EAP-AKA를 적용한 WiBro 무선 네트워크의 인증구조 연구

정회원 임 선 희*, 이 옥 연**, 전 성 익*** 한 진 희****

A Study on EAP-AKA Authentication Architecture for WiBro Wireless Network

Sun Hee Lim*, Okyeon yi**, Sungik Jun***, Jin-Hee Han**** ***Regular Members***

요 약

WiBro(휴대 인터넷)는 언제 어디서나 고속으로 무선 인터넷 접속이 가능한 서비스를 위한 기술이다. 노트북을 비롯한 휴대가 간편한 PDA, 스마트폰으로 사람이 보행 또는 차량 주행 중에서도 끊김없이(seamless) 무선 인터넷 서비스가 가능하다. 휴대 인터넷 서비스는 무선랜과 3G 이동통신이 제공하는 데이터 통신을 융합하고, 두 서비스의 단점을 보완하는 형태의 무선 통신 서비스라고 할 수 있다. 이동성과 고속 무선 통신이 가능한 서비스에서 가장 중요한 기술 요소 중 하나가 보안이다. 본 논문은 안전한 서비스를 제공하기 위하여 WiBro 무선 네트워크에서의 UICC 기반의 EAP-AKA 인증 프로토콜을 적용한 사용자 인증 메커니즘의 상세한 프로토콜을 제안한다. 따라서 EAP-AKA 기반의 무선 네트워크 인증을 통하여 WiBro 무선 네트워크에서 뿐만 아니라 USIM 기반의 WCMDA 등의 이기종 무선 네트워크와의 연동(interworking)에서도 보다 효율적으로 적용할 수 있다.

Key Words : WiBro Security mechanism, IEEE 802.16e, Authentication, EAP-AKA

ABSTRACT

WiBro(Portable Internet Service) is service being capable to provide a high data rate wireless internet access with Personal Subscriber Station under the stationary or mobile environment, anytime and any where. It will fill the gap between very high data rate wireless local area networks and very high mobility cellular systems. The security is an important point of WiBro providing high data and mobile wireless services. This paper proposes user authentication mechanism of WiBro wireless networks applied EAP-AKA authentication protocol. As a result of Wireless authentication based on EAP-AKA, this mechanism is capable to be used in WiBro-WLAN-3GPP interworking scenario as well as the WiBro authentication mechanism.

Ⅰ. 서 론

언제 어디서나 인터넷에 접속하여 필요한 정보를 얻을 수 있는 고속 이동 인터넷 환경을 제공하기 위한 서비스가 2.3GHz 휴대인터넷(WiBro: Wireless Broadband)이다.[12] 사용자가 보행 또는 차량 주행 등의 이동환경에서 고속으로 인터넷에 접속해 필요한 정보나 멀티미디어를 즐길 수 있는 무선 네트워크를 이용한 데이터 서비스로서 이동 멀티미디어 서비스가 가능하다.[8] 고속 이동 중에도 인터넷에

※본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음
* 고려대학교 정보보호대학원 (capsunny@korea.ac.kr), ** 국민대학교 자연과학대학 수학과 (oyyi@kookmin.ac.kr),
*** 한국전자통신연구원 (sijun@etri.re.kr), **** 한국전자통신연구원 (hanjh@etri.re.kr)
논문번호 : KICS2005-11-457, 접수일자 : 2005년 11월 11일, 최종논문접수일자 : 2006년 3월 22일

접속할 수 있다는 점에서 기존 핫스팟 공중망 무선 랜과 차별화되고 있으며, 고속으로 데이터 통신이 가능한 점에서 기존 이동통신의 데이터 서비스와 차별화되는 강점을 가진다.

그러나 이러한 휴대인터넷의 안전한 서비스를 위해 중요한 기술 요소 중 하나가 보안이다. 안전한 고속 이동 무선 네트워크 서비스를 제공하기 위해서는 기본적으로 네트워크 보안, 단말 보안, 사용자 보안을 고려할 수 있고, 더불어 타 망과의 연동 시 망간의 보안 연동 구조도 설계되어야 하며, Mobile IP, 무선 그룹 멀티캐스팅 등의 여러 보안 요소들이 고려되어야 한다.

본 논문에서는 여러 보안 요소들 중에서 IEEE 802.16에서 제안하고 있는 WiBro 무선 네트워크 보안의 취약점을 분석한다.[1, 9]

WiBro 무선 네트워크 보안에서의 취약점을 해결하기 위한 방법으로 본 논문에서는 EAP-AKA 인증 프로토콜 적용을 제시한다.

3GPP에서 무선랜과의 연동을 위해 제안한 인증 프로토콜인 EAP-AKA를 WiBro 무선 네트워크에서도 적용하여 사용자와 네트워크간의 상호 인증 및 사용자 인증 정보를 UICC 기반의 스마트 카드에서 관리 및 처리하여 보다 안전한 인증 메커니즘을 설계할 수 있는 세부적 방안을 제시한다.

Ⅱ. WiBro 네트워크 보안 구조 분석

WiBro MAC 보안 구조는 IEEE 802.16e Privacy 계층을 기반으로 정의한다.[1, 6] 이는 IEEE 802.16의 MAC 구조와 동일하게 그림 1과 같다. 인증 및 키 관리를 위한 PKM(Privacy Key Management) 프로토콜과 패킷 데이터에 대한 암호화를 위한 Encryption 프로토콜로 구성된다.

