情報保護學會論文誌
第17卷 第2號, 2007. 4

이기종 FMIPv6 기반의 이동 망에서 이동 노드 주도형 핸드오버 인증 기법

최 재 덕,† 정 수 환‡
숭실대학교 정보통신전자공학부

A Handover Authentication Scheme initiated by Mobile Node for Heterogeneous FMIPv6 Mobile Networks

Jaeduck Choi,† Souhwan Jung‡
School of Electronic Engineering, Soongsil University

요 약

기존의 이동 네트워크에서는 링크 계층에서 액세스 인증과 네트워크 계층에서 FMIPv6의 핸드오버 인증이 독립적으로 수행되어 AAA 인증 서버의 오버헤드 증가 및 잦은 핸드오버 인증 수행으로 인증 지연을 초래하는 문제점이 있었다. 본 논문에서는 이기종 FMIPv6 기반의 이동 네트워크에서 이동 노드 주도형 통합 핸드오버 인증 프로토콜을 제안한다. 제안 기법은 FMIPv6 환경에서 이동 노드가 직접 핸드오버 인증키를 생성하여 인증 서버를 통해 안전하게 NAR로 전송하고, NAR에서는 AP들과 계층적 키 관리 구조를 갖는다. 이동 노드에서 생성한 인증키는 FMIPv6에서 핸드오버 할 때 PAR과 이동 노드 사이에서 FBU 메시지를 안전하게 전송할 수 있고, NAR에서 계층적 키 관리를 통해 이동 노드의 링크 액세스 인증을 수행할 수 있다. 제안 기법은 이동 노드에서 핸드오버 인증키 생성, AAA 서버 기능의 단순화로 AAA 서버의 오버헤드를 줄이고, 잦은 핸드오버 인증 수행 절차를 감소시킴으로써 핸드오버 인증 지연 시간을 감소시킨다. 또한 제안 기법은 PFS, PBS를 제공하고 DoS 공격에 안전하다.

ABSTRACT

The existing handover authentication schemes have authentication delay and overhead of the authentication server since they have been separately studied handover authentication at the link layer and the network layer. This paper proposes a handover authentication scheme initiated by Mobile Node on FMIPv6 based mobile access networks. The main idea of the paper is to generate a session key at the mobile node side, and transfer it to the next Access Router through the authentication server. Also, the scheme has a hierarchical key management at access router. There are two advantages of the scheme. First, the generated session key can be utilized for protecting the binding update messages and also for access authentication. Second, hierarchical key management at the access router reduced the handover delay time. The security aspects on the against PFS, PBS, and DoS attack of proposed scheme are discussed.

Keywords : *Handover Authentication, Network Access, Securing FBU, IEEE 802.11, FMIPv6*

접수일: 2006년 10월 10일; 채택일: 2007년 1월 31일
* 본 연구는 숭실대학교 교내연구비 지원에 의해 이루어진 연구 결과임.

† 주저자, cjduck@cns.ssu.ac.kr
‡ 교신저자, souhwanj@ssu.ac.kr

Ⅰ. 서 론

IETF MIPSHOP WG은 MIPv6 (Mobile IPv6)[1] 기본 모델에서 이동성 감지, CoA 설정, 위치 정보 업데이트 때문에 발생하는 핸드오버 지연을 개선하기 위하여 FMIPv6 (Fast MIPv6)[2] 프로토콜을 제정하였다. FMIPv6에서는 이동 노드가 현재 액세스 라우터 PAR (Previous Access Router)에서 다음 액세스 라우터 NAR (Next Access Router)로 이동하기 전에 네트워크 계층에서 핸드오버 과정을 FBU (Fast Binding Update) 메시지를 통하여 미리 수행하기 때문에 기본 MIPv6 모델보다 핸드오버 지연 시간을 줄일 수 있다. 네트워크 계층 핸드오버 기술인 FMIPv6는 다양한 링크 계층 기술 기반과 함께 이동 노드의 이동성을 지원하는데 사용된다. FMIPv6와 함께 고속 핸드오버를 지원하기 위해 활발히 논의되는 링크 계층 기술로는 IEEE 802.11과 802.16이 있다.[3][4]

이동 노드의 핸드오버시 안전한 고속 핸드오버를 지원하기 위하여 네트워크 및 링크 계층에서 각각 핸드오버 인증에 대해 활발히 연구가 진행되고 있다. MIPv6 및 FMIPv6 환경에서 이동 노드들은 초기 EAP full 인증을 수행한 후, 이동 노드와 AAA 서버 간에 EMSK (Extended Master Session Key)를 생성하고, AAA 서버는 현재 AR에게 BU 또는 FBU 메시지를 보호하기 위한 키를 분배한다. 이동 노드의 네트워크 계층 핸드오버 인증은 핸드오버 할 때마다 AR들과 이동 노드간 BU 또는 FBU 시그널링 메시지 보호에 대한 PFS (Perfect Forward Secrecy)와 PBS (Perfect Backward Secrecy)를 제공해주기 위하여 초기 EAP full 인증 과정을 통해 생성된 EMSK를 사용하여 새로운 핸드오버 인증키를 새롭게 생성한다. 이러한 네트워크 계층에서 핸드오버 인증 방식이[5][6] 연구되고 있지만, 모든 이동 노드들의 인증키 생성 및 분배 과정을 AAA (Authentication, Authorization and Accounting) 서버에서 수행하기 때문에 AAA 서버의 오버헤드가 발생한다. 링크 계층의 인증 기술로는 IEEE 802.1x 표준 문서에서 정의하고 있는 802.11 WLAN (Wireless LAN) 인증 기술과[7] IEEE 802.16 표준에서 정의하고 있는 PKM (Privacy and Key Management)[8] 인증 기술이 있다. 그러나 EAP-TLS (Extensible Authentication Protocol-Transport Layer Security) 기반의 802.1x 인증 기술은 약 1000ms의 인증 시간을[9] 요구하고 있기 때문에 핸드오버 인증 기술로 적합하지 않다. 또한 802.16 인증 기술인 PKM 프로토콜은 현재 BS (Base Station)에서 다음 BS로 핸드오버 인증키를 해쉬해서 전달하기 때문에 PFS가 제공되지 않는 보안상 취약성이 존재한다. 이와 같은 문제점을 해결하기 위해 초기 이동 노드의 부팅 과정에서는 EAP-TLS와 같은 인증을 수행하고, 핸드오버가 발생할 때에는 EAP-TLS 초기 인증 과정에서 생성된 EMSK를 기반으로 핸드오버 인증키를 생성하고, 핸드오버 인증키를 기반으로 무선 채널에서 데이터를 보호하기 위한 키를 생성하는 방식이 다양하게 연구되었다. 이와 같은 방식으로는 링크 계층에서 proactive 방식과[10] 이동성 예측 기반의 핸드오버 인증 방식[11], 두 방식을 혼합한 방식[12]들이 있다. 그러나 표준 및 기존의 핸드오버 인증 기법들은 다수의 인증키 생성 및 인증 트래픽 발생, AP (Access Point) 토폴로지 상태 관리, 이동성 예측과 같은 오버헤드가 AAA 서버에 집중되어 있다.

