휴대인터넷의 보안 구조 및 인증 프로토콜

이지용* · 추연성** · 안정철*** · 류대현*

*한세대학교, **LG전자, ***NSRI

Security Architecture and Authentication Protocol in Portable Internet

J. Y. Lee* · Y. S. Choo** · J. C. Ahn*** · D. H. Ryu*

*Hansei University, **LG Elec. Co., ***NSRI

E-mail : sharp026@daum.net

요 약

무선랜을 확장한 휴대인터넷은 그 셀크기가 이동통신처럼 크고 중저속의 이동성을 지원하면서 이음매 없는(seamless) 서비스를 제공할 수 있다. 휴대인터넷 국제 표준인 IEEE 802.16e에서는 단말과 기지국간 권한인증 및 키 교환을 위해서 PKMv2(Privacy Key Management) 프로토콜을 사용하고 있다. 본 연구에서는 먼저, WMAN(Wireless Metropolitan Area Network) 표준인 IEEE 802.16 표준을 기반으로 이동성을 지원하는 IEEE 802.16e 표준과 TTA 휴대인터넷 표준을 바탕으로 휴대인터넷의 전체 보안 구조를 파악하였다. 그리고 MSS(Mobile Subscribe Station)가 서비스를 제공받는 BS(Base Station)를 옮겨갈 경우 인증 및 키 교환을 위한 기존의 프로토콜을 분석하였다.

ABSTRACT

Portable Internet extended from wireless LAN has a large cell size, similar to a wireless mobile communication, and can provides the seamless service which offers middle-low speed mobility. IEEE 802.16e, the international standard of Portable Internet, uses PKMv2(Privacy Key Management) protocol for authorization and key exchange between a MSS(Mobile Subscriber Station) and a BS(Base Station). This paper first reviews and studies overall security architecture of TTA HPi standard and IEEE 802.16e which supports mobility based on WMAN(Wireless Metropolitan Area Network) standard(IEEE 802.16)

키워드

Portable Internet, Authentication protocol, Fast soft handover, IEEE 802.16e, PKMv2

Ⅰ. 서 론

국내 초고속 인터넷 및 이동통신 시장의 한계에 도달함에 따라서 경쟁력 있는 무선 인터넷 제공을 위한 솔루션의 하나로 2.3GHz 대역의 주파수를 이용한 휴대인터넷이 주목받고 있다. 휴대인터넷은 무선랜과 이동통신 기반 무선인터넷의 중간에 위치해, 두 서비스의 장점을 고루 갖춘 서비스로서 휴대용 무선 단말기를 이용하여 언제, 어디서나 정지 및 중저속 이동 상태에서 고속 전송속도로 인터넷에 접속하여 다양한 정보와 컨텐츠를 얻거나 활용할 수 있는 서비스를 의미한다[10].

국내에서는 2004년 6월말에 TTA에서 휴대인터넷 국내표준[7,8,9]을 정했으며, 휴대인터넷 국내표준은 대부분 IEEE 802.16e[3]를 기반으로 하고 있으며, 국내 기술을 국제 표준으로 만들기 위해서 노력하고 있다.

휴대인터넷에서는 이동성이 매우 중요한 요소가 된다. 따라서 인접한 기지국간의 소프트 핸드오버 및 Mobile IPv6 기술을 이용한 네트워크의 이동에 따른 핸드오버 등 이동성에 관한 여러 연구가 진행 중이다. 이들 연구의 대부분은 빠르게 핸드오버를 지원하기 위한 프로토콜에 대한 연구로서, Mobile IPv6와 AAA 서버와의 연동을 위한 인증 프로토콜에 관한 연구가 활발히 진행 중이다.

본 연구에서는 먼저, WMAN(Wireless Metropolitan Area Network) 표준인 IEEE 802.16 표준을 기반으로 이동성을 지원하는 IEEE 802.16e 표준과 TTA 휴대인터넷 표준을 바탕으로

휴대인터넷의 전체 보안구조를 파악하였다. 그리고 MSS(Mobile Subscribe Station)가 서비스를 제공받는 BS(Base Station)를 옮겨갈 경우 인증 및 키 교환을 위한 기존의 프로토콜을 분석하였다.

본 논문 II에서 휴대인터넷 시스템 구조 및 서비스 절차에 대해서 살펴보고, III장에서 IEEE 802.16e 표준에서 정의하고 있는 MSS와 BS간의 권한인증 및 키 교환 프로토콜인 PKMv2에 대해서 분석하였으며, 마지막으로 IV장에서 결론을 맺는다.