Privacy 부계층은 PKM 메시지 기반으로 인가 제어(Authorization/SA Control), RSA 기반 인증, EAP 캡슐화로 이루어진다. PKMv1에서는 기지국(RAS/ACR)이 단말(MS)을 인증하는 단방향 인증 구조이다. 현재는 단말과 기지국간의 양방향 인증을 제공하는 PKMv2가 제안되었다. PKM 기반의 인증 프로토콜에서는 다음과 같은 두 단계의 보안 구조로 이루어진다.

<1> MS Authorization and AK Exchange 단계
<2> TEK Exchange 단계

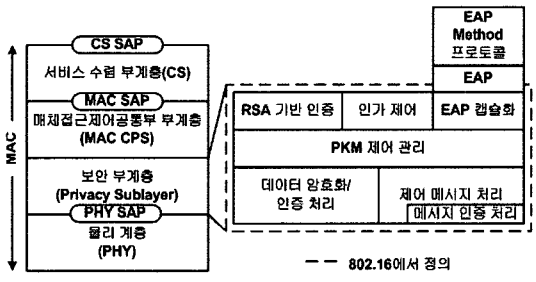

그림 1. IEEE 802.16e MAC 계층 보안 구조

2.1 PKMv1 인증 시나리오

<1>의 과정에서 PKMv1에서는 RSA 기반 인증을 필수로 단말 인증을 제공한다. 제조업체로부터 각 단말마다 유일하게 발급받은 X.509 인증서를 통해 BS(RAS/ACR)에게 인증 요청을 하면 BS는 단말의 인증서를 검증한다. 검증이 성공하면 BS는 AK(Authentication Key)를 생성하여 단말 인증서의 공개키를 통해 WiBro 단말에게 전송한다. 단말은 자신의 공개키로 암호화된 AK를 수신하면 AK를 복호화한다. 이로서 단말과 BS간의 AK를 공유하게 된다.

무선 네트워크간의 AK를 안전하게 공유하게 된 결과로 단말과 BS는 AK를 통해 키 전송 암호화 키(KEK : Key Encryption Key)와 MAC 키(HMAC_KEY_D/HMAC_KEY_U)를 유도할 수 있다.

과정 <2>에서는 MS가 BS에게 키 요청 메시지를 보내면 BS가 생성한 TEK(Traffic Encryption Key)를 AK에서 유도한 KEK로 암호화하여 전송한다. KEK로 암호화된 TEK를 수신한 MS는 TEK를 복호화 하여 MS와 BS 무선 네트워크간의 데이터를 암호화할 키 분배가 성공적으로 이루어진다.

그림 2는 앞에서 설명한 PKMv1 인증 절차와 키 분배 과정이다.

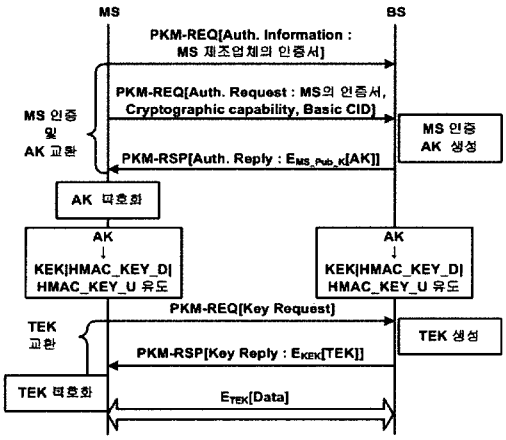

그림 2. PKMv1 RSA 기반 인증 프로토콜 및 키 분배 과정

2.2 PKMv1 보안 취약점

PKMv1은 무선 네트워크가 제조업체나 제 3의 신뢰기관으로부터 발급 받은 인증서로 단말을 인증하는 단방향 단말 인증 메커니즘이다. 사용자 인증 및 네트워크 인증은 지원하지 않고 있다. 이와 같은 인증 메커니즘은 무선 네트워크를 신뢰할 수 있다는 전제 조건이 필요하다. 그렇지 않으면 rogue BS의 위장 공격이 가능하다. 뿐만 아니라 인증 키(AK)와 데이터 암호화 키(TEK)를 BS가 일방적으로 생성하여 전송하는 키 분배 방식으로 무선 네트워크 인증 절차 없이 네트워크에서 생성한 키로 서비스를 하는 점에서 PKMv1은 보안에 매우 취약하다. 고속의 이동성을 제공하는 WiBro 무선 네트워크 환경에서의 인증 메커니즘으로 PKMv1은 취약하여 상위 계층에서의 보안이 반드시 필요하다. 그리고 이동하는 단말을 BS에서 단말의 인증서를 검증해야 하는 오버헤드의 문제가 있다.

이러한 PKMv1 인증 및 키 분배 방식의 취약점 및 비효율성을 보완하여 PKMv2가 제안되었다[1].

2.3 PKMv2 인증 시나리오

PKMv2는 단말 인증과 사용자 인증을 제공하고 사용자와 무선 네트워크 간의 양방향 인증을 지원한다. PKMv2는 RSA 기반 인증과 EAP 기반 인증 두 가지 인증 메커니즘이 사용가능하다.

2.3.1 RSA 기반 상호 인증 메커니즘 및 키 분배

PKMv2 RSA 기반에서의 MS와 BS간의 상호 인증 및 AK 교환은 그림 3과 같다.

MS가 Authentication Information 메시지에 제조업체의 인증서를 포함하여 보냄으로 BS는 클라이언트 MS의 인증서의 정보를 알 수 있다. 이 메시지는 제조업체 인증서의 정보만을 포함한 메시지로 BS는 이 메시지를 무시할 수도 있다. MS는 BS에게 SAID(Security Association Identity)와 AK 요청 메시지를 보낸다. Authentication Request 메시지 <1>은 다음과 같은 인증 정보를 포함한다.

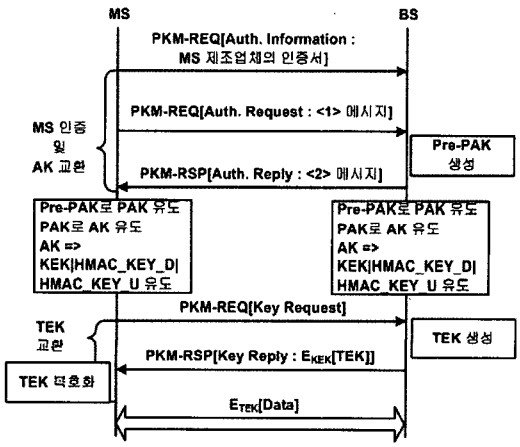

그림 3. PKMv2 RSA기반 상호 인증 및 키 분배 과정

<1> Authentication Request
(1) MS의 인증서
(2) MS의 cryptographic capability
(3) MS의 Basic CID. 즉, primary SAID
(4) MS가 생성한 64비트 랜덤 넘버

(1)~(4) 정보를 포함한 Authentication Request 메시지를 수신한 BS는 MS의 인증서를 검증하여 MS와 안전한 통신을 하기 위한 암호 알고리즘 및 프로토콜을 결정한다. 정당한 MS를 검증하면 BS는 자신을 검증시키기 위한 인증 정보와 AK를 유도하기 위한 Pre-PAK를 MS의 공개키로 암호화하여 전송한다.

BS가 MS에게 보내는 Authentication Reply 메시지 <2>는 다음과 같은 인증 정보를 포함한다.

(1)* BS의 인증서
(2)* $E_{MS\_Pub\_K}$(Pre-PAK)
(3)* 64비트 PAK sequence number
(4)* PAK lifetime
(5)* SAID
(6)* 수신된 MS에서 생성한 64비트 랜덤 넘버
(7)* BS에서 생성한 64비트 랜덤 넘버
(8)* RSA 서명

MS는 BS가 (1)*~(8)*과 같은 인증 정보를 포함한 Authentication Reply 메시지를 수신하면 BS의 정당성을 검증한다. 이로서 MS와 BS간의 상호 인증 절차가 이루어지고 BS에서 생성하여 전송한 Pre-PAK로 MS와 BS는 PAK, AK를 유도한다. RSA 기반의 PKMv2 인증 프로토콜은 MS와 BS간의 상호 인증을 제공하고 PKMv1에서 AK를 전송하는 키 분배 방식이 아닌 Pre-PAK를 통해 MS와 BS가 각각 AK를 유도하는 방식으로 보다 안전한 키 분배 방식이 적용된다. 하지만 RSA 기반의 인증 방식은 사용자 인증이 아닌 단말 MS의 인증만을 제공한다.

PAK는 다음과 같이 Pre-PAK로부터 생성된다.

EIK(EAP Integrity Key)는 옵션으로 부가적으로 수행할 EAP(Extensible Authentication Protocol) 메시지를 보호하기 위한 키이다.

$$EIK||PAK=Dot16KDF(pre\text{-}PAK,\ MS\ MAC\ Address||BSID||"EIK+PAK",\ 320)$$

2.3.2 EAP 기반의 상호 인증 메커니즘 및 키 분배

PKMv2 RSA 기반 인증 메커니즘은 단말이 제조업체로부터 발급받은 인증서로 인증을 수행하는 방식이다. 이는 단말 인증은 가능하지만 그 단말을 사용하는 사용자 인증은 제공하지 못한다. 사용자 인증을 제공하기 위해 PKMv2에서는 추가적으로 EAP 기반의 인증 메커니즘을 선택할 수 있도록 제공하고 있다.

그림 4는 PKMv2 EAP 기반의 인증 메커니즘과 키 분배 과정을 나타낸다.

PKMv2 EAP 인증은 다양한 인증 프로토콜 방식을 적용할 수 있는 메커니즘이다. RFC 3748[4]에서 정의한 EAP를 이용한 EAP-TLS, EAP-SIM 등 다양한 인증 프로토콜을 사용할 수 있기 때문에 RSA 기반의 인증에서 제공하는 단말 MS와 BS의 상호 인증 뿐만 아니라 다양한 인증 프로토콜을 적용하여 사용자와 무선 네트워크간의 상호 인증이 가능하다.

EAP 기반의 인증 메커니즘에서는 AAA 인증 서버를 구성함으로서 고속 이동 무선 네트워크의 인증 절차 기능을 세분화하고 앞으로 무선 네트워크 사용자가 증가되어도 BS가 모든 사용자와 단말 MS을 관리해야 하는 오버헤드가 생기지 않는다.

BS는 EAP 프로토콜 절차에서는 MS와 AAA 인증 서버와의 릴레이 기능만을 수행한다.

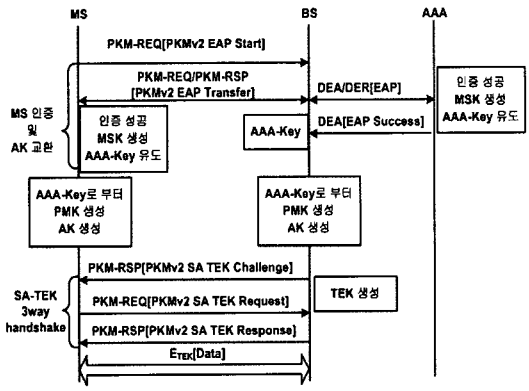

그림 4. PKMv2 EAP 기반 인증 메커니즘 및 키 분배 과정

인증 서버(AAA : Authentication, Authorization, Account)가 사용자 인증 정보를 관리함으로서 보다 효율적이고 안전한 보안 메커니즘을 제공한다.[10]

해당 장치의 권한을 부여받은 사용자에 한해서 인증이 수행된다. 사용자 인증은 BS를 통해 인증 서버로 인증 요청을 시작으로 인증 절차가 이루어진다. PKMv2에서는 RSA 기반 인증과 EAP 기반 인증 둘 중 하나를 선택하거나 모두 선택 가능하다. 하지만 앞에서 언급한바와 같이 RSA 기반 상호 인증을 통해 단말 MS와 BS간의 상호 인증을 수행하여 결합한 후에 EAP 기반 인증 프로토콜을 사용하여 사용자 인증 절차를 수행하면 보다 안전한 무선 네트워크를 구성할 수 있다.

EAP 인증 프로토콜 결과로 MS와 인증 서버에서 생성된 AAA-Key를 인증 서버가 BS에게 전송한다. 인증 서버와 BS간의 네트워크는 안전한 구간이라고 전제한다. AAA-Key를 수신한 BS는 MS와의 안전한 통신을 위해 다음과 같이 PMK와 AK를 유도한다. EIK는 MS와 BS에서 협의하여 추가로 EAP 인증 절차를 수행할 경우에 EAP 메시지를 보호하기위한 키이다.

$$EIK\ ||\ PMK\ =\ truncate(AAA\text{-}Key,\ 320)$$

$$if(PAK\ and\ PMK)$$
$$AK <= Dot16KDF(PAK \oplus PMK,\ MS\ MAC\ Address||BSID||PAK||"AK",\ 160)$$

$$else\ if(PAK)$$
$$AK <= Dot16KDF(PAK,\ MS\ MAC\ Address||BSID||PAK||"AK",\ 160)$$

$$else$$
$$AK <= Dot16KDF(PMK,\ MS\ MAC\ Address||BSID||"AK",\ 160)$$

EAP 인증 방식에 따라 단방향 사용자 인증과 양방향 사용자 인증이 가능하고 성공적인 인증 결과에 따른 키 생성 결과도 다르다. 보다 안전하고 효율적인 인증 프로토콜의 적용은 무선 네트워크 환경에 따라 운용되어야 할 것이다.

Ⅲ. WiBro 무선 네트워크에서 EAP-AKA 인증 프로토콜 적용 및 효과

IEEE 802.16은 WiBro 무선 네트워크에서의 MAC 계층 보안 요소에 대해 정의한다. RSA 기반 인증

과 EAP 기반 인증 메커니즘을 제안하고 있다. EAP 기반의 다양한 인증 프로토콜 적용은 IEEE 802.16에서는 제안하고 있지 않다.

본 논문에서는 EAP 기반 인증 메커니즘에서 UICC(Universal IC Card)를 사용하는 EAP-AKA 인증 프로토콜을 WiBro 무선 네트워크 인증 메커니즘에 적용하고 그에 따른 효율성을 분석한다.

3.1 EAP 프로토콜

EAP[4]는 IEEE 802.1x 포트 기반의 가입자 인증 데이터 전송을 위한 표준 프로토콜이다. 다중 인증 메커니즘을 지원하는 프로토콜로서 스마트 카드, Kerberos, 공용키 암호화, OTP(One Time Password)를 포함한 수많은 인증 방식을 지원한다. 현재 IETF에 EAP 워킹 그룹이 설치되어 ID/Password, 인증서, 스마트 카드 등 다양한 인증 방식을 지원하는 알고리즘과 각 인증 알고리즘을 이용한 세션 키 생성 방법의 표준화를 추진하고 있다.

3.2 AKA(Authentication and Key Agreement) [2][5]

3GPP(3rd Generation Partnership Project)에서 제안하여 유럽 3G 이동통신에서 사용되는 인증 및 키 일치 메커니즘이다. AKA 인증 및 키 일치 프로토콜은 GSM(Global System for Mobile Communication) 인증 메커니즘과의 backward compatibility를 지원하고, GSM과 비교하여 볼 때 키 길이가 충분히 크고, 클라이언트 뿐만 아니라 서버까지 인증하는 상호 인증 방식을 제공한다. 또한 UICC/USIM (UMTS Subscriber Identity Module) 등 스마트 카드 기반으로 하는 인증 및 키 일치 메커니즘이다.

3.3 EAP-AKA[2]

3GPP에서 제안한 AKA 방식을 EAP의 인증 프로토콜에 적용하여 3GPP와 무선랜과의 seamless한 연동 보안 인증 프로토콜로 EAP-AKA를 3GPP에서 제안하고 있다[3]. 본 논문에서는 EAP-AKA를 WiBro 무선 네트워크 인증 메커니즘 PKMv2 EAP 기반의 인증 절차에 적용하여 사용자와 무선 네트워크간의 상호 인증과 세션 키를 생성한다. 그리고 사용자 인증 정보를 단말이 아닌 UICC에 안전하게 저장, 관리, 처리함으로서 사용자 인증 정보를 보호할 수 있다.

EAP-AKA를 적용한 3GPP-WLAN 연동 네트워크에서 EAP-AKA를 적용한 WiBro 무선 네트워크까지도 쉽게 접목시킬 수 있는 seamless한 연동 보안 인증 메커니즘이 가능하다.

EAP-AKA는 그림 5와 같은 시스템이 구성된다.

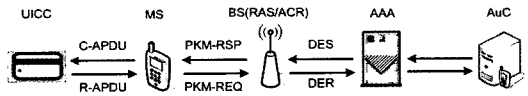

그림 5. EAP-AKA를 위한 WiBro 네트워크 구성

① AuC(Authentication Center)

인증 데이터 센터로서 3GPP에서는 별도의 AuC가 구성된다. 3GPP-WLAN과의 연동을 고려한 경우는 연동 보안을 관리하는 AuC가 AV(Authentication Vector)를 생성한다.

$$AV = RAND \parallel XRES \parallel CK \parallel IK \parallel AUTN$$

WiBro 무선 네트워크 인증 메커니즘만을 고려할 경우 AuC의 역할을 AAA 인증 서버가 할 수 있다.

② UICC

네트워크를 검증하기 위해 AUTN 값을 검증한다. AUTN 검증이 실패한 경우는 인증 실패로 연결 시도를 끊는다. Sequence number가 동기 범위 안에 들지 않으면 동기화 과정을 다시 수행한다. AUTN의 검증이 성공하면 UICC는 RES, IK(Integrity Key), CK(Cipher Key)를 생성하고 이를 단말에게 전송한다.

③ Terminal(단말 MS)

단말에서 MSK를 생성할 경우 수신된 CK, IK로부터 새로운 키를 유도한다. New temporary identifier를 복호화하여 다음 인증에 사용하기 위해 단말에 저장한다. 무선 네트워크에서의 데이터 암복호화와 무결성 처리를 한다.

④ BS(Authenticator)

AAA 프로토콜을 사용한 인증 서버(Authentication Server 혹은 EAP Server)와 연결하는 시스템이다. EAP 서버와 클라이언트 사이의 EAP 메시지를 relay 하는 기능을 한다. 무선 네트워크에서의 데이터 암복호화와 무결성 처리를 한다.

⑤ EAP Server/AAA 인증 서버

가입자 Identity를 확인 후에 가입자 인증을 위한 AV값을 AuC로부터 받는다. AV를 통해 key material을 유도하여 Authenticator에게 전송한다. AAA

인증 서버는 Diameter 프로토콜 혹은 RADIUS 프로토콜로 구현될 수 있다.

3.4 WiBro에서의 PKMv2/EAP-AKA 인증 프로토콜 적용 메커니즘

스마트 카드 기반의 UICC에 안전하게 보관된 사용자 Identity와 암호화키를 이용하여 사용자와 단말 개념의 인증을 동시에 수행하고, Pseudonym Identity를 이용하여 강화된 보안성을 제공한다.[7] AKA 알고리즘을 이용하여 인증 절차에서 서버와 단말에 서로 독립적이면서 동일한 값으로 생성되는 MSK로부터 AK를 생성하므로, RSA 기반 방식과는 달리 서버에서 단말로 암호화 키를 전달할 필요가 없다.

그림 6은 UICC를 사용한 WiBro 무선 네트워크에서의 EAP-AKA 인증 프로토콜을 이용한 전체 인증 성공 시나리오를 나타낸다. 이때의 EAP 프로토콜의 종단은 UICC와 AAA 인증 서버이다.

UICC를 사용한 EAP-AKA 인증 프로토콜은 UICC와 AAA 인증 서버간의 EAP 프로토콜을 통해 상호 인증을 한다. UICC에서 EAP-AKA 패킷을 생성하기 때문에 MS는 EAP 하위 계층에서 EAP 패킷을 송수신한다. EAP 패킷의 MAC(AT_MAC) 계산 및 검증을 포함한 인증 프로토콜의 절차를 모두 UICC에서 처리하므로 사용자는 단말에 독립적이고 또한 단말을 통한 인증 정보의 노출을 막을 수 있다.

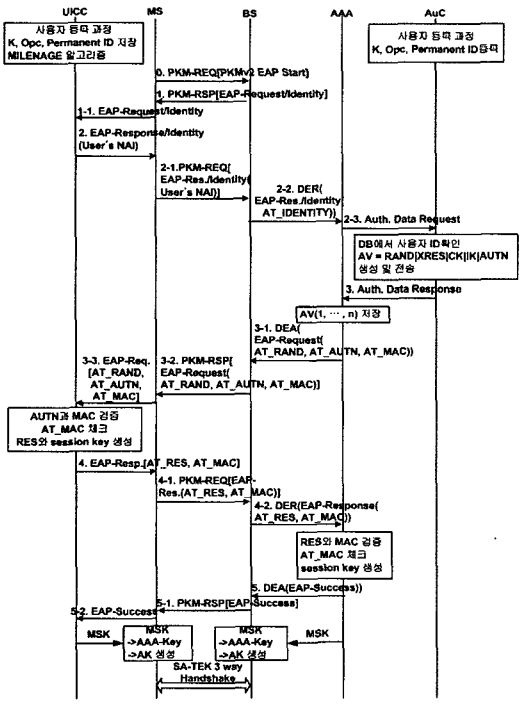

그림 6. WiBro 무선 네트워크에서의 EAP-AKA를 적용한 전체 인증 성공 시나리오(UICC에서 EAP 종단 시나리오)

그림 7은 UICC에서 AKA 인증 절차를 수행하고 단말에서 EAP 프로토콜 과정이 이루어지는 전체 인증 시나리오를 나타낸다. 이때의 EAP 프로토콜의 종단은 MS와 AAA 인증 서버이다. 그림 7과 같은 시나리오에서는 UICC에서 AKA 인증 프로토콜의 절차를 수행하고 MS에서 EAP Encapsulation/Decapsulation 기능을 한다. MS에서 송수신된 EAP 패킷의 MAC 검증 및 계산을 수행한다. 단말은 UICC로부터 CK, IK, Identity를 수신하여 MK를 유도한다. 이 절차는 단말에 의존적으로 EAP-AKA 인증 절차를 수행하게 된다.

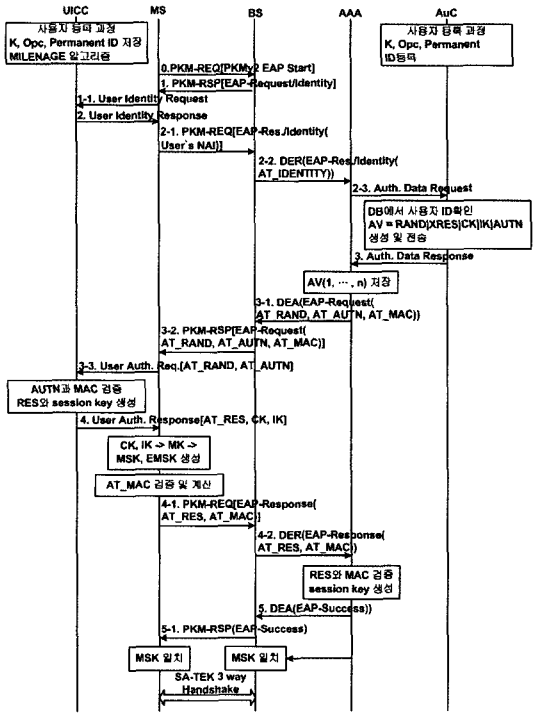

그림 7. WiBro 무선 네트워크에서의 EAP-AKA를 적용한 전체 인증 성공 시나리오(MS에서 EAP 종단 시나리오)

3.4.1 초기 사용자 등록 데이터

① UICC에 저장된 데이터 및 암호학적 함수

표 1은 WiBro 무선 네트워크 초기 사용자 등록 후에 UICC에 저장되는 데이터와 암호학적 함수 이다.

② AuC에 초기 저장된 데이터 및 암호학적 함수

AuC에 초기 저장된 데이터는 통신 사업자가 임의로 생성한 키 값 OP, SQN을 생성하기 위한 메

표 1. 사용자 등록 후 저장된 데이터와 암호학적 함수

기호	설명
OPc	통신 사업자 키 OP값을 암호화한 값
K	AuC와 공유하는 비밀키
THRESHOLD	재인증(fast re-auth.)의 lifetime 제어
Permanent Identity	사용자의 유일한 ID. 3G와 연동할 경우 IMSI를 NAI 형식으로 변환
SQN_{UICC}	사용자 등록 후 HE로부터 받은 초기값
f1	네트워크를 인증(MAC)을 계산하기 위한 메시지 인증 함수
f1*	재동기화를 위한 메시지 인증 함수
f2	사용자 인증(RES/XRES) 계산하기 위한 메시지 인증 함수
f3	암호화 키(CK)를 유도하기 위한 키 생성 함수
f4	무결성 키(IK)를 유도하기 위한 키 생성 함수
f5	정상적인 과정에서 익명성 키(AK:Anonymity Key)를 유도하기 위한 키 생성 함수
f5*	재동기화에서 익명성 키를 유도하기 위한 키 생성 함수

커니즘 SQN_{HE}, 난수 생성 함수 f0, 인증 함수 및 키 생성 함수인 f1~f5, f1*, f5* 함수가 있다.

사용자 초기 등록 후 AuC에는 K, OPc, Permanent ID, THRESHOLD 저장 및 SQN_{HE} 초기 값을 할당한다.

3.4.2 UICC에서의 EAP 종단 인증 절차

Step 0. (MS ⇒ BS)
PKM-REQ[PKMv2 EAP Start]

단말은 BS에게 PKM 요청 메시지로 PKMv2 EAP Start 메시지를 보내어 인증 시작을 요청한다. PKMv2 EAP Start 메시지를 수신한 BS는 EAP 인증 절차를 시작하고 인증 서버와 연결하여 EAP 프로토콜의 중계 역할을 한다.

Step 1. (BS ⇒ MS)
PKM-RSP[EAP Request/Identity]
Step 1-1. (MS ⇒ UICC) *EAP Request/Identity*

단말로부터 PKMv2 EAP start 메시지를 수신한 BS는 단말에게 ID 요청 메시지를 보낸다.

BS로부터 ID 요청 메시지를 수신한 단말은 UICC 카드로 사용자 신원 요구 메시지를 EAP 패킷으로 보낸다.

Step 2 : (UICC ⇒ 단말)
EAP-Response/Identity(User's NAI)
Step 2-1 : (MS ⇒ BS)
PKM-REQ[EAP-Res./Identity(User's NAI)]
Step 2-2 : (BS ⇒ AAA)
DER(EAP Res./Identity(AT_IDENTITY))
Step 2-3 : (AAA ⇒ AuC)
Authentication Data Request

사용자 신원 요구 메시지를 수신한 UICC는 AuC까지 Permanent Identity 혹은 Pseudonym Identity를 보낸다. Permanent Identity는 각 사용자의 유일한 식별자로 NAI(Network Access Identifier) 형식에 맞아야 하며 3G와 연동할 경우는 IMSI를 변환하여 사용한다.