이와 같이 IEEE 802.11 및 802.16 기반의 링크 계층과 FMIPv6의 네트워크 계층의 통합 핸드오버에 대한 연구가 활발히 진행되고 있지만, 핸드오버 인증 기술은 각 계층에서 독립적으로 연구되고 있다. 이는 AAA 서버에서 이동 노드의 AP 또는 BS 간 잦은 핸드오버 인증 수행으로 AAA 서버의 오버헤드를 유발하고, 네트워크 계층과의 중복된 인증 수행으로 이동 노드의 핸드오버 인증 시간이 지연될 수 있다. 또한 IEEE 802.11에서 802.16으로 핸드오버 할 때와 같이 이기종 액세스 기술 간의 핸드오버가 발생할 때, 이동 노드는 새로운 링크 액세스를 위하여 초기 인증과 같은 인증을 수행해야 하기 때문에 AAA 서버에서 오버헤드를 갖는다. 이러한 AAA 서버의 오버헤드는 이동 노드가 밀집되어 있는 환경이나 AAA 네트워크 및 서버의 용량이 제한되어 있는 환경에서 핸드오버 지연의 원인이 된다.

본 논문에서는 IEEE 802.11 또는 802.16과 같은 액세스 링크 기술 기반의 FMIPv6 환경에서 AAA 서버의 오버헤드를 최소화하고, 링크 계층과 네트워크 계층에서 핸드오버 인증을 통합하여 인증 지연 시간을 줄일 수 있는 이동 노드 주도형 핸드오버 인증 기법을 제안한다. 제안 기법은 FMIPv6 환경에서 핸드오버 인증키를 각 이동 노드가 직접 생성하는 기본 원리를 사용하여 AR 간에만 핸드오버 인증을 수행하고, AP 또는 BS와 같은 링크 계층에서는 계층적 키 구조를 적용하여 AAA 서버의 오버헤드를 최소화하는 핸드오버 인증 기

법이다. 제안하는 핸드오버 인증 기법은 기존의 링크 계층과 네트워크 계층에서 독립적으로 수행하는 핸드오버 인증 기법을 연동한 모델보다 핸드오버시 AAA에서 인증키 생성 및 트래픽 발생을 최소화하였고, 이동 노드의 핸드오버 인증 요청에 대한 MAC (Message Authentication Code) 검증과 핸드오버 인증키 복호화에 대한 역할만을 수행하도록 AAA 서버의 역할을 단순화하였다. 또한 제안 기법은 링크 계층의 액세스 인증, FMIPv6 시그널링 메시지 보호, 무선 채널에서 데이터 보호, PFS 및 PBS (Perfect Backward Secrecy)를 제공하고 DoS 공격에 안전하다.

본 논문의 구성은 다음과 같다. Ⅱ 장에서 기존의 핸드오버 인증 기술과 문제점을 살펴보고, Ⅲ 장에서는 본 논문에서 제안하는 핸드오버 인증 기술의 기본 원리와 프로토콜을 설명하고, 통합 핸드오버 인증 모델을 제안한다. Ⅳ장에서는 제안하는 핸드오버 인증 모델과 기존 기법들을 연동한 통합 모델과의 비교 분석 및 안전성을 서술하며, 마지막으로 Ⅴ장에서 결론을 맺는다.

Ⅱ. 기존 핸드오버 인증 관련 연구 및 문제점

IEEE 802.11 WLAN 환경에서 AAA 기반의 핸드오버 인증 지연 시간을 줄이기 위한 인증 기술들이 많이 연구되었다. Proactive 방식은 AAA 서버가 이동 노드의 핸드오버 마스터 키를 주변의 N개의 AP 들에게 미리 분배하는 기법으로써 이동 노드가 실제 핸드오버 하는 시점에서 핸드오버 마스터 키 교환 과정을 수행하지 않기 때문에 인증 지연 시간을 단축시킬 수 있다.[10] 모든 AP들의 토폴로지 상태를 유지하고 있는 AAA 인증 서버는 이동 노드가 핸드오버 하기 전에 주변의 모든 M개의 AP 들에게 NOTIFY-REQUEST 메시지를 전송하여 PMK (Pairwise Master Key) 사전 분배에 대해 요청한다. 이 요청을 수락하는 N 개의 AP들에 대해서 AAA 서버는 PMK_n를 생성하고 N 개의 AP들에게 각각 분배한다. 이동 노드가 AP_i로 핸드오버하면 이동 노드는 AAA 서버와 초기 부팅 인증 과정에서 공유한 MK를 사용하여 PMK_i를 생성하고 AP_i와 4-way 핸드쉐이크를 통하여 새로운 세션키를 생성한다. 그러나 proactive 인증 기법은 하나의 이동 노드에 대해서 AAA 서버가 N 개의 PMK를 생성하여 N 개의 AP들에게 각각의 PMK를 전송하기 때문에 AAA 네트워크에서 인증으로 인한 다량의 트래픽이 발생한다. 또한 AAA 서버는 AP들의 토폴로지 상태를 유지해야 하는 오버헤드가 있다.

이동성 예측 기반의 고속 핸드오버 인증 기법은[11] WLAN 환경에서 이동성 예측 기반의 인증 방식으로써 FHR (Frequent Handoff Region) 알고리즘을 사용하여 초기 부팅 인증 과정보다 인증 시간을 50% 단축시켰다. FHR 선택 알고리즘은 이동 노드의 이동 패턴을 분석하는 알고리즘으로 proactive 키 분배 방식과 달리 새로운 개념의 주변 AP들을 정의하였다. 새로 정의된 주변 AP 개념은 이동 노드가 자주 이동하는 AP들을 FHR 그룹으로 정의한다. 이동 노드가 FHR 내에서 핸드오버 할 때 FHR 그룹에 정의되어 있는 AP 들에게 미리 키를 분배하기 때문에 핸드오버 인증 지연 시간을 단축시킬 수 있다. 그러나 이동성 예측 기반의 핸드오버 인증은 이동 패턴을 분석하는 알고리즘 자체가 복잡하여 AAA 서버에게 큰 부담이 되고 이동 노드의 이동성을 예측하는 것이 제한적이기 때문에 실제 적용하는데 어려움이 있다.

Proactive 키 분배 방식과 이동 노드의 이동성 예측성 기반의 방식을 혼합한 기법은[12] WLAN 환경에서 AAA 네트워크의 트래픽 오버헤드를 neighbor graphs 기법을 사용한 proactive 방식과 비교하여 AAA 네트워크에서 발생하는 인증 메시지를 60% 감소시켰다. 이 혼합한 방식에서 제안한 기법 중 DSTPA (Dual State Transition Predictability Algorithm)는 이동 노드의 과거 이동성 기록을 기반으로 AP들에게 PMK를 분배하는 방식이다. 그러나 DSTPA는 과거의 이동성 기록이 없는 이동 노드에 대해서는 이동성을 기록하여 DSTPA를 적용하는데 시간이 필요하기 때문에 고속 핸드오버 인증 지원에 제한이 있다. 이러한 DSTPA 문제점을 해결하기 위해 혼합 방식에서는[12] SWA (Sliding Window Algorithm)도 제안하였다. SWA는 과거 이동성 기록이 존재하지 않는 새로운 이동 노드에 대해서는 neighbor graph 기법의 proactive 방식을 사용하고 이동 노드의 이동성 기록이 유지되어 DSTPA를 적용할 수 있는 시점이 되면 DSTPA로 전환하는 방식이다. DSTPA와 SWA는 기존 기법들보다 AAA 네트워크의 인증 트래픽 양을 줄이고 시간을 단축시켰지만 이동 노드의 이동성 예측을 기반으로 하고 있기 때문에 실제 적용하는데 제약이 따르고 AAA 서버에서 이동성 예측 알고리즘 및 AP들의 토폴로지 상태를 유지해야 하는 오버헤드가 존재한다.