II. 시스템 구조 및 서비스 절차

2.1 시스템 구조

휴대인터넷 시스템의 구조는 그림 1과 같이 MSS(Mobile Subscriber Station), BS(Base Station), PAR(Packet Access Router)과 PAR들을 연결하는 백본(Backbone)망으로 구성된다. 백본망은 AAA(Authorization, Authentication and Accounting) 서버, HA(Home Agent) 서버, 관리 서버와 다른 특정 목적을 위한 서버들을 포함할 수 있다. MSS, BS, PAR과 백본망과의 상호 동작은 제어 메시지들이 정의하는 방식에 의해 구체화 된다[12,13].

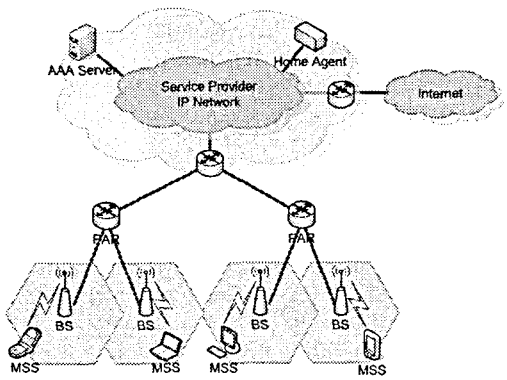

그림 1. 휴대인터넷 시스템 구성도

2.2 서비스 과정

휴대인터넷 서비스를 받기 위해서는 먼저 망 접속 절차를 거쳐야 한다. 망 접속 절차는 초기접속 과정(initial access)과 기본 제공능력 협상 과정(basic capability negotiation), 사용자 또는 터미널 인증 과정(authentication), 등록 과정(registration)으로 구성된다. 망 접속 절차가 끝나면 서비스가 시작되고, 서비스 중에 트래픽 상황에 따른 트래픽 플로우의 변경이나 삭제, 다른 셀로의 이동 시의 핸드오버와 그에 따라 발생되는 IP의 관리 및 과금 등이 일어난다. 서비스가 끝나면, 등록해제 과정을 거쳐 해당 MSS의 자원 점유가 해제된다[11].

그림 2는 휴대인터넷에서 전체 서비스가 이루어지는 과정을 나타낸 것이다.

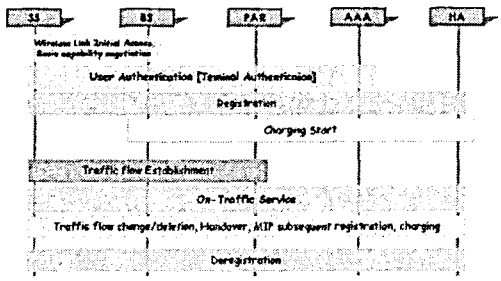

그림 2. 휴대인터넷 서비스 절차

III. 무선 구간 권한인증 및 키 교환

휴대인터넷 보안 구조는 첫 번째로 AAA 서버를 통해서 사용자 및 터미널의 인증과 서비스 권한 설정, 과금에 관한 처리 과정, 두 번째로 인증된 MSS와 BS간의 PKMv2 프로토콜을 사용한 무선 구간의 권한인증 및 키 교환 과정, 세 번째로 인증 과정의 결과로 분배된 AK(Authorization Key)로부터 유도한 TEK(Traffic Encryption Key) 교환 절차를 마치고 무선 구간의 데이터를 암호화하는 과정으로 나눌 수 있다[13]. 이번 장에서는 무선 구간에서의 사용자 인증과 키 교환 프로토콜에 대해서 살펴본다.

3.1 표기

o CertManufacture(SS) : 휴대인터넷 접속을 위한 MSS 장비 제조사 인증서.
o SS-R(SS-Random)/BS-R(BS-Random) : MSS/BS가 난수 생성기를 사용하여 생성한 예측 불가능한 임의의 값.
o CertSS : MSS의 인증서, CertManufacture(SS)에 의해 서명되어진 인증서.
o SecCap(Security Capabilities) : MSS가 제공하는 암호화 슈트.
o : BS가 난수 생성기를 사용하여 생성한 예측 불가능한 임의의 값.
o pSAID(primary SAID) : MSS와 BS 사이의 기본 연결 식별자.
o EncSS_pk(msg) : MSS의 공개키(SS_pk)를 사용하여 RSA 알고리즘을 통해서 메시지 msg를 암호화.
o SAID-list : 보안 협상(SA, Security Association)를 위한 값의 배열로써 SAID, SA 타입, SA 암호화 슈트를 포함.
o AK-sNo(sequence Number) : AK의 순차 번호, AK가 갱신될 때 마다 1씩 증가. 12-bit.
o AK-lt(lifetime, 생명주기) : AK가 만료될 시간. 32-bit.
o pre-AK : BS가 생성한 랜덤한 값으로 AK를 생

성하기 위한 기본 key로써 사용.
o CertBS : BS의 인증서.
o SigBS_sk( ) : BS의 개인키로 메시지를 공개키 서명 알고리즘을 사용해서 서명한 값.
o SAID : MSS와 BS 사이의 보안상으로 안전한 링크의 기본 식별자.
o HMAC( ), OMAC( ) : SHA1을 사용하여 계산한 메시지 무결성 검증 값.
o EncKEK(msg) : KEK(Key Encryption Key)를 사용하여 대칭키 알고리즘인 3DES나 AES-ECB로 msg를 암호화.
o SS-HMAC-Addr/ BS-HMAC-Addr : MSS/BS의 MAC 주소값.

