IEEE 802.16e 네트워크에서 익명성을 제공하는 사업자간 로밍 인증 및 키 설정 프로토콜

정회원 박 영 만*, 박 상 규**°

An Inter-provider Roaming Authentication and Key Establishment Protocol Providing Anonymity in IEEE 802.16e Networks

Young Man Park*, Sang Kyu Park** *Regular Members*

요 약

본 논문에서는 IEEE 802.16e 네트워크에서 통신 사업자간 로밍을 위한 새로운 인증 및 키 설정(AKE: Authentication and Key Establishment) 프로토콜을 제안한다. 제안된 프로토콜은 두 개의 다른 인증 credentials를 사용하여 사용자(user) 및 단말(device) 인증을 함께 수행하며 사용자 익명성과 키 설정을 제공한다. 또한, 제안된 프로토콜에서 홈 네트워크(Home Network: HN)와 외부 네트워크(Foreign Network: FN) 사이의 메시지 교환 횟수는 단지 2 라운드(round) 수가 필요하다.

Key Words : IEEE 802.16e, Roaming, Authentication, Anonymity

ABSTRACT

In this paper, we present a novel authentication and key exchange(AKE) protocol for inter-NSP(provider) roaming in IEEE 802.16e networks. The proposed protocol allows performing both user and device authentication jointly by using two different authentication credentials and provides user anonymity and session key establishment. Also, this protocol requires only two round number message exchange between foreign network and home network.

Ⅰ. 서 론

모바일 사용자들에게 광대역 무선접속 서비스를 제공하는, mobile WiMAX(Worldwide Interoperability for Microwave Access)라고도 알려져 있는, IEEE 802.16e 규격이 2006년 2월 확정 발표되었다[1]. 이 규격은 주파수 재사용, 핸드오버 및 보안 기능 등을 PHY 계층(Physical layer)과 MAC 계층(Media Access Control layer)에서 정의하고 있다. 그리고 현재, WiMAX 포럼의 네트워크 워킹그룹(NWG: Network Working Group)에서는 IEEE 802.16e규격 및 IETF 규격을 기본으로 해서 단대단(end-to-end) 네트워크 시스템 아키텍처를 정의하는 과정에 있다[2,3].

IEEE 802.16e 네트워크 서비스사업자(NSP: Network Service Provider)들은 그들의 가입자들에게 홈 네트워크 커버리지를 확대하여 궁극적으로 글로벌 액세스 서비스를 제공하는 글로벌 로밍을 제공하고자 한다. 이것을 이루기 위해서는 홈 네트워크의 가입자가 다른 사업자 영역(domain)의 외부 네트워크에 접속할 수 있는 사업자간(inter-provider) 로밍이 기본적으로 필요하며 이것에는 인증, 과금, 클리어링 하우스(clearing house), 로밍 협정(roaming agree-

* KT 인프라연구소 (youngman@kt.co.kr), ** 한양대학교 전자통신컴퓨터공학부 (skpark@hanyang.ac.kr) (° : 교신저자)
논문번호 : KICS2006-10-419, 접수일자 : 2006년 10월 11일, 최종논문접수일자 : 2006년 10월 20일

ment) 등 여러 가지 이슈들이 있다. 특히, 사업자간 로밍에서는 한정된 컴퓨팅 리소스를 가진 모바일 단말에 구현될 수 있는 인증과 익명성을 제공하는 사용자 프라이버시(privacy)를 고려하여야 한다.

IEEE 802.16e 규격은 사용자(user)와 단말(device) 인증을 위하여 EAP(Extensible Authentication Protocol)[4]를 지원하는 PKMv2(Privacy Key Management version 2)를 규정하고 있는데 사용자와 단말 인증이 모두 수행되어야 할 필요가 있는 경우에는 Double EAP 모드(Authenticated EAP-after-EAP) 또는 single EAP 모드를 사용하도록 정의하고 있다[1]. 일반적으로 Double EAP 모드는 single EAP 모드보다 MS(Mobile Station)와 인증 서버 간의 메시지 교환 횟수가 많아지게 되어 인증 설정 지연 시간이 길어지고 통신 대역폭을 많이 사용하게 되는 단점을 가지고 있다. 이러한 단점은 글로벌 로밍 환경에서는 더 심각한 단점이 될 수 있다. 또한, single EAP를 사용하여 사용자와 단말을 함께 인증하는 EAP method나 발표된 솔루션은 현재까지 거의 없는 것으로 알려져 있다.