FMIPv6 환경에서 네트워크 계층의 핸드오버 인증 기술은[6] MN (Mobile Node)과 PAR 간에 시그널링을 보호하기 위해 이동 노드와 AAA 서버 사이에 EAP 초기 인증을 통해 생성된 HMK (Handover Master Key)를 사용하여 이동 노드와 PAR 간에 HK (Handover Key)를 생성한다. PAR의 HK는 AAA 서버에서 HK를 생성하여 PAR에게 안전한 채널을 통해 전송한다. FMIPv6 핸드오버 인증 기술은 FBU와 같은 시그널링 메시지를 보호하지만 인증키 HK를 모든 이동 노드에 대해서 AAA 서버가 생성해야 하는 오버헤드가 있다.

기존에는 IEEE 802.11과 IEEE 802.16 환경의 핸드오버 인증 기법들과 MIPv6 또는 FMIPv6 환경에서 핸드오버 인증 기법들이[5][6] 각 계층별로 독립적으로 적용되고 연구되어 왔다. 이는 IEEE 802.11 또는 802.16과 같은 링크 계층에서 잦은 핸드오버 인증으로 AAA 서버의 오버헤드가 발생하고, 다양한 액세스 링크 기반의 FMIPv6 환경에서 AR 간 핸드오버가 발생할 경우 링크 계층과 네트워크 계층의 중복된 핸드오버 인증 수행으로 AAA 서버의 오버헤드가 발생한다. 이와 같이 기존의 기법들은 인증키 생성, 인증 트래픽, 주변 AP들의 토폴로지 상태 유지 및 이동 노드의 이동성 관리 등 핸드오버 인증 과정이 전적으로 AAA 서버에 집중되어 있기 때문에 이동 노드가 밀집되어 있는 환경이나 AAA 서버의 네트워크 환경 및 용량이 제한되어 있는 조건에서 핸드오버 인증 지연이 발생한다. 따라서 기존의 AAA 서버 중심의 각 계층별로 독립적으로 연구되었던 핸드오버 인증 기법들을 다양한 액세스 링크 기술 기반의 FMIPv6 환경에서 핸드오버 인증 지연 시간을 줄이기 위해 AAA 서버의 오버헤드를 최소화하는 통합 핸드오버 인증 기법이 필요하다.

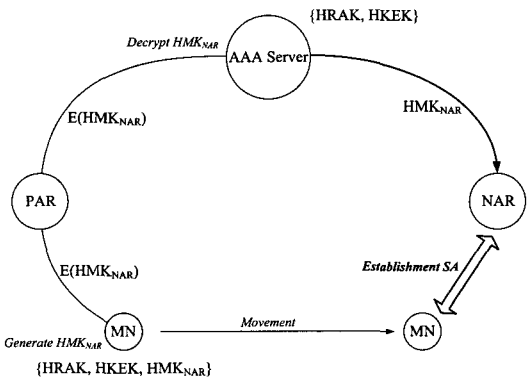
Ⅲ. 이동 노드 주도형 핸드오버 인증 프로토콜

3.1 기본 원리

본 논문에서 제안하는 핸드오버 인증 기법의 기본 원리는 이동 노드가 인증키를 직접 생성하여 AR 간에만 핸드오버 인증을 수행하고, 링크 계층에서는 계층적 키 구조를 적용하여 AAA 서버의 오버헤드를 줄이고, 잦은 핸드오버 인증 수행 횟수를 줄여 인증 지연 시간을 줄이는 것이다. 제안 프로토콜은 FMIPv6 환경에서 AR과 AAA 인증 서버 간에 TLS 또는 IPSec 보안 프로토콜을 사용하여 안전한 채널이 형성되어 있음을 가정한다. 그리고 이동 노드는 부팅 과정에서 EAP-TLS와 같은 초기 인증 수행을 통하여 AAA 서버와 공유된 EMSK를 단말에서 안전하게 저장하고 있음을 가정한다.[13][14] 다음은 이동 노드의 초기 인증 이후, 본 논문에서 제안하는 핸드오버 인증에서 사용되는 용어들을 정의한 것이다.

▲ 용어정의

- HMK_X (Handover Master Key) : 이동 노드와 Access Router (X) 간 핸드오버 인증 마스터 키
- HRAK (Handover Request Authentication Key) : 핸드오버 인증 요청을 검증하기 위한 키
- HKEK (Handover Key Encryption Key) : HMK를 암호화하기 위한 키
- SMK (Session Master Key) : 이동 노드와 AP (BS) 간에 IK, EK를 생성하기 위한 세션 마스터 키
- IK (Integrity Key) : 무선 구간에서 메시지 무결성을 위한 키
- EK (Encryption Key) : 무선 구간에서 메시지 기밀성을 위한 키
- AAuthReq : 핸드오버 인증 요청 메시지
- AAuthResp : 핸드오버 인증 응답 메시지
- H( ) : HMAC-SHA1 함수
- $E_K()$: 키 K를 사용한 암호화 함수
- MAC_{X_Y} : X와 Y 노드간의 MAC (Message Authentication Code)
- $Nonce_X$: 노드 X에서 생성한 임의의 랜덤 값
- ID_X : 노드 X의 식별자



〔그림 1〕 AR 간 핸드오버 인증 기법의 기본 원리

먼저 AR 간 핸드오버 인증의 기본 원리는 이동 노드가 핸드오버 인증키 HMK_{NAR}을 식 (3)과 같이 직접 생성하여 신뢰 구간이 형성되어 있는 AAA 서버를 통해 NAR로 전송하는 것이다. HMK_{NAR}의 안전성은 해쉬 함수의 안전성을 기반으로 한다. [그림 1]은 FMIPv6 환경에서 AR 간 핸드오버 인증 프로토콜의 기본 원리를 보여준다. 이동 노드가 초기 인증을 통하여 EMSK를 AAA 서버와 공유하면 이동 노드와 AAA 서버는 식 (1)과 같이 HRAK와 HKEK를 생성하여 단말에서 안전하게 저장한다. 여기서 AAA 서버는 모든 이동 노드들의 핸드오버 인증키 HMK_{NAR}을 생성하지 않고 이동 노드의 초기 부팅 인증시 형성된 HRAK와 HKEK를 기반으로 이동 노드의 핸드오버 인증 요청 메시지를 검증하고 핸드오버 인증키를 복호화하여 NAR에게 전송하는 역할만을 수행한다. 또한 AAA 네트워크에서 발생하는 메시지는 인증 요청 메시지와 응답 메시지 1 Phase로 이루어져 있어 트래픽 발생을 최소화 한다.

$$HRAK=H(EMSK\_0\_31,\text{"Authentication Key"}) \quad (1)$$

$$HKEK=K1||K2$$

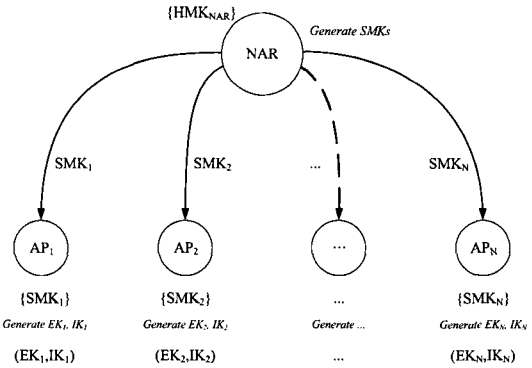
$$K1=H(EMSK\_32\_47,\text{"Encryption Key"}||0x01)$$

$$K2=H(EMSK\_48\_63,\text{"Encryption Key"}||0x02) \quad (2)$$

$$HMK=H(TimeStamp,ID_{MN}||ID_{NAR}||\text{"Handover Key"}) \quad (3)$$

{여기서, EMSK_X_Y는 EMSK의 X비트에서 Y비트를 나타냄}

링크 계층에서는 핸드오버 인증 수행 대신 [그림 2]와 같이 계층적 키 관리 구조를 갖는다. 계층적 구조는 각 AR에서 HMK를 기반으로 n 개의 SMK를 식 (4)와 같이 생성하고, AR에서 관리하는 n 개의 AP 또는 BS들에게 각 SMK를 분배하는 구조이다. SMK는 이동 노드들이 AP 및 BS로 핸드오버 할 때 AAA 서버와 핸드오버 인증 대신 이동 노드를 인증하는 키이다. 또한 SMK는 무선 구간에서 데이터를 보호하기 위한 EK와 IK를 식 (5)와 같이 생성하는데 사용된다. 링크 계층에서 계층적 키 구조는 AP 또는 BS와 같이 잦은 핸드오버 인증을 수행하는 환경에서 AAA 서버의 오버헤드를 줄일 수 있다. 이와 같이 제안 기법의 기본 원리들은 기존의 AAA 서버 오버헤드의 주요 요인이었던 AR 간 핸드오버시 링크 계층과 네트워크 계층의 중복된 핸드오버 인증 수행, 이동 노드의 인증키 생성, 인증 메시지 교환 개수, AP 토폴로지 상태, 이동성 관리와 같은 오



[그림 2] 계층적 키 관리 구조

버헤드를 최소화하고 AAA 서버의 동작을 단순화하여 핸드오버 인증 지연 시간을 줄인다. 또한 네트워크 계층의 핸드오버 인증 수행으로 이기종 액세스 기술 간 핸드오버시에도 안전한 고속 핸드오버를 지원할 수 있다.

$$SMK=H(HMK_{NAR}, ID_{AP}||ID_{MN}||\text{"Session Master"}) \quad (4)$$

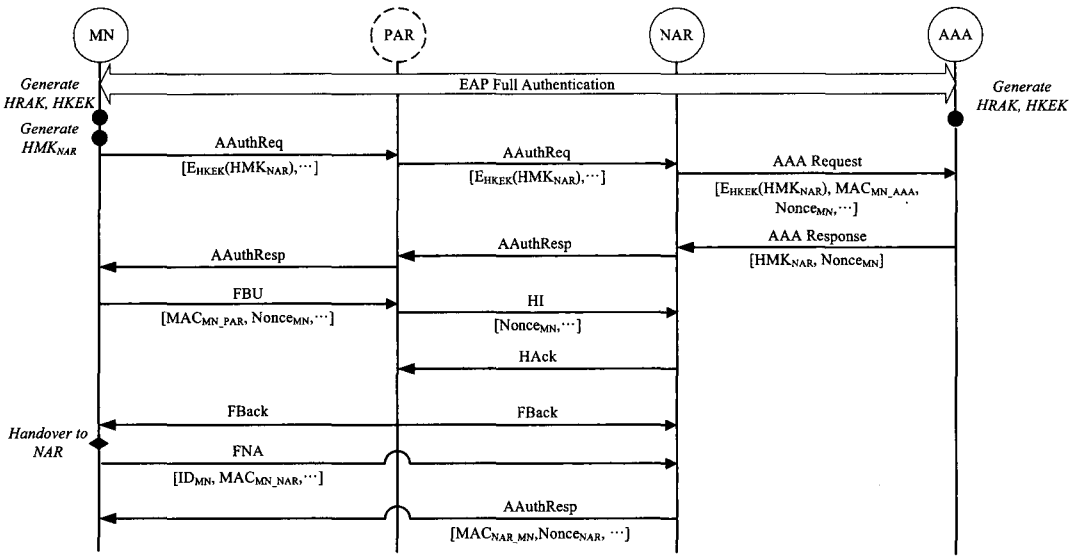
$$EK=H(SMK, ID_{MN}||ID_{AP}||Nonce_{MN}||Nonce_{AP}||\text{"Encryption Key"})$$

$$IK=H(SMK, ID_{MN}||ID_{AP}||Nonce_{MN}||Nonce_{AP}||\text{"Integrity Key"}) \quad (5)$$

3.2 FMIPv6 Predictive 모드에서 핸드오버 인증

FMIPv6에서는 이동 노드가 핸드오버 하는 시점에 따라 predictive와 reactive 핸드오버 모드를 정의하고 있다.[2] Predictive 핸드오버 인증은 FMIPv6에서 이동 노드가 PAR에서 RtSolPr (Router Solicitation for Proxy Advertisement)과 PrRtAdv (Proxy Router Advertisement) 메시지들을 사용하여 NAR에 대한 정보를 미리 파악한 후, NAR로 핸드오버 하기 전에 FBU 메시지를 사용하여 NAR에서 사용할 CoA (Care of Address)를 미리 설정하는 방법이다. Reactive 모드는 이동 노드가 FBU 메시지를 링크 계층에서 핸드오버하기 전에 NAR로 전송하지 못 했을 경우, NAR로 핸드오버 한 후에 FBU 메시지를 전송하는 모드이다.

본 절에서는 predictive 모드에서 핸드오버 인증 프로토콜을 설명한다. [그림 3]에서 이동 노드는 링크 계층에서 핸드오버가 이루어지기 전에 AAuthReq와 AAuthResp 메시지를 사용하여 핸드오버 인증을 수행한다. 먼저 이동 노드는 식 (6)과 같이 구성된 AAuthReq 메시지를 PAR에



〔그림 3〕 FMIPv6 Predictive 모드에서 핸드오버 인증

게 전송하여 핸드오버 인증 과정을 구동한다.

$$AAuthReq[ID_{MN},\ ID_{NAR},\ ID_{AAA},\ Nonce_{MN},\ E_{HKEK}(HMK_{NAR}), MAC_{MN\_PAR},\ MAC_{MN\_AAA}] \quad (6)$$

{여기서,

$MAC_{MN\_PAR}=H(HMK_{PAR}, Nonce_{MN}||ID_{MN}||ID_{NAR}||ID_{AAA}||E_{HKEK}(HMK_{NAR})||MAC_{MN\_AAA})$,

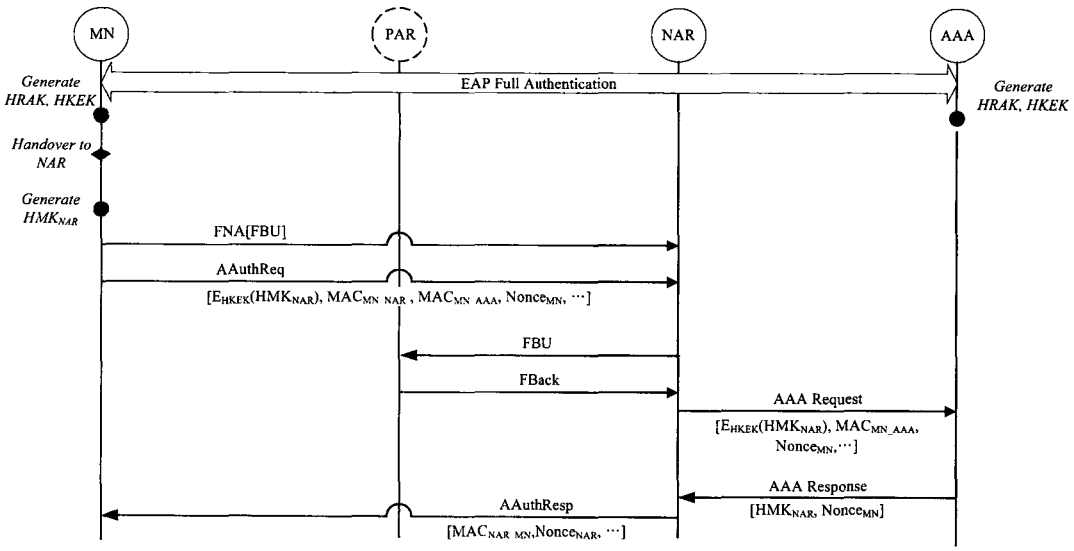
$MAC_{MN\_AAA}=H(HRAK,\ Nonce_{MN}||ID_{MN}||ID_{NAR}||ID_{AAA}||E_{HKEK}(HMK_{NAR}))$}

AAA 서버는 이동 노드에 대한 핸드오버 인증 요청에 대해서 AAuthReq 메시지에 있는 ID_{MN}를 확인하고 AAA 서버에서 관리하는 각 이동 노드들에 대한 인증 정보 테이블에서 HRAK와 HKEK를 사용하여 MAC_{MN_AAA} 값을 검증하고, HMK_{NAR}을 복호화한다. 복호화 된 HMK_{NAR}은 AAA 서버에 의해 ID_{NAR}을 갖는 NAR에게 안전하게 전송된다. 제안 프로토콜에서 AAA 서버는 단지 이동 노드의 핸드오버 요청에 대해 인증 요청에 대한 검증과 인증키만을 전달하는 것으로 핸드오버 인증 처리를 단순화하였다. 이는 AAA 서버의 오버헤드를 줄일 수 있다. HMK_{NAR}을 전달받은 NAR은 이동 노드가 FNA (Fast Neighbor Advertisement) 메시지를 NAR로 전송하여 핸드오버 했음을 알리면, 식 (7)과 같이 인증값 MAC_{MN_NAR}을 생성하고 교환하여 이동 노드와 상호 인증을 수행한다. 상호 인증이 확인되면 NAR은 이동 노드와 AP 또는 BS 간에서 데이터를 보호하기 위한 키 SMK를 생성하여 각 AP 또는 BS에게 전송한다. 만약 이동 노드가 링크 계층 핸드오버가 이루어지기 전에 핸드오버 인증 과정이 완료되지 못하면, 이동 노드는 reactive 핸드오버 인증을 수행한다.

$$MAC_{MN\_NAR}=H(HMK_{NAR},\ Nonce_{MN}||ID_{MN}||ID_{NAR})$$
$$MAC_{NAR\_MN}=H(HMK_{NAR},\ Nonce_{NAR}||ID_{MN}||ID_{NAR}) \quad (7)$$

3.3 FMIPv6 Reactive 모드에서 핸드오버 인증

〔그림 4〕는 FMIPv6에서 reactive 핸드오버 인증을 보여준다. Reactive 핸드오버 인증 모드에서 이동 노드는 핸드오버 인증 요청 메시지를 링크 계층과 네트워크 계층 핸드오버가 NAR로 이루어진 후에 전송한다. 먼저 이동 노드는 PAR과 이미 공유하고 있는 HMK_{PAR}을 사용하여 FBU 메시지에 대한 인증값을 생성하고 FNA 메시지와 함께 NAR에게 전송한 후, 핸드오버 인증 요청 AAuthReq 메시지를 식 (8)과 같은 형태로 NAR에게 전송한다. NAR이 FBU 메시지를 PAR에게 전송하고 FBU 과정이 완료되면 NAR은 PAR로부터 FBack (Fast Binding Acknowledgment) 메시지를 수신한다. 여기서 NAR은 악의적인 노드로부터 AAuthReq 메시



〔그림 4〕 FMIPv6 Reactive 모드에서 핸드오버 인증

지를 사용한 DoS 공격에 대응하기 위하여 PAR에서 FBU 과정이 성공적으로 이루어졌을 경우에만 AAA 서버에게 AAA Request 메시지를 전송한다.

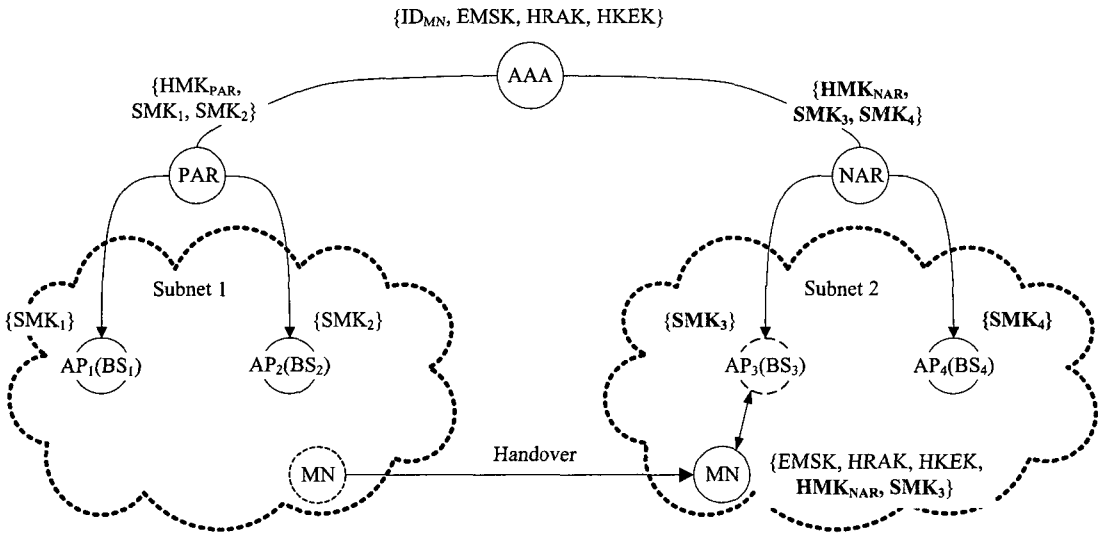
$$AAuthReq[ID_{MN},\ ID_{NAR},\ ID_{AAA},\ Nonce_{MN},\ E_{HKEK}(HMK_{NAR}),\ MAC_{MN\_NAR},\ MAC_{MN\_AAA}] \quad (8)$$

$\{$여기서, $MAC_{MN\_AAA}=H(HRAK,\ ID_{MN}||ID_{NAR}||ID_{AAA}||Nonce_{MN}||E_{HKEK}(HMK_{NAR}))||MAC_{MN\_NAR})\}$

3.4 이기종 액세스 기술 기반의 FMIPv6 환경에서 핸드오버 인증 기법

본 절에서는 앞서 제안한 핸드오버 인증 프로토콜을 IEEE 802.11과 802.16 네트워크 기반의 FMIPv6 환경에 적용한 통합 핸드오버 인증 모델을 제안한다. 제안하는 핸드오버 인증 모델에서 이동 노드의 네트워크 계층 핸드오버시에는 AAA 서버 기반의 이동 노드 주도형 핸드오버 인증을 수행하고, 링크 계층 핸드오버시에는 AR에서 각 AP 또는 BS들의 핸드오버 인증키를 계층적으로 관리하는 구조이다. 〔그림 5〕와 같은 환경에서 이동 노드의 핸드오버시 인증 절차를 살펴보면 다음과 같다. 먼저, 이동 노드는 AP_1 영역에서 초기 부팅을 하고, PAR을 통해 AAA 서버와 함께 초기 인증 과정을 수행한다. 여기서 PAR은 초기 부팅 과정에서 AAA 서버로부터 안전한 채널을 통한 HMK_{PAR} 키를 공유한다. 이동 노드가 AP_2로 핸드오버 할 때, AP_1-AP_2 간에 핸드오버 인증은 PAR의 HMK_{PAR}로부터 파생된 SMK_2를 사용하여 이동 노드의 링크 계층 핸드오버 인증 과정을 대신한다. 네트워크 계층과 링크 계층 간의 핸드오버가 동시에 이루어지는 AP_2-AP_3 간에서는 PAR-NAR 간 AAA 기반의 이동 노드 주도형 핸드오버 인증을 수행한 후, 링크 계층의 인증을 수행한다. 이동 노드는 FMIPv6 FBU 메시지를 PAR과 공유하고 있는 HMK_{PAR}을 사용하여 PAR에게 안전하게 전송하고, AAA 서버를 통해 HMK_{NAR}을 전달받은 NAR은 NAR 영역에서 이동 노드의 핸드오버 인증을 수행한다. 이동 노드와 NAR 사이에 HMK_{NAR}로 상호 인증이 확인되면 NAR은 HMK_{NAR}로부터 AP_3 (BS_3)와 AP_4 (BS_4)에게 각각 SMK를 식 (4)와 같이 생성하여 전송한다. 여기서 NAR과 AP (BS) 간에는 안전한 채널이 형성되어 있음을 가정한다. NAR 영역에서 이동 노드는 각 AP 및 BS와 SMK를 사용하여 링크 계층에서 AAA 서버의 핸드오버 인증 수행을 대신한다.

제안하는 이기종 FMIPv6 기반의 이동 망에서 이동 노드 주도형 핸드오버 인증 기법은 이동 노드가 AP (BS) 간 핸드오버 할 때마다 수행하는 잦은 링크 액세스 인증 수행 횟수를 AR 간 핸드오버 수행 횟수로 줄일 수 있기 때문에 인증키 생성 및 트래픽 발생과 같은 AAA



〔그림 5〕 이기종 액세스 링크 기술 기반의 FMIPv6 환경에서 핸드오버 인증 기법에 따른 키 계층적 구조

서버의 오버헤드를 최소화 할 수 있다. 예를 들어, 〔그림 5〕에서 (이동 노드가 AP_1에서 초기 부팅 인증을 수행한 상태) 기존의 링크 계층 인증과 네트워크 계층 인증 기술을 연동한 모델에서 이동 노드는 AP_1에서 AP_4까지 이동할 때 총 4회의 AAA 핸드오버 인증을 수행한다 (AP_1-AP_2, AP_2-AP_3, PAR-NAR, AP_3-AP_4). 그러나 제안한 핸드오버 인증 모델에서 이동 노드는 AR 간에만 총 1회의 AAA 인증만을 수행한다 (PAR-NAR).

Ⅳ. 기존 통합 핸드오버 인증 모델과 제안 기법 비교 분석

이번 장에서는 FMIPv6 환경에서 제안하는 핸드오버 인증 기법과 기존 AAA 서버 기반의 링크 계층과 네트워크 계층 인증이 연동되어 적용된 통합 모델을 비교 분석하고, 제안 기법의 안전성을 서술한다. 본 논문에서 제안하는 핸드오버 인증 기법의 비교 대상은 기존에 IEEE 802.11 및 802.16 기반의 FMIPv6 환경에서 통합 인증 모델이 없기 때문에 링크 계층의 proactive 방식[10], 이동성 예측 기반 방식[11], 혼합 방식의[12] 인증 기법과 네트워크 계층의 핸드오버 인증을[6] 연동한 통합 모델로 한다.

4.1 핸드오버 인증 기법 비교 분석

핸드오버 인증 방식은 AAA 기반의 인증 방식과 AAA 서버를 사용하지 않고 AR, AP, BS들 간 security context를 전달하는 방식으로 분류된다. 본 논문에서 제안하는 기법은 AAA 서버를 사용하는 방식이므로 본 비교 대상에서 security context 전달 방식은 제외한다. 〔표 1〕은 IEEE 802.11 또는 802.16 기반의 FMIPv6 환경에서 기존의 proactive 방식과 이동성 예측 기반 방식, 혼합 방식의 링크 계층 인증과 FMIPv6 핸드오버 인증을 연동한 모델과 본 논문에서 제안하는 핸드오버 인증 기법을 비교 분석한 표이다. 표 1은 각 통합 인증 모델을 이동 노드가 AP와 AR 간 핸드오버 할 때 AAA 인증 서버에서 발생하는 트래픽 양, 인증키 생성 및 인증 서버의 역할과 같은 오버헤드를 비교한 결과로서 제안 기법이 기존의 각 계층별로 연구된 인증 기술을 연동한 것보다 인증 서버의 오버헤드를 최소화하였음을 보여준다. 먼저 인증키 생성은 기존의 네트워크 계층과 링크 계층을 연동한 모델이 모두 AAA 서버에서 생성되는 반면 제안 기법은 각 이동 노드에서 자신의 핸드오버 인증키를 생성하여 제안 기법의 AAA 서버에서 인증키 생성에 대한 오버헤드가 발생하지 않는다.

통합 모델에서, AAA 서버가 링크 계층 인증 기술에서 생성하는 인증키 개수를 분석하면, 먼저 proactive 방식은 neighbor graph 개념을 사용하여 현재 이동 노드가 있는 AP를 기준으로 주변의 모든 AP들에게 이동

〔표 1〕 FMIPv6 통합 핸드오버 모델에서 AAA 인증 서버의 오버헤드 비교 분석

		기존 통합 핸드오버 인증 모델			제안 기법
네트워크 계층 인증		FMIPv6 핸드오버 인증[4]			제안 프로토콜
링크 계층 인증		Proactive 방식[10]	이동성 예측 (FHR)[11]	혼합 방식[12] (Proactive + 이동성 예측)	계층적 구조
인증키 생성 주체		AAA 서버	AAA 서버	AAA 서버	이동노드
AAA 서버에서 인증키 생성 개수 (X)	AP 간 핸드오버	N	1	1≦X≦N (단,L≦N)	0
	AR 간 핸드오버	N+1	2	2≦X≦N+1 (단,L≦N)	0
AAA 서버에서 인증키 분배를 위해 교환하는 메시지 개수 (Y)	AP 간 핸드오버	2M+N	L+1	L+1≦Y≦2M+N	0
	AR 간 핸드오버	2M+N+2	L+3	L+3≦Y≦2+2M+N	2
AAA 서버의 역할		Neighbor Graph 토폴로지 상태, 데이터 유지 관리, 인증요청 메시지 검증 및 인증키 전달	이동성 예측 알고리즘 동작 (FHR), 인증요청 메시지 검증 및 인증키 전달	Neighbor Graph 토폴로지 상태 및 데이터 유지 관리, 이동성 예측 알고리즘 동작 (DSTPA, SWA), 인증요청 메시지 검증 및 인증키 전달	인증요청 메시지 검증 및 인증키 전달

M:AP의 이웃하는 모든 AP들의 개수, N:ACCESS-ACCEPT 전송하는 AP 개수, L:이동성 예측 알고리즘에 의해 선택된 AP 개수, (0≦N≦M, 0≦L≦N)

노드의 핸드오버 인증키 PMK를 미리 분배할 것인지를 주변 AP들에게 확인한 후, 이를 수용하는 N개의 AP들에게 N개의 PMK를 분배한다. 이동성 예측 기반 방식은 AAA 서버에서 이동 노드가 현재 소속되어 있는 AP를 기준으로 이동 노드의 이동성 예측 알고리즘에 의해서 선택된 L개의 AP들에게 동일한 1개의 PMK를 분배한다. 혼합 방식은 proactive 방식을 사용할 때 N 개의 생성에서 이동성이 예측되면 L 개의 인증키로 줄일 수 있다. 네트워크 계층 인증 기술에서[6] 생성하는 인증키는 각 AR 당 1개의 인증키 HMK를 생성한다. 이동 노드가 AR 간 핸드오버 할 때는 AAA 서버에서 링크 계층 인증키와 네트워크 계층 인증키를 생성해야 한다. 그러나 제안하는 핸드오버 인증 기법은 인증키를 이동 노드에서 생성하기 때문에 AAA 서버에서 생성하는 인증키 개수가 없다. 따라서 제안 기법은 AAA 서버에서 인증키 생성에 따른 오버헤드를 최소화하였다.