Step 3 : (AuC ⇒ AAA)
Authentication Data Response
Step 3-1 : (AAA ⇒ BS)
DEA(EAP-Req.(AT_RAND,AT_AUTN, AT_MAC))
Step 3-2 : (BS ⇒ MS)
PKM-RSP[EAP-Req.(AT_RAND,AT_AUTN,AT_MAC)]
Step 3-3 : (MS ⇒ UICC)
User Auth. Req.[AT_RAND,AT_AUTN,AT_MAC]

UICC로부터 사용자 Permanent Identity 혹은 Pseudonym Identity를 수신한 AuC는 사용자 DB에 확인 한 후에 AV를 생성하여 AAA 인증 서버에 전송한다. AuC로부터 AV를 수신한 인증 서버는 AV값 중에 AT_RAND, AT_AUTN, 이 값들을 포함한 EAP 패킷의 keyed 해쉬 값(AT_MAC)을 계산하여 전송한다.

$$AT\_RAND = f0()$$
$$AK = f5_K(RAND)$$
$$MAC = f1_K(SQN_{HE} \,||\, RAND \,||\, AMF)$$
$$AUTN = SQN_{HE} \oplus AK \,||\, AMF \,||\, MAC$$
$$AT\_MAC = HMAC\_SHA1\_128_{K\_aut}(EAP\ Packet)$$

AT_RAND, AT_AUTN, AT_MAC 값을 수신한 UICC는 수신한 AUTN의 MAC값과 계산한 XMAC을 비교하여 검증한다. MAC 검증에 실패하면

AuC에게 인증 실패 메시지를 보낸다.

$$XMAC = f1_K(SQN_{HE} \parallel RAND \parallel AMF)$$

MAC 검증이 성공하면 수신한 SQN값을 자신이 체크하고 있는 SQN_{UICC} 범위 안에 들면 동기화에 성공한다. 동기화에 실패하면 UICC는 재동기 요청 메시지를 AuC에게 전송하면서 AT_AUTS값을 보내어 AuC에서 SQN을 갱신하도록 한다. Step 3의 과정은 무선 네트워크를 검증한다.

Step 4 : (UICC ⇒ MS)
EAP-Response[AT_RES, AT_MAC]
Step 4-1 : (MS ⇒ BS)
PKM-REQ[EAP-Res.(AT_RES, AT_MAC)]
Step 4-2 : (BS ⇒ AAA)
DER(EAP-Res.(AT_RES, AT_MAC))

네트워크 인증이 검증되면 UICC는 RES를 계산하여 EAP 패킷으로 보낸다. 이 EAP 패킷의 AT_MAC을 계산하여 같이 보낸다.

$$RES = f2_K(RAND)$$

AAA 서버는 수신한 RES와 AT_MAC을 자신이 계산한 XRES와 비교 검증한다.

$$XRES = f2_K(RAND)$$

성공적으로 검증되면 사용자 인증이 성공이다. Step 4 결과로 상호 인증이 이루어지다.

Step 5 : (AAA ⇒ BS) *DES(EAP-Success)*
Step 5-1 : (BS ⇒ MS) *PKM-RSP[EAP-Success]*
Step 5-2 : (MS ⇒ UICC) *EAP-Success*

인증 서버와 사용자간의 상호 인증이 성공적으로 이루어지면 UICC와 인증 서버는 MK(Master Key)를 생성하고 PRF(Pseudo-Random number Function)함수를 이용하여 MK로부터 K_encr, K_aut, MSK(Master Session Key), EMSK(Extended Master Session Key)를 유도한다. *MK = SHA1(Identity || IK || CK)*

PRF(MK) := K_encr(128bit), K_aut(128bit), MSK(512bit), EMSK(512 bit)

유도한 MSK를 각 무선 구간의 단말과 BS에게 전송하여 무선 구간의 세션 키를 분배한다.

WiBro 무선 네트워크에서 EAP-AKA 인증 프로토콜을 적용하여 사용자와 네트워크간의 상호 인증과 독립적으로 키를 유도한다.

3.4.3 단말에서의 EAP 종단 인증 절차

UICC에서 AKA 절차를 수행하고 단말에서 EAP Encapsulation/Decapsulation을 하는 인증 절차이다. 모든 인증 절차를 UICC에서 수행하는 경우와 비슷한 메커니즘으로 이루어지지만, 단말에서 EAP Encapsulation/Decapsulation하기 위해서 UICC에서 받은 CK, IK, Identity로 MK 및 MSK, EMSK, K_encr, K_aut 키를 유도한다.

Step 0. (MS ⇒ BS)
PKM-REQ[PKMv2 EAP Start]

Step 1. (BS ⇒ MS)
PKM-RSP[EAP Request/Identity]
Step 1-1. (MS ⇒ USIM) *User Identity Request*

Step 2 : (UICC ⇒ MS)
User identity Response
Step 2-1 : (MS ⇒ BS)
PKM-REQ[EAP-Res./Identity(User's NAI)]
Step 2-2 : (BS ⇒ AAA)
DER(EAP-Res./Identity(AT_IDENTITY))
Step 2-3 : (AAA ⇒ AuC)
Authentication Data Request

Step 3 : (AuC ⇒ AAA)
Authentication Data Response
Step 3-1 : (AAA ⇒ BS)
DEA(EAP-Req.(AT_RAND,AT_AUTN, AT_MAC))
Step 3-2 : (BS ⇒ MS)
PKM-RSP[EAP-Req.(AT_RAND,AT_AUTN)]
Step 3-3 : (MS ⇒ UICC)
User Auth. Req.[AT_RAND,AT_AUTN,AT_MAC]

Step 3의 절차가 성공적으로 이루어지면 네트워크 인증이 성공이다.