따라서, 본 논문에서는 앞서 언급한 문제점들을 해결하기 위하여 한 번의 인증 scheme(single EAP)으로 사용자와 단말을 함께 인증할 수 있는 새로운 로밍 인증 및 키 설정 프로토콜을 제안한다. 이 프로토콜은 두 개의 다른 credentials, 즉, 패스워드와 단말(또는, 스마트카드)에 저장된 대칭키(symmetric key)를 사용하여 사용자와 단말을 함께 인증한다. 또한, 매 인증마다 동적으로 변경되는 AID(Anonymity Identity)를 사용하여 모바일 사용자의 익명성을 제공하고, 인증 지연시간(delay time)을 최소화하기 위하여 외부 네트워크(Foreign Network: FN)와 홈 네트워크(Home Network: HN) 간의 메시지 교환 횟수는 단 한번의 round trip이 필요하도록 설계하였다.

본 논문의 구성은 2장에서 IEEE 802.16e 네트워크의 로밍 구조를 알아보고, 3장에서는 제안된 로밍 인증 프로토콜의 동작을 등록단계와 로밍인증 단계로 나누어 설명한다. 4장에서는 프로토콜의 안전성을 분석하고 마지막으로 5장에서 최종적인 결론을 맺는다.

Ⅱ. IEEE 802.16e 네트워크 로밍 구조

이 장에서는 IEEE 802.16e 네트워크에서 사업자간 로밍을 제공하기 위한 시스템 모델과 인증 모드에 대하여 알아본다.

2.1 시스템 모델

WiMAX 포럼에서는 IEEE 802.16e 시스템 구조를 2개의 구성 요소 즉, ASN(Access Service Network)과 CSN(Connectivity Service Network)으로 정의하고 있다[4]. ASN은 BS(Base Station)와 ASN-GW(ASN gateway)으로 이루어져 있으며 사용자에게 무선접속을 제공하는 여러 가지 기능들을 가지고 있다. CSN은 인증서버와 HA(Home Agent) 등으로 이루어져 있으며 사용자에게 IP connectivity를 제공하는 일련의 네트워크 기능들을 가지고 있다. 그림 1은 IEEE 802.16e 네트워크에서 MS가 Home NSP에서 Foreign NSP로 이동시 특정 BS의 무선링크를 경유하여 외부 네트워크에 연결되는 로밍을 나타낸 것이다. 이러한 로밍 서비스를 제공하기 위해서는 사전에 MS가 Home NSP에 서비스 가입이 되어 있어야 하고 Home NSP와 Foreign NSP 간의 로밍 협정(roaming agreement)이 설정되어 있어야 한다.

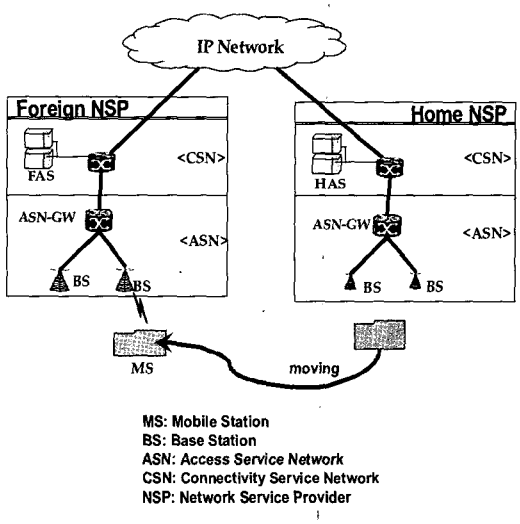

그림 1. 로밍 시스템 모델

2.2 인증 모드

IEEE 802.16e 네트워크 접속 인증은 사용자 및 (또는) 단말 인증을 요구하고 있다. 단말 인증은 사용하는 단말이 IEEE 802.16e 규격을 준수하는 단말인지, 그리고 그 단말이 분실된 단말인지를 결정하는데 사용된다. 사용자 인증은 가입자에게 제공된 서비스들을 정확하게 요금 청구하기 위하여 가입자를 인증하는데 사용된다. 네트워크 접속 인증은 적절한 EAP method를 사용하여 제공할 수 있으며 여기에는 여러 가지 인증 모드가 있다[2]. MS는 다

음의 인증 모드들 중에서 하나를 선택한다.