제안 기법은 기존의 연동 모델보다 AAA 네트워크의 인증 메시지 발생 수도 최소화하였다. 링크 계층의 proactive 방식은 주변의 모든 M개의 AP들에게 NOTIFY-REQUEST 메시지를 전송하여 PMK 보안 협상을 요청한다. 보안 협상을 수락하는 N개의 AP들은 NOTIFY-ACCEPT 메시지를 AAA 서버에게 전송하고, 보안 협상을 거절하는 (M-N)개의 AP들은 NOTIFY-REJECT 메시지를 전송한다. NOTIFY 응답을 수신한 인증 서버는 보안 협상을 수락한 N개의 AP들에게 PMK를 포함한 ACCESS-ACCEPT 메시지들을 전송하므로 총 2M+N개의 메시지를 교환한다. 이동성 예측 기반 방식은 이동 노드가 핸드오버를 인증 서버에게 요청하는 1개의 access-request 메시지를 전송하면 AAA 인증 서버는 이동 노드가 이동할 L 개의 AP들을 예측하여 각 AP들에게 WEP (Wired Equivalent Privacy) 키를 포함한 L개의 access-accept 메시지들을 전송한다. 혼합 방식은 초기에 proactive 방식을 사용할 때 메시지 수 2M+N을 이동성 예측 기반의 메시지 수 1+L까지 줄일 수 있다. FMIPv6에서 핸드오버 인증 기술은[6] AR 간 핸드오버 할 때 2 개의 메시지를 교환한다. 이동 노드의 AR 간 핸드오버시에는 링크 계층 인증과 네트워크 계층 인증의 이중 수행으로 다량의 인증 트래픽이 발생한다. 그러나 제안 기법은 이동 노드가 AR 간 핸드오버 할 때 NAR과 AAA 서버 간에 AAA-Request와 AAA-Response 메시지만을 교환하고 AP 간 핸드오버에서는 계층적 키 관리 구조를 적용하였기 때문에

AAA 서버에서 메시지 발생이 없다.

제안 기법은 AAA 서버의 역할을 단순화하여 오버헤드 발생을 최소화하였다. 링크 계층의 proactive 방식은 인증 서버에서 neighbor graph 토폴로지 상태 및 데이터를 유지 관리해야 하는 오버헤드가 있다. 또한 이동성 예측 기반 방식도 인증 서버에서 복잡한 이동 노드의 이동성 예측 알고리즘을 동작시키고 이동성을 관리해야 하기 때문에 오버헤드가 발생한다. Proactive와 이동성 예측 기반 방식의 특성을 갖는 혼합 방식은 두 방식에서 갖는 오버헤드를 모두 갖는다. 기존의 FMIPv6 핸드오버 인증에서는 인증키를 생성하고 암호화하여 PAR에게 전송하는 역할로 비교적 단순하지만 기존의 링크 계층의 인증 기술과 연동되어 사용될 경우에 전체적으로 AAA 서버의 오버헤드는 증가한다. 그러나 제안 모델에서 인증 서버는 AR 간 이동 노드의 핸드오버 인증 요청에 대해서 인증하고 HMK_{NAR}을 암·복호화하여 NAR에게 전송하는 것으로 인증 서버의 역할을 최소화하고 단순화하였다.

마지막으로 제안하는 통합 핸드오버 인증 모델에서는 AR에서 링크 계층의 AP 또는 BS의 잦은 핸드오버 인증 절차를 줄이기 위하여 계층적 키 관리 구조를 제안하였다. 이는 이동 노드가 링크 계층에서 핸드오버 인증 수행을 위하여 AAA 서버와 통신하는데 따른 패킷 지연 시간을 AR에서 관리하는 핸드오버 인증키로 대신할 수 있기 때문에 핸드오버 인증 시간을 줄일 수 있다.

그러나 앞서 설명한 것과 같이 제안 모델이 AAA 서버의 오버헤드를 줄이는 장점은 있지만 인증키를 이동 노드에서 생성하고 AP 또는 BS에서 계층적 키 관리를 수행해야하기 때문에 기존의 연동 모델보다 이동 노드와 AP 또는 BS에서 오버헤드가 발생한다. 그러나 제안 모델에서 이동 노드에게 요구하는 오버헤드는 해쉬 연산들이기 때문에 큰 부담이 되지 않는다. 기존의 핸드오버 인증 방식에서도 이동 단말에서 해쉬 연산을 수행하고 있다. AR에서 링크 계층의 핸드오버 인증을 위한 키 계층적 구조는 기존의 방식에 비해 AR에서 오버헤드가 발생하지만 핸드오버 인증 지연 시간을 줄여 seamless 서비스를 제공 할 수 있는 장점이 있다.

4.2 안전성 분석

핸드오버 인증 기술은 멀티미디어 데이터와 같이 패킷 지연 시간에 민감한 데이터 전송을 고려하여 인증 시간을 최소화하는 것뿐만 아니라, 핸드오버 과정에서 안전하게 인증키를 분배하고 정당한 이동 노드만이 네트워크 액세스 서비스를 이용할 수 있어야 한다. 제안 기법은 기존의 AAA 기반의 인증 방식과[6][10][11][12] 마찬가지로 AAA 서버와 AR 간, AR과 AP (BS) 간 안전한 채널을 가정하였기 때문에 각 구간별 HMK_{NAR} 또는 SMK 전달하는데 있어서 안전하다. 또한 제안하는 핸드오버 인증 기법은 네트워크 액세스, FMIPv6 시그널링 보호, 무선 구간에서 채널 보호를 제공한다. 핸드오버 인증 기술은 이동 노드가 NAR로 핸드오버 할 때 NAR은 이동 노드에 대해서 네트워크 액세스 인증을 수행해야 한다. 악의적인 이동 노드가 정상적인 이동 노드의 단말 정보 등을 사용하여 NAR을 통해 불법적으로 네트워크에 접속할 수 있기 때문에 이동 노드가 핸드오버 할 때 NAR은 이동 노드에 대해 액세스 인증을 수행하고 인증된 이동 노드에 대해서만 네트워크 접근을 허가해야 한다. 제안 기법은 이동 노드가 NAR로 핸드오버 할 때 HMK_{NAR}을 두 노드가 안전하게 공유하기 때문에 NAR은 HMK_{NAR}을 사용하여 이동 노드의 네트워크 접속에 대해 인증을 수행할 수 있다. 이동 노드가 NAR로 핸드오버 할 때 생성된 HMK_{NAR}은 AP 또는 BS에서 사용한 세션키 SMK를 생성하기 때문에 SMK를 기반으로 이동 노드의 네트워크 액세스를 제어하고 무선 구간에서 데이터를 보호하는데 사용 할 수 있다. HMK_{PAR}은 이동 노드가 NAR로 핸드오버 할 때 FBU 메시지를 보호하는데 사용한다.