Step 4 : (UICC ⇒ MS)
User Auth. Res.[AT_RES, CK, IK]

Step 4-1 : (MS ⇒ BS)
PKM-REQ[EAP-Res.(AT_RES, AT_MAC)]
Step 4-2 : (BS ⇒ AAA)
DER(EAP Res.(AT_RES, AT_MAC))

네트워크 인증이 검증되면 UICC는 계산한 RES 값과 CK, IK를 단말로 전송한다. CK, IK를 수신한 단말은 CK, IK, Identity값으로 MK를 유도하고, MSK, EMSK, K_encr, K_aut를 생성한다. K_aut 키로 Step 3 과정의 AT_MAC을 검증하고, Step 4 과정의 AT_MAC을 계산한다.

$CK = f3_K(RAND)$
$IK = f4_K(RAND)$

Step 5 : (AAA ⇒ BS)
DES(EAP-Success)
Step 5-1 : (BS ⇒ MS)
PKM-RSP(EAP-Success)

Step 5과정에서 EAP-success로 완료되면 사용자와 무선 네트워크간의 상호 인증과 키 일치가 이루어진다.

단말에서 EAP 프로토콜을 수행하기 때문에 단말에 의존적이며 CK, IK 키가 단말에 전송되어 MK를 단말에서 생성하는 방법으로 단말을 신뢰해야 한다는 전제가 필요하게 된다.

Ⅳ. 결 론

본 논문에서 제안한 WiBro 무선 네트워크에 보안을 위한 UICC 기반의 EAP-AKA 인증 프로토콜을 적용함으로서 IEEE 802.16에서 제공하는 RSA 기반 PKM 인증 프로토콜에서 제공하는 단말 인증, PKM 메시지 보안, TEK의 암호화 전송, EAP 인증에 무결성 제공, 무선 구간 데이터 암호화 기능 뿐만 아니라 스마트 카드 기반의 UICC에 안전하게 보관된 Identity와 암호화 키를 이용하여 사용자와 단말 인증을 동시에 수행하며, Pseudonym Identity를 이용하여 보다 강화된 보안성을 제공할 수 있다.

따라서 본 논문에서는 WiBro 무선 네트워크 보안을 위하여 EAP-AKA의 적용 메커니즘에 대한 상세한 프로토콜을 제안하였으며, 향후 UICC 기반의 WiBro 무선 네트워크, 3G 이동통신, 공중망 무선랜 등의 이기종 무선 네트워크와의 상호 연동(interworking) 보안이 보다 쉽게 이루어질 수 있다.

참 고 문 헌

[1] IEEE, "Standard for Local and metropolitan area networks-Part16:Air Interface for Fixed and Mobile Broadband Wireless Access Systems", IEEE P802.16e/D12,October 2005.

[2] RFC 4187, "Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement(EAP-AKA)", January 2006.

[3] 3GPP TS 33.234, "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security, Wireless Local Area Network(WLAN) interworking security", June 2005.

[4] RFC 3748, "Extensible Authentication Protocol(EAP)", June 2004.

[5] 3GPP TS 33.102, "3rd Generation Patnership Project; Technical Specification Group Services and System Aspects; 3G Security, Security architecture", June 2003.

[6] TTA, "2.3GHz 휴대인터넷 표준-물리계층 및 매체접근제어계층", TTAS.KO-06.0082, Jun. 2005.

[7] 김영세, 이정우, 한진희, 신진아, 전성익, "무선 네트워크 연동 보안 기술 동향", 전자통신동향분석 제20권 제1호, 2005.2

[8] 이문규, 김도우, 전성익, "이동통신과 무선인터넷의 연동 시장 동향 및 전망", 전자통신동향분석 제19권 제1호, 2004.2

[9] IEEE, "Standard for Local and metropolitan area networks-Part16:Air Interface for Fixed and Mobile Broadband Wireless Access Systems", EEE P802.16, Jun 2004.

[10] Moby Dick WP4, "AAAC Design", IST-2000-25394 Project Moby Dick, Jan 2002.

[11] 전성익, 김영세, 한진희, 정교일, 손승원, "Interworking Security for Public WLAN, WiBro and WCDMA : Mobile and wireless systems", 한국통신학회 제22권 8호, 2005.8

[12] 홍대형, 강충구, 조용수, "2.3GHz 휴대인터넷 기술의 국내표준화", TTA 저널 제92호

임 선 희 (Sun Hee Lim) 정회원

1999년 2월 고려대학교 컴퓨터학과 졸업
2005년 2월 고려대학교 정보보호대학원 석사
2005년 3월~현재 고려대학교 정보보호대학원 박사과정
<관심분야> 무선통신, 정보보호

이 옥 연 (Okyeon Yi) 정회원

1988년 2월 고려대학교 수학과 졸업
1990년 2월 고려대학교 이학석사
1996년 8월 Univ. of Kentucky Ph.D.
1999년~2001년 ETRI 선임연구원
2001~현재 국민대학교 수학과 조교수
<관심분야> 무선통신, 정보보호

전 성 익 (Sungik Jun) 정회원

1985년 중앙대학교 전자계산학과(학사)
1987년 중앙대학교 전자계산학과(석사)
1997년~현재 한국전자통신연구원 책임연구원
2003년~현재 한국전자통신연구원 무선보안응용연구 팀장
<관심분야> 정보보호, 무선 보안, 실시간운영체제, 스마트카드기술

한 진 희 (Jin-Hee Han) 정회원

1997년 숭실대학교 전산학과(학사)
1999년 광주과기원 정보통신과(석사)
1999년~현재 한국전자통신연구원 무선보안응용연구팀 선임연구원
<관심분야> 암호설계, 스마트카드, 자바카드, 무선보안기술