- Single EAP/User-only Authentication : single EAP 사용하여 단말은 인증하지 않고 사용자만 인증함.
- Single EAP/Device-only Authentication : single EAP 사용하여 사용자는 인증하지 않고 단말만 인증함.
- Double EAP/Device and User Authentication : Double EAP 사용하여 단말과 사용자를 모두 인증함.
- Single EAP/Device and User Authentication : Single EAP 사용하여 단말과 사용자를 모두 인증함.

Ⅲ. 제안된 로밍 인증 프로토콜

제안된 프로토콜은 모바일 사용자 MS(mobile station)와 홈 네트워크의 인증 서버 HAS(home authentication server), 그리고 외부 네트워크의 인증 서버 FAS(foreign authentication server)가 관련되는 3자 개체(entity) 기반의 로밍 인증 및 키 설정 프로토콜이다. 제안된 프로토콜의 상세한 동작은 등록(registration) 및 로밍인증(roaming authentication) 단계로 구분하여 설명한다. 다음은 프로토콜이 어떻게 수행되는지를 나타낸다.

3.1 기호 정의

- $ID_M/ID_F/ID_H$: Mobile Station/Foreign Network/Home Network의 식별자(identifier)
- PW : 패스워드
- K_{MH}/K_{FH} : 대칭키 암호 알고리즘에 사용되는 MS와 HAS간/FAS와 HAS간 대칭키들
- AID : anonymous identity
- FAS/HAS : 외부 네트워크 인증서버/홈 네트워크 인증서버
- $N_M/N_F/N_H$: MS/FAS/HAS가 생성한 랜덤 넘버(nonce)
- $E_K(\ )/D_K(\ )$: 키 K를 사용하여 대칭키 암호화/복 호화
- H( ) : 일방향 해쉬함수
- ⊕ : eXclusive OR 연산
- PSK : pre secret key
- MSK : master secret key

3.2 등록 단계

사용자(MS)와 홈 네트워크 서비스사업자(H-NSP)는 통신서비스 가입을 통하여 서로 신뢰 관계(trust relationship)를 설정하고 암호학적으로 안전한(엔트로피가 높은) 대칭키 K_{MH}, 사용자 식별자(ID_M)/패스워드(PW), AID=h(ID_M, PW, K_{MH}), 그리고 홈 네트워크 HN의 식별자 ID_H를 서로 공유 한다. 사용자는 K_{MH}, AID, ID_H를 모바일 단말 또는 스마트 카드에 저장 할 수 있다.

HN과 FN은 서로 다른 NSP에 의해서 관리되고 로밍 협정을 통해서 보안연계(Security Association)를 설정하고 있으며 서로의 식별자 ID_F/ID_H, 그리고 대칭키 K_{FH}를 알고 있다고 가정 한다. 반면에 MS와 FN은 사전에 어떠한 관계도 설정되어 있지 않다고 가정한다.

3.3 로밍 인증 단계

다음의 메시지 흐름 절차는 프로토콜이 성공적으로 수행되었을 경우에 어떻게 상호 개체 인증과 키 설정이 이루어지는지를 설명한다.(그림 2 참조)

(M1) MS → BS → FAS : AID

홈 네트워크에 등록된 사용자(MS)가 외부 네트워크로 이동하여 네트워크 접속 서비스를 요청하고자 하는 경우, 사용자는 자신의 AID를 NAI(Network access Identifier)형식[5]을 이용하여(ex : AID@homerealm.com) FAS로 보낸다. 이것은 FN의 기지국(BS : base station)을 경유하여 FAS로 보내어 진다.

(M2) FAS → BS → MS : IDF, NF

메시지 (M1)을 받은 FAS는 MS가 자신의 시스템에 등록된 가입자가 아니라는 것을 알게 되며, 자신의 랜덤 넘버 N_F를 생성하여 MS에게 ID_F와 N_F를 함께 보낸다.

(M3) MS → BS → FAS : E1, $Auth_{MH}$

MS는 메시지 (M2)를 수신한 후, $E1=E_{K_{MH}}(N_M, N_F)$과 $AUTH_{MH}$=H(PW, N_M, ID_M, ID_F)을 계산하는데 E1은 대칭키 K_{MH}를 이용하여 N_M 과 N_F를 암호화한 값이고 $AUTH_{MH}$는 PW, N_M, ID_M, ID_F를 일방향 해쉬 함수한 값이다. 그 후, MS는 FAS에게 E1, $AUTH_{MH}$를 보낸다.