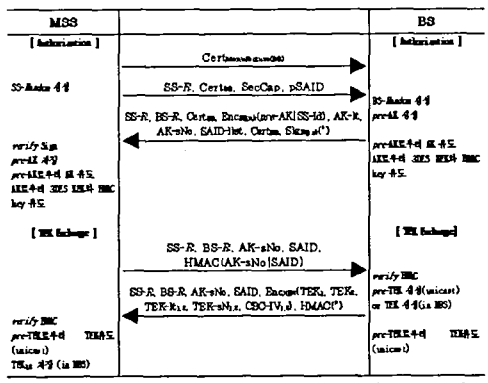

그림 3. PKMv2 권한인증 및 키 교환 프로토콜

[권한인증(Authorization) 과정]

① MSS → BS : 인증 정보

MSS가 신뢰할 수 있는 장치인지 확인할 수 있도록 MSS 제조사의 인증서를 보낸다. $Cert_{Manufacture(SS)}$를 수신한 BS는 해당 인증서를 검증한다. 상위 인증서인 $Cert_{Manufacture(SS)}$는 하위인증서인 $Cert_{SS}$의 검증에 사용된다.

② MSS → BS : 권한인증 요청

MSS의 X.509 인증서 $Cert_{SS}$, 암호화 제공능력인 Security Capability, BS와의 연결을 구분하기위한 primary SAID, Replay Attack의 방지와 다른 세션과 동일한 AK의 생성을 방지하기 위한 MSS의 SS-*Random*을 포함해서 권한인증 요청 메시지를 전송한다.

③ BS → MSS : 권한인증 응답

권한인증 요청 메시지를 수신하고 BS는 MSS의 X.509 인증서에 포함된 공개키를 사용해서 난수 생성기[4]로 부터 생성한 *pre*-AK와 SS-Id를 암호화한다. BS는 권한인증 응답 메시지에 MSS가 생성한 랜덤 값과 자신이 생성한 랜덤 값, SS의 X.509 인증서, RSA 공개키 알고리즘[5]으로 pre-AK를 암호화한 EncSS_pk(pre-AK|SS-Id), SS-Id, AK 파라미터, 보안 협상을 위한 SAID, SA 타입, SA 암호화 슈트를 포함하는 SAID-list를 포함한다. 마지막으로 전체 메시지를 BS의 개인키로 서명한 값을 메시지에 첨부하여 MSS에게 전송한다.

권한인증 과정을 성공적으로 마칠 경우,MSS와 BS는 아래의 키 유도 함수를 통해서 AK를 공유하게 된다.

AK = HMAC-SHA1(*pre*-AK, SS-*R* | BS-*R* | SS-MAC-Addr | BS-MAC-Addr | 160)

[암호화 키 교환(TEK Exchange)과정]

TEK 교환과정을 통해서 MSS와 BS는 data SA(보안협상)를 만들고 트래픽 암호화 키(TEK)와 MAC 키는 각각 트래픽의 기밀성과 무결성을 제공하기 위해 사용된다.

④ BS → MSS, MSS → BS : 키 요청 (상향/하향 채널별)

BS가 MSS에게 보내는 키 요청 메시지는 선택적으로 전송된다. 키 요청 메시지에는 SA를 위한 파라미터를 요청한다. MSS는 이전 권한인증 프로토콜을 통해서 전송된 SAID list중 하나의 SAID를 선택하여 보내야 한다. 메시지의 변조를 막기 위해서 HMAC() 함수[6]를 사용한다.

⑤ BS → MSS : 키 응답

BS는 AK로부터 유도한 3DES KEK(Key Encryption Key)를 사용하여 TEK(Traffic Encryption Key)를 암호화 하여 전송한다. TEK_1과 TEK_2는 TEK의 전체 생명주기의 1/2씩 사용하게 된다. 키 응답 메시지의 무결성을 확인하기 위해서 AK Sequence Number와 SAID를 AK로부터 유도한 HMAC Key를 사용하여 메시지 인증 값을 포함하여 전송한다.

암호화 키 교환과정을 성공적으로 마칠 경우, MSS와 BS는 아래의 키 유도 함수를 통해서 TEK를 공유하게 된다. MBS(Multicast Broadcast System)의 경우, BS는 셀 안에 있는 모든 MSS(Group member)에게 동일한 TEK를 암호화해서 전송하게 되고, unicast의 경우만 아래와 같이 TEK를 유도하게 된다.

TEK = HMