를 통해 로컬 인증 서버에게 전달한다. LMK_j를 받은 로컬 인증 서버는 이제 PMK를 생성할 수 있으므로 이를 다음과 같이 생성한다.

$$PMK_0 = prf(LMK_j, HOK_i \mid AP\_MAC \mid MN\_MAC)$$

모바일 노드의 로밍에 의한 PMK_0의 계산은 PMK_{i-1} 대신에 HOK를 사용한다. 로컬 인증 서버는 생성된 PMK와 LMK 및 PMK 인덱스 정보를 그림 6의 PMK Response 메시지를 이용하여 요청한 AP에게 전달한다. 이러한 키들의 인덱스 정보는 모바일 노드가 이동해 왔을 때 키들의 동기를 맞추는데 사용될 것이다. 홈 인증 서버와 로컬 인증 서버와의 통신 채널은 Ⅱ장에서 언급한 신뢰관계에 의해 보호될 것이다. 모바일 노드의 로밍이후에 같은 도메인 내의 핸드오버를 위한 PMK의 계산은 다음과 같다.

$$PMK_i = prf(LMK_j, PMK_{i-1} \mid AP\_MAC \mid MN\_MAC)$$

3.4 Post-authentication

Pre-authentication 이후에 모바일 노드는 이웃 AP중에 어느 노드든지 이동할 수 있다. 만일 모바일 노드가 하나의 AP로 이동하였다면 모바일 노드와 이 AP는 re-association 이후에 미리 공유된 PMK의 동일 여부를 확인하고 키의 인덱스 정보를 통해 동기를 확인하여야 한다. 이 과정 후에 PMK는 암호화 키와 메시지 인증키의 추출에 사용된다.

Ⅳ. 보안 분석

이 논문에서 제안하는 인증 방법의 주요 목적은 핸드오버나 로밍을 위한 간소화된 pre-authentication 방법의 보안을 강화하는 것이다. 제안한 방법에서 로컬 인증 서버간은 해시 체인에 의해 모바일 노드의 인증키가 각각 분리되었다. 이는 홈 인증 서버가 모바일 노드의 로밍에 대해 두 개의 서로 다른 랜덤 함수를 사용하여 로컬 인증 서버에게 각기 다른 LMK를 할당하기 때문에 가능하다. 만일 공격자가 LMK_j를 얻었다 할지라고 랜덤 함수의 특성에 의해 LMK_{j-1}나 LMK_{j+1}을 얻을 수 없다. 즉, LMK_j는 F' 함수에 의해 고립된다. 제안하는 방법은 또한 LMK와 이전 PMK를 이용한 PMK 계산으로 AP들 간의 보안적 독립을 보장한다. AP는 일반적으로 공공의 장소에 설치되는 장비로 공격자가 쉽게 접근하여 메모리의 내용을 파악할 수 있다. 그러나 제안하는 방법은 로컬 인증 서버의 LMK 없이 이 AP에서 유출된 PMK를 이용하여 핸드오버 이전 혹은 이후의 PMK를 생성할 수 없다. 또한 PMK의 요청은 오직 현재 모바일 노드를 서비스 중인 AP의 이웃 노드들만이 가능하다. 왜냐하면 로컬 인증 서버는 PMK 요청과 동시에 전달되는 HOK를 확인하기 때문에 요청 AP는 IAPP의 안전한 채널을 통해 전달되는 현재 AP의 HOK를 가져야 하기 때문이다.

Ⅴ. 성능 분석

핸드오버 중에 인증을 수행하는 방법들은 pre-authentication 방법들에 비해 많은 지연 시간을 가질 수밖에 없기 때문에 성능 비교에서 제외한다. Predictive authentication 방법과 Wang에 의해 제안된 난수 교환을 통한 인증 방법은 앞에서 언급한 같은 인증키의 분배 및 난수 도청을 통한 이전 AP의 인증키 유추 등 보안적 문제를 가지므로 역시 제안하는 방법과 성능을 비교하기에 적합하지 않다. 따라서 이 장에서는 802.11i에 정의된 pre-authentication 방법과 proactive key distribution 인증 방법을 제안하는 HiFA와 비교할 것이다.