(M4) FAS → HAS : AID, E1, $Auth_{MH}$, $Auth_{FH}$

메시지 (M3)를 수신한 FAS는 $Auth_{FH}=H(K_{FH}, N_F, Auth_{MH})$를 계산하여 AID, E1, $Auth_{MH}$, $Auth_{FH}$가 포함된 메시지 (M4)를 HAS에게 보낸다.

(M5) HAS → FAS : E2, $Auth_{HF}$

FAS로부터 메시지 (M4)를 수신한 HAS는 요청된 AID와 일치하는 AID가 자신의 인증 데이터베이스 (DB)에 있는지를 확인한다. 만약, 일치하는 AID가 없다면, HAS는 FAS에게 fail 메시지를 보낸다. 그러나 일치하는 AID가 있는 경우에는, 데이터베이스에서 MS의 ID_M, PW, K_{MH} 등을 가져와 E1을 복호화하여 N_M과 N_F를 구하고($D_{K_{MH}}(E1)=(N_M, N_F)$), 랜덤넘버 N_H를 생성한다. HAS는 수신된 $Auth_{MH}$와 자신이 계산한 $H(PW, N_M, ID_M, ID_F)$가 같은지를, 그리고 수신한 $Auth_{FH}$와 자신이 계산한 $H(K_{FH}, N_F, Auth_{MH})$가 같은지를 검증한다($Auth_{MH} \stackrel{?}{=} H(PW, N_M, ID_M, ID_F)$, $Auth_{FH} \stackrel{?}{=} H(K_{FH}, N_F, Auth_{MH})$). 이 검증이 모두 성공할 경우에는 $PSK=H(N_M, N_F, PW, K_{MH})$와 $E2=E_{K_{FH}}(N_M, N_H, PSK)$, 그리고 $Auth_{HF}=H(PSK, ID_H, ID_F)$를 계산하여 FAS에게 E2, $Auth_{HF}$가 포함된 메시지 (M5)를 보낸다. 또한, HAS는 사용된 AID를 새로운 $AIDnew=h(ID_M, AID, PSK)$로 갱신(update)하여 인증 데이터베이스 (DB)에 저장한다.

(M6) FAS → BS → MS : E3, $Auth_{FM}$

메시지 (M5)를 수신한 FAS는 HAS가 MS와 FAS를 성공적으로 인증하였다는 것을 알게 된다. FAS는 E2을 복호화하여 N_M, N_H, PSK를 구하고 ($D_{K_{FH}}(E2)=(N_M, N_H, PSK)$), 랜덤 넘버 R_F를 생성한다. FAS는 수신된 $Auth_{HF}$와 자신이 계산한 $H(PSK, ID_H, ID_F)$가 같은지를 검증한다($Auth_{HF} \stackrel{?}{=} H(PSK, ID_H, ID_F)$). 이 검증이 성공할 경우에는 $E3=E_{PSK}(R_F \oplus N_H)$와 $MSK=H(R_F \oplus N_H, N_M)$, 그리고 $Auth_{FM}=H(MSK, Auth_{HF})$를 계산하여 MS에게 E3, $Auth_{FM}$이