제안 기법은 HMK 간 PFS 및 PBS를 제공한다. AAA 기반의 핸드오버 인증 기술은 security context 전달 방식에 비해서 각 AP에게 독립적인 핸드오버 인증키를 분배한다. 즉, AAA 기반의 인증 방식은 PFS와 PBS를 제공하지만, security context 전달 방식은 AAA 서버를 사용하지 않고 현재 AP에서 다음 AP에게 인증키를 암호화하여 전달하거나 해쉬하여 전달하기 때문에 PFS 및 PBS 보안 서비스가 제공되지 않는다. Security context 방식에서 이동할 AP가 이동 노드와 랜덤값 nonce를 주고받아 새로운 인증키를 생성한다 하더라도 nonce 값은 공개 채널로 주고받기 때문에 이전 AP가 nonce를 스니핑 한다면 새로운 인증키를 생성해 낼 수 있다. 제안 기법은 핸드오버시 각 이동 노드가 새로운 인증키 HMK를 생성하기 때문에 AR들 간 독립적인 HMK를 유지할 수 있다. 생성된 HMK_{NAR}의 안전성은 해쉬 함수의 안전성을 기반으로 한다. 이동 노드가 PAR에서 NAR로 핸드

오버 할 때 임의로 생성된 HMK_{NAR}을 AAA 서버와 공유하고 있는 HKEK를 사용하여 NAR에게만 전달하기 때문에 PAR에서는 HMK_{NAR}을 알 수 없다. 마찬가지로 NAR에서는 PAR과 이동 노드 사이에서 사용되었던 HMK_{PAR}을 알 수 없다.

제안 기법은 핸드오버 인증 과정에서 DoS 공격에 안전하다. 이동 노드가 NAR로 핸드오버 할 때 PAR에게 AAuthReq 메시지를 전송한다. Predictive 모드에서 AAuthReq 메시지는 이동 노드와 PAR 간에 공유하고 있는 HMK_{PAR}을 사용하여 AAuthReq 메시지를 해쉬하기 때문에 PAR에서는 정당한 이동 노드가 아닌 임의의 AAuthReq 메시지에 대해서 인증 요청을 거절할 수 있다. AAA 서버에 대한 DoS 공격은 이동 노드가 AAA 서버와 공유하고 있는 HRAK를 사용하여 핸드오버 요청을 하기 때문에 AAA 서버는 악의적인 AAA Request 메시지에 대해서 인증 요청을 수행하지 않는다.

V. 결 론

기존의 핸드오버 인증 기법은 IEEE 802.11 또는 802.16에서 링크 계층 인증과 FMIPv6 환경에서 네트워크 계층 인증이 독립적으로 연구되고 있어 두 계층의 인증 기술을 연동한 통합 모델에서는 이동 노드가 핸드오버 할 때 중복된 핸드오버 인증 절차로 AAA 서버에서 이동 노드의 인증키 생성, 인증 메시지 교환 개수, AP 토폴로지 상태 및 이동성 관리와 같은 오버헤드가 존재하고 핸드오버 인증 지연이 발생한다. 본 논문에서는 이기종 액세스 링크 기술 기반의 FMIPv6 환경에서 이동 노드 주도형 핸드오버 인증 기법을 제안하였다. 제안 기법은 FMIPv6 환경에서 이동 노드가 직접 핸드오버 인증키를 생성하여 인증 서버를 통해 안전하게 NAR로 전송하고, NAR에서 AP들과 계층적 키 관리 구조를 갖는다. 이동 노드에서 생성한 인증키는 FMIPv6에서 AR 간 핸드오버 할 때 FBU 메시지를 보호할 수 있고, NAR에서 계층적 키 관리를 통해 이동 노드의 링크 액세스 인증을 수행할 수 있다. 제안 기법은 이동 노드에서 핸드오버 인증키를 생성하고, 핸드오버 인증에 따른 메시지 교환 횟수와 네트워크 계층과 링크 계층 간의 중복된 핸드오버 인증 횟수를 줄여 AAA 서버의 오버헤드를 최소화하였다. 또한 링크 계층에서 자주 일어나는 핸드오버 인증 수행 대신 AR의 계층적 키 관리 구조를 통해 이동 노드의 핸드오버 인증 지연 시간을 줄일 수 있도록 하였다. 그러나 제안 기법은 기존의 방식에 비해 핸드오버 인증 지연 시간을 줄일 수 있지만 AR에서 계층적 키 관리를 수행해야하기 때문에 AR에서 오버헤드가 발생한다. 마지막으로 본 논문에서는 제안 기법의 PFS와 PBS를 제공 및 DoS 공격에 대한 안전성을 분석하였다.

참고문헌

[1] Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6," IETF RFC 3775, June 2004.

[2] C Koodli, R., "Fast Handovers for Mobile IPv6," IETF RFC 4068, July 2005.

[3] P. McCann, "Mobile IPv6 Fast Handovers for 802.11 Networks," IETF RFC 4260, November 2005.

[4] Heejin Jang, Junghoon Jee, Youn-Hee Han, Soohong Daniel Park, and Jaesun Cha, "Mobile IPv6 Fast Handovers over IEEE 802.16e Networks," IETF Internet Draft draft-ietf-mipshop-fh80216e-00, April 2006.

[5] Patel, A., "Authentication Protocol for Mobile IPv6," IETF RFC 4285, January 2006.

[6] Narayanan, V., "Handover Keys Using AAA," IETF Internet Draft draft-vidya-mipshop-handover-keys-aaa-03, October 2006.

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

[8] IEEE standard, "Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands," IEEE 802.16e, 2005.

[9] M. Yasuhiko, Ana Sanz M., S. Manish, S. Takashi, and Randy H. Katz, "Secure authentication system for publie WLAN roaming," *ACM/WMASH*, 2003.

[10] Arunesh Mishra, Min Ho Shin, Nick L. Petroni, Jr., T. Charles Clancy, and William A. Arbaugh, "Proactive Key Distribution Using Neighbor Graphs," *IEEE Wireless Communications*, February 2004.

[11] S. Pack and Y. Choi, "Fast handoff scheme based on mobility prediction in public wireless LAN systems," *IEE Proceedings Communications*, October 2004.

[12] Anindo Mukherjee, Tarun Joshi, and Dharma P. Agrawal, "Minimizing Reauthentication overheads in infrastructure IEEE 802.11 WLAN networks," IEEE WCNC2005, 2005.

[13] Aboba, B., "Extensible Authentication Protocol (EAP)," IETF RFC 3748, June 2004.

[14] Aboba, B., "Extensible Authentication Protocol (EAP) Key Management Framework," IETF draft-ietf-eap-keying-15, October 2006.

〈著者紹介〉

최 재 덕 (Jaeduck Choi) 학생회원
2002년 2월: 숭실대학교 정보통신전자공학부 졸업
2004년 2월: 숭실대학교 정보통신공학과 석사
2005년 3월~현재: 숭실대학교 전자공학과 박사과정
<관심분야> 이동 네트워크 보안, VoIP 보안, 네트워크 보안

정 수 환 (Souhwan Jung) 종신회원
1985년 2월: 서울대학교 전자공학과 학사
1987년 2월: 서울대학교 전자공학과 석사
1988년~1991년: 한국통신 전임 연구원
1996년 6월: University of Washington 박사
1996년~1997년: Stellar One SW Engineer
1997년~현재: 숭실대학교 정보통신전자공학부 부교수
<관심분야> 이동 네트워크 보안, VoIP 보안, 네트워크 보안, RFID/USN 보안