모바일 노드가 외부 도메인에 방문하여 그 도메인 내에서 계속 이동하는 경우에 앞의 3가지 비교 인증 방법들의 인증 메시지 경로를 그림 7에서 보여주고 있다. 도메인 내부의 이동임에도 불구하고 그림에서 pre-authentication으로 표시된 802.11i의 인증방법은 모바일 노드부터 현재 AP와 이웃 AP

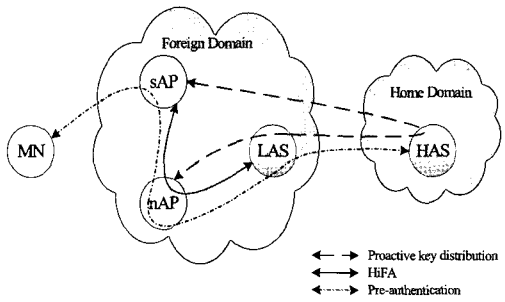

그림 7. MN의 외부 도메인내 이동에 대한 pre-authentication 경로 비교

그리고 홈 인증 서버까지의 모든 경로를 거쳐 인증을 수행한다. 또한 proactive key distribution 인증 방법 역시 홈 인증 서버를 거쳐 인증 절차를 수행하고 있다. 그러나 제안하는 인증 방법인 HiFA는 현재 AP와 이웃 AP가 같은 도메인 내에 위치하는 로컬 인증 서버를 통해 인증을 수행하므로 상대적으로 적은 경로를 가지게 된다.

표 1. 과부하 비교 (u는 이웃 AP들의 평균수이며 통신 과부하는 메시지의 수를 의미한다.)

		Pre-authentication of 802.11i	Proactive key distribution	HiFA	
				Intra-domain	Inter-domain
Comm. overhead per a MN	MN-sAP	$8u$	0	0	0
	sAP-nAP	$8u$	0	u	u
	nAP-LAS	$6u$	$4u$	$2u$	$2u$
	LAS-HAS	$6u$	$4u$	0	$2u$
Neighbor discovery		MN	HAS	APs	

표 2. 시뮬레이션 파라미터

Parameters	Description
u	the average number of neighboring APs u = 6.
h	the number of handovers per ten minutes in intra-domain h = 10.
r	the number of roaming per hour in inter-domain r = 6.
Comm. cost	the number of messages.

성능 관점에서 pre-authentication 방법들은 핸드오버 시에 지연 시간을 추가하지 않기 때문에 주요 초점은 통신 및 계산 과부하이다. 특히, 이러한 과부하는 하나의 노드에 집중되어서는 안 된다. 802.11i의 인증방법에서 미리 설립된 TLS 세션을 사용한다고 가정하면, 비교하는 세 개의 인증 방법들은 유사한 계산 과부하를 가지게 되지만 proactive key distribution 인증 방법은 이웃 그래프의 계산과 PMK의 계산 및 전달 등 모든 인증 처리가 홈 인증 서버에 집중되는 단점이 있다. 표 1은 세 인증 방법들의 과부하 비교를 보여주고 있다. 메시지의 비교에서 802.11i의 인증방법은 모바일 노드에서 홈 인증 서버까지 많은 메시지의 교환이 필요하다. 이것은 또한 메시지 교환동안에 많은 지연 시간이 발생하는 것을 의미한다. 그러나 제안하는 인증 방법은 적은 메시지 교환으로 인증을 수행하며 특히, 같은 도메인내의 이동에 대해서는 로컬 인증 서버만을 경유한 상대적으로 가장 적은 메시지를 교환한다. Proactive key distribution 인증 방법은 이웃 AP들의 검색을 홈 인증 서버가 수행하지만 HiFA의 경우 AP들에 의해 수행되므로 과부하가 분산되는 것을 알 수 있다.