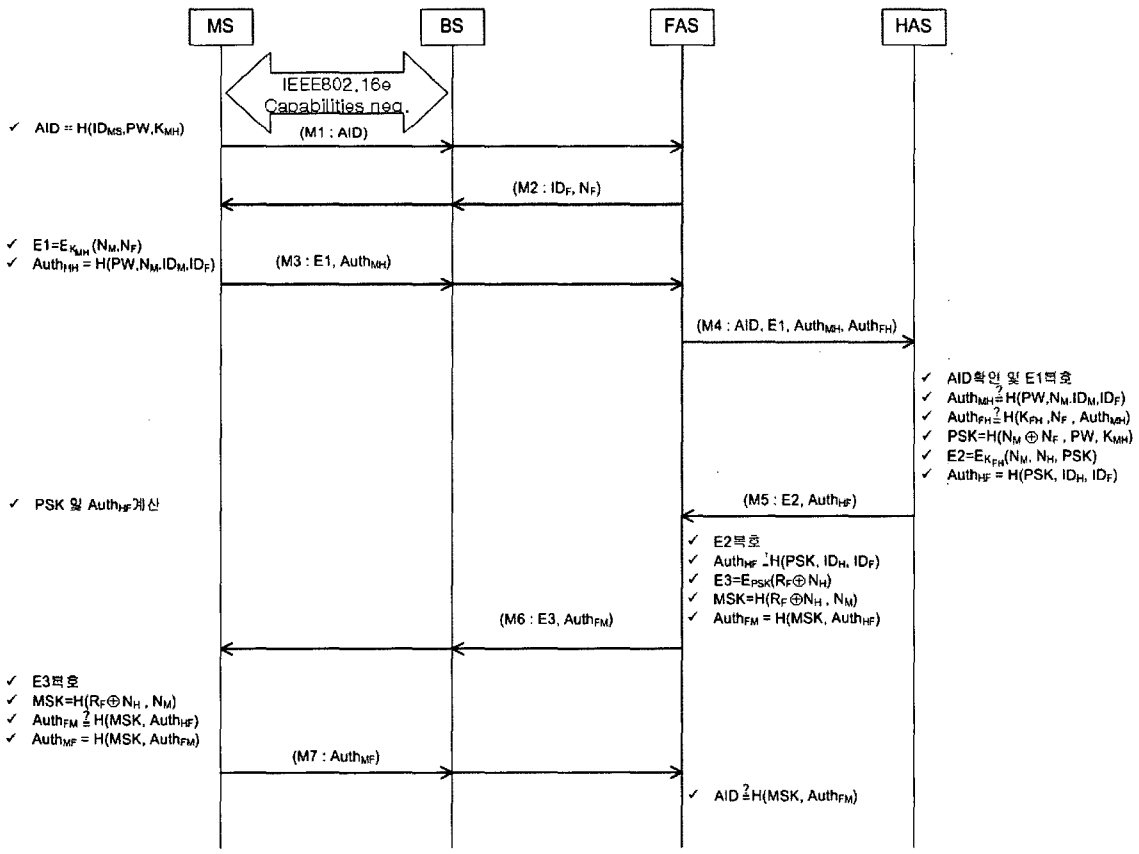

그림 2. 제안된 로밍 인증 및 키 설정 프로토콜

포함된 메시지 (M6)을 보낸다.

(M7) MS → BS → FAS : $Auth_{MF}$

MS는 메시지 (M3)을 FAS에게 보낸 후부터 메시지 (M6)을 수신하기 전까지 대기하는 시간 동안에 PSK와 $Auth_{HF}$를 미리 계산해 놓을 수 있다. 이것은 인증 설정 시간을 단축 시켜준다. 메시지 (M6)를 수신한 MS는 PSK로 E3을 복호화하여 ($R_F \oplus N_H$)를 구한다(D_{PSK}(E3)=($R_F \oplus N_H$)). MS는 수신된 $Auth_{FM}$과 자신이 계산한 H(MSK, $Auth_{HF}$)가 같은지를 검증한다($Auth_{FM} \stackrel{?}{=} H(MSK, Auth_{HF})$). 이 검증이 성공할 경우, MS는 $Auth_{MF}$=H(MSK, $Auth_{FM}$)을 계산하여 FAS에게 보낸다. MS는 사용된 AID를 새로운 AIDnew=h(ID_M, AID, PSK)로 갱신, 저장하여 다음 번 인증 프로토콜 수행 시에 사용한다.

메시지 (M7)를 수신한 FAS는 수신된 $Auth_{MF}$와 자신이 계산한 H(MSK, $Auth_{FM}$)이 같은지를 검증한다($Auth_{MF} \stackrel{?}{=} H(MSK, Auth_{FM})$). 만약, 이 검증이 성공하면, 로밍 인증 및 키 설정 프로토콜이 성공적으로 완료된 것이다.

Ⅳ. 안전성 분석

제안된 프로토콜 수행은 다음과 같은 여러 가지 특성들을 제공한다.

4.1 인증(Authentication)

- HAS에 의한 사용자/단말 양자 인증(Both user and device authentication by the HAS) : 제안된 프로토콜은 IEEE 802.16e에서 요구하는 사용자와 단말 인증을 모두 제공하는데, 사용자 인증에는 사용자가 기억하는 패스워드(PW)가, 그리고, 단말 인증에는 단말(또는 스마트 카드)에 저장된 대칭키(K_{MH})가 credentials로 사용된다. 프로토콜 수행에서, HAS는 메시지 (M4)를 수신 후, E1복호 및 $Auth_{MH} \stackrel{?}{=} H(PW, N_M, ID_M, ID_F)$를 검증함으로써 사용자 및 단말을 모두 인증할 수 있다.
- 사용자에 의한 HAS 인증(HAS authentication by the user) : 사용자는 HAS와 사전에 공유된 credentials를 HAS가 알고 있다는 것을 증명함으로써 HAS를 인증한다. 즉, 사용자는 메시지 (M6) 수신 후, $Auth_{FM} \stackrel{?}{=} H(MSK, Auth_{HF})$를 검증함으로써 HAS를 인증 할 수 있다.
- FAS와 MS의 상호 인증(Mutual authentication of FAS and MS) : FAS와 MS는 사전에 어떠한 credentials도 공유하지 않았기 때문에 서로가 간접적으로 상호 인증을 하게 된다. 즉, FAS는 신뢰할 수 있는 HAS가 MS의 신원(identity)을 보증하고, MS는 신뢰할 수 있는 HAS가 FAS의 신원을 보증하였기 때문에 MS와 FAS는 $Auth_{FM} \stackrel{?}{=} H(MSK, Auth_{HF})$와 $Auth_{MF} \stackrel{?}{=} H(MSK, Auth_{FM})$을 서로 검증하여 MSK를 소유하고 있다는 것을 증명함으로써 상호 인증하게 된다.
- FAS와 HAS의 상호 인증(Mutual authentication of HAS and FAS) : FAS와 HAS는 사전에 공유된 credentials인 대칭키 K_{FH}를 서로가 알고 있다는 것을 증명함으로써 상호 인증을 하게 된다. 즉, HAS는 메시지 (M4)를 수신 후, $Auth_{FH} \stackrel{?}{=} H(K_{FH}, N_F, Auth_{MH})$를 검증함으로써 FAS를 인증 할 수 있고 FAS는 메시지 (M5)를 수신 후, E2와 $Auth_{HF} \stackrel{?}{=} H(PSK, ID_H, ID_F)$를 검증함으로써 HAS를 인증 할 수 있다.

4.2 키 설정(Key establishment)

제안된 프로토콜이 성공적으로 수행되는 경우, 암호학적으로 강력한 2개의 키가 유도 된다. 하나는 MS와 HAS간에 설정되는 PSK이며, 이것은 E3=E_{PSK}($R_F \oplus N_H$)와 D_{PSK}(E3)=($R_F \oplus N_H$)를 계산하는데 사용되고 AID를 갱신하는데 사용된다. 또 하나는 MS와 FN간에 설정되는 MSK이며, 이것은 무선구간의 비밀성을 보장하는 시드(seed)로 사용될 수 있다. MSK는 HAS가 아닌 FAS에서 이 키를 유도하는 것이 네트워크 효율성 측면이나 사용자 프라이버시 측면에서 더 바람직하다[6]. 2개의 키들은 랜덤성과 신규성을 제공하는데 이것은 각 개체들의 동적인 임의의 수 선택에 기인한다.

4.3 사용자 프라이버시(User privacy)

로밍시 모바일 사용자의 신원(ID_M)은 프라이버시 측면에서 중요한 정보이다. 그러므로, 도청자와 공격자들이 사용자의 신원을 알지 못하게 비밀로 유지하여야 한다. 제안된 프로토콜에서는 사용자와 HAS를 제외한 어느 누구도 즉, 외부 공격자(attacker) 및 다른 정당한 사용자, 그리고 FAS 조차도 모바일 사용자의 실제 신원(ID_M)을 알 수 없고 사용자의 이동 내력 및 활동 패턴 등도 추적할 수 없다. 왜냐하면, MS와 HAS만이 유도할 수 있

는 매 인증마다 암호학적으로 그 값이 변하는 ephemeral AID를 사용하고 실제 신원(ID_M)은 인증 메시지에서 평문으로 전송되지 않기 때문이다.

4.4 사전(Dictionary) 공격 및 replay 공격에 대한 안전

-사전(Dictionary) 공격 : 엔트로피가 낮은 패스워드는 이 공격에 취약할 수 있으나 제안된 프로토콜에서는 엔트로피가 높은 대칭키가 사용되고 패스워드는 다른 비밀정보(N_M, ID_M) 등과 함께 사용되므로 이 공격에 안전하다. 즉, 공격자는 패스워드뿐만 아니라 다른 비밀정보들을 함께 추측하여 공격하여야 한다.

-Replay 공격 : 이 공격은 공격자가 사용된 메시지를 재전송하여 이전 키들을 다시 설정하려는 공격방법이다. 제안된 프로토콜에서는 MS와 FAS 및 HAS가 매 인증마다 임의의 수 N_M, N_F, N_H, R_F 를 각각 생성하여 PSK와 MSK를 생성하기 때문에 replay 공격에 안전하다.

4.5 효율성(Efficiency)

-FAS와 HAS 사이의 유선 네트워크 관점 : 글로벌 로밍에서 FAS와 HAS간의 메시지 교환 횟수는 인증 지연시간을 최소화하는데 중요한 요소일 수 있다. FAS와 MS는 지리적으로 가까이에 있어 이들간의 메시지 교환은 전체 인증 대기(latency)시간에 영향을 주지 않지만 FAS와 HAS 간은 지리적으로 떨어져 있어 수 많은 홉(hop)을 거쳐서 교환되기 때문에 인증 대기시간을 크게 증가 시킬 수 있다[9]. 따라서, FAS와 HAS간의 메시지 교환 횟수는 최소화하여야 한다. 제안된 프로토콜에서 FAS와 HAS간의 메시지 교환 횟수는 단지 한번의 round-trip 메시지 교환 수(메시지 M4, M5)가 필요하다.

-무선 대역폭(bandwidth) 관점 : 일반적으로, IEEE 802.16e 네트워크에서 모바일 사용자가 로밍 인증 받기 전에 사용할 수 있는 무선 대역폭은 한정되어 있을 것이다. 따라서, MS와 FN의 BS간 무선 대역폭 사용을 최소화하기 위해서 메시지 M1, M2, M3, M6 그리고 M7의 크기를 가능한 작게 하여야 한다. 메시지 M1에서 AID는 해쉬(hash) 출력 비트(bit) 수이고, 메시지 M2에서는 1개의 ID_F와 1개의 랜덤 넘버 N_F의 비트 수를 가진다. 그리고 메시지 M3에서는 2개의 랜덤넘버 비트 수(E1)와 1개의 해쉬 출력 비트 수($Auth_{MH}$)이고 메시지 M6에서는 1개의 랜덤넘버 비트 수(E3)와 1개의 해쉬 출력 비트 수($Auth_{FM}$)이고 메시지 M7에서는 1개의 해쉬 출력 비트 수($Auth_{MF}$)이다. 표 1에서 보는 바와 같이 해쉬 출력을 128비트, ID_F를 128비트, 랜덤 넘버를 160비트로 가정하면 전체 사용 비트수는 1280 비트 정도로 1.5K 비트를 넘지 않는다.

표 1. 무선 대역폭 사용량

	해쉬출력 (128비트)	IDF (128비트)	랜덤넘버 (160비트)
메시지 (M1)	1		
메시지 (M2)		1	1
메시지 (M3)	1		2
메시지 (M6)	1		1
메시지 (M7)	1		
총 계	4(512비트)	1(128비트)	4(640비트)

-연산 부하의 관점 : 프로토콜 수행에서 MS 측의 계산 량이 많아지면 실시간 인증에 걸리는 시간도 많이 소요되며 배터리 소모도 많아진다. 그리고 MS는 한정된 자원(resource)을 가지고 있기 때문에 가능한 MS의 계산 량을 최소화하여야 한다. 제안된 프로토콜에서 MS의 계산 량은 표 2와 같이 대칭키 암호 1번 및 복호 1번과 해쉬 7번 등이 필요하다. FAS의 계산 량은 대칭키 암호 2번 및 복호 1번, 그리고 해쉬 5번 등이 필요하며 HAS의 계산 량은 대칭키 암호 1번 및 복호 1번, 그리고 해쉬 5번 등이 필요하다. 이러한 연산 부하는 각 개체들이 수행할 수 있는 적당한 계산량이다.

표 2. 각 개체들의 연산 부하

	MS	FAS	HAS
해쉬	7	5	5
대칭키 암호화	1	2	1
대칭키 복호화	1	1	1
랜덤넘버 생성	1	2	1
eXclusive OR	2	2	1

V. 결 론

IIEEE 802.16e 시스템에서 사용자(user)와 단말(device) 인증을 제공하기 위해서는 디지털 인증서, 단말용 사전 공유 비밀(preshared secret), 사용자용

사전 공유 비밀(preshared secret) 등과 같은 여러 가지 credentials들이 지원되어야 할 것이다. 본 논문에서 제안된 프로토콜은 2가지 다른 credentials를 사용하여 단말과 사용자를 함께 인증하였다. 사용자용 사전 공유 비밀은 패스워드를 사용하여 사용자를 인증하였고 단말용 사전 공유 비밀은 단말에 저장된 대칭키를 사용하여 단말을 인증하였다. 그리하여, 2번의 EAP(Double EAP) 수행을 할 필요 없이 1번의 EAP(single EAP) 수행으로 사용자와 단말 인증이 가능하게 되었다.

본 논문은 IEEE 802.16e 네트워크 서비스 사업자들간의 로밍 인증 및 키 설정 프로토콜을 제안하고 분석하였는데 이것은 가입자들에게 글로벌 로밍 서비스를 제공하기 위해서는 필요한 연구분야라고 할 수 있다. 실제로 제안된 프로토콜을 IEEE 802.16e 네트워크에 구현하기 위해서는 EAP 및 AAA(Authentication, Authorization and Accounting) 프로토콜 형태로 적용하는 작업이 필요하고 미래의 연구 내용은 ALL IP 기반의 4G 모바일 시스템에서 타원곡선 암호(Elliptic Curve Cryptography) 기반의 인증 프로토콜에 대한 것이다.

참 고 문 헌

[1] IEEE Std. 802.16e-2005, "Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems," February 2006.

[2] WiMax Forum Network Working Group Draft, "WiMAX End-to-End Network Systems Architecture, Stage 3: Detailed Protocols and Procedures," April 2006.

[3] WiMax Forum Network Working Group Draft, "WiMAX End-to-End Network Systems Architecture, Stage 2: Architecture Tenets, Reference Model and Reference Points ," April 2005.

[4] B. Aboba, L. Blunk, and J. Vollbrecht, "Extensible Authentication Protocol (EAP)," IETF RFC 3748, June 2004.

[5] B. Aboba, M. Beadles, J. Arkko and P.Eronen, "The Network Access Identifier," IETF RFC 4282, December 2005.

[6] U. Meyer, J. Cordasco, and S. Wetzel, "An Approach to Enhance Inter-Provider Roaming Through Secret Sharing and its Application to WLANs," *Proceedings of The ACM Workshop on Wireless Mobile Applications and Services on WLAN Hotspots(WMAHS'05)*, September 2005.

[7] C. Rigney, S. Willens, A. Rubens, and W. Simpson, "Remote Authentication Dial-In User Service (RADIUS)," IETF RFC 2865, June 2000.

[8] Guonin Yang, D.S.Wong, X.Deng, "Efficient Anonymous Roaming and Its Security Analysis", *Proceedings of the 3rd International Conference on Applied Cryptography and Network Security(ACNS2005)*, LNCS 3531, Springer-Verlag, 2005.

[9] L. Salgarelli, M. Buddhikot, J. Garay, S. Patel, and S. Miller, "Efficient authentication and key distribution in Wireless IP networks," *IEEE Wireless Communications Magazine*, 10(6), 2003.

[10] A. Menezes, P. C. van Osrschot, and S. A.Vanstone, "Handbook of Applied Cryptography", CRC Press, 1996.

박 영 만 (Young Man Park) 정회원

1982년 2월 한양대학교 전자통신공학 (공학사)
1998년 9월 한양대학교 전자통신공학 (공학석사)
2004년 8월 한양대학교 전자통신전파공학 (공학박사)
1990년~현재 KT인프라연구소
<관심분야> 무선 통신, 네트워크 보안, 정보보호

박 상 규 (Sang Kyu Park) 정회원

1974년 2월 전기공학 (공학사)
1980년 5월 Duke Univ. 통신공학 (공학석사)
1987년5월 Univ.of Michigan 통신공학 (공학박사)
1976년 7월~1978년 10월 국방과학 연구소
1990년 8월~1991년 8월 Univ. of Southern California 객원교수
1987년 3월~현재 한양대학교 공과대학 전자통신컴퓨터공학부 교수
<관심분야> 무선 통신, 디지털통신, 네트워크 보안