모바일 노드의 같은 도메인 내 이동은 도메인간 이동보다 상대적으로 많은 것을 알 수 있다. 특히,

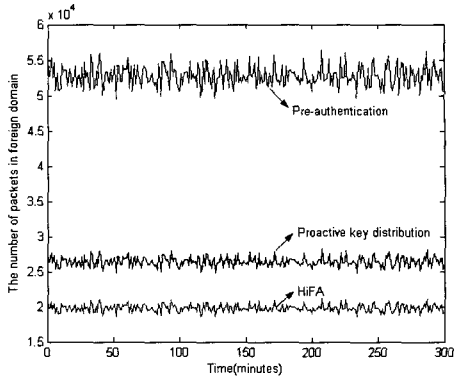

그림 8. MN이 위치하고 있는 방문 도메인 내부의 통신 과부하

모바일 노드가 방문 도메인 내에서 움직일 경우, 홈 인증 서버까지의 거리는 멀기 때문에 홈 인증 서버를 자주 경유해야 하는 인증 방법은 상대적으로 많은 통신 과부하를 유발한다. 앞 서 언급한 세 인증 방법의 통신 과부하를 비교하기 위해 시뮬레이션을 수행하였다. 1000개의 모바일 노드를 가정하고 각 모바일 노드는 10분에 10번의 도메인내 이동과 한 번의 도메인간 이동이 랜덤하게 발생한다고 가정하였다. 시뮬레이션의 파리미터는 표 2에 정의하였다. 시뮬레이션에서는 MN이 외부 도메인에 위치하고 위와 같은 횟수로 이동한다고 가정한 환경에서 각 인증 방법들이 생성하는 메시지를 MN이 위치한 방문 도메인 내부와 방문 도메인과 홈 도메인 사이에서 관찰하였다. 그림 8은 각 방법에 대해 방문 도메인 내에서 매 분마다 메시지의 수를 관찰한 수치이다. 그림에서 pre-authentication으로 표기된 802.11i의 인증방법은 TLS 핸드쉐이크에 의해 가장 많은 메시지가 생성되는 것을 볼 수 있으며, HiFA의 경우 모바일 노드의 도메인 내부 이동에 의한 핸드오버마다 3개의 메시지가 필요하고, 이를 6개의 이웃 노드에 대해 수행하므로 일분 동안 약 이만개의 메시지가 소요되므로 상대적으로 적은 통신 과부하를 유발한다.

그림 9는 같은 시뮬레이션에서 홈 도메인과 방문 도메인 사이에서 메시지 수를 관찰한 것이다. 모바일 노드의 로컬 도메인내 이동에 대해 802.11i 인증 방법과 proactive key distribution 인증 방법은 인증을 위해 원거리의 홈 인증 서버를 거쳐야 하지만 HiFA 방법은 로컬 인증 서버에서 인증을 수행하므로 도메인간 메시지가 발생하지 않는다. 단지, 도메인이 바뀌는 상황에서만 홈 인증 서버를 거쳐 인증을 수행하므로 훨씬 적은 메시지가 발생한다.

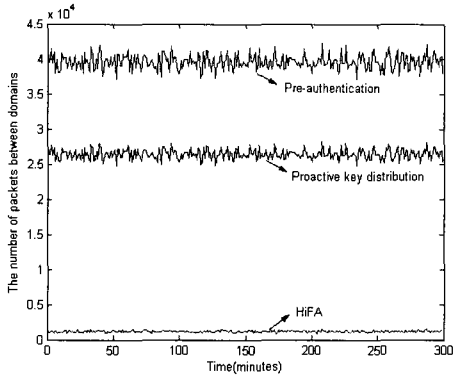

그림 9. MN이 위치하고 있는 방문 도메인과 홈 도메인 사이의 통신 과부하

결과적으로 이 논문에서 제안하는 인증 방법에서 이웃 검색은 AP들에 의해 수행되고 PMK 생성 및 전달은 모바일 노드가 방문중인 도메인내의 로컬 인증 서버에 의해 수행되므로 홈 인증 서버의 부담과 도메인간의 트래픽을 줄일 수 있다.

Ⅵ. 결 론

본 논문에서는 모바일 노드의 외부 도메인 이동에 의해 발생하는 핸드오버와 로밍을 위한 빠른 인증 방법을 제안하였다. 기존 방법들의 주요 문제인 홈 인증 서버의 관리 과부하 문제와 보안 약화를 분석하고 이를 해결할 수 있는 방법을 제안하였다. 제안된 방법은 인증키를 AP와 로컬 인증 서버 그리고 홈 인증 서버 등 계층적으로 관리하여 모바일 노드의 이동 형태에 따라 각 레벨에서 자체적으로 인증을 수행할 수 있도록 한다. 이러한 방법은 홈 인증 서버의 관리 부담을 분산하며 각 레벨간의 인증키의 분리를 통해 보안을 강화할 수 있다. 제안된 방법은 모바일 노드의 이동에 대해 적은 지연 시간과 과부하 분산을 통해 VoIP나 온라인 영화 등 실시간 서비스를 지원하는 모바일 네트워크에 적용될 수 있을 것이다.

참 고 문 헌

[1] IEEE standard, "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 6," IEEE 802.11i, 2004.

[2] IEEE standard, "IEEE Trial-Use Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol Across Distribution Systems," IEEE 802.11f, 2003.

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

[4] S. Pack, Y. Choi, "Fast handoff scheme based on mobility prediction in public wireless LAN systems," *Communications*, IEE Proceedings vol. 151, issue 5, pp. 489-495, Oct. 2004.

[5] A. Mishra, M. Shin, N. L. Petroni, T. C. Clancy, W. A. Arbauch, "Proactive key distribution using neighbor graphs," *IEEE Wireless Communications*, vol. 11, issue 1, pp. 26-36, 2004.

[6] A. Mishra, M. Shin, W. A. Arbauch, "Context Caching using Neighbour Graphs for Fast Handoffs in a Wireless Network," *Proc. of IEEE INFOCOM*, Hong Kong, Mar. 2004.

[7] H. Wang, A. R. Prasad, "Fast Authentication for Inter-domain Handover," ICT 2004, *LNCS* 3124, pp. 973-982, 2004.

[8] M. S. Bargh, R. J. Hulsebosch, E. H. Eertink, A. Prasad, H. Wang, P. Schoo, "Fast Authentication Methods for Handovers between IEEE 802.11 Wireless LANs," *Proc. of WMASH'04*, Oct. 2004.

[9] K. Hong, S. Jung, S. Felix Wu, "A Hash-chain Based Authentication Scheme for Fast Handover in Wireless Network," WISA 2005, *LNCS* 3786, pp. 96-107, Jan. 2006.

[10] A. Perrig, R. Canetti, J. D. Tygar, D. Song, "Efficient Authentication and Signing of Multicast Streams over Lossy Channels," *Proc. of IEEE Security and Privacy Symposium S&P2000*, May 2000.

홍 기 훈 (Kihun Hong) 정회원

2000년 2월 숭실대학교 정보통신공학과 학사
2002년 2월 숭실대학교 정보통신공학과 석사
2006년 2월 숭실대학교 정보통신공학과 박사
2006년 4월~8월 숭실대 유비쿼터스 네트워크 연구센터 선임연구원
2006년 9월~현재 미 캘리포니아 주립대(데이비스) 박사후 연구원
<관심분야> 인증 프로토콜, NGN, VoIP 보안

정 수 환 (Souhwan Jung) 정회원

1985년 2월 서울대학교 전자공학과 졸업
1987년 2월 서울대학교 전자공학과 석사
1988년~1991년 한국통신전임연구원
1996년 미 워싱턴 주립대(시애틀) 박사
1996년~1997년 'Stellar One SW Engineer
1997년~현재 숭실대학교 정보통신전자공학부 부교수
<관심분야> 모바일 인터넷 보안, NEMO Security, VoIP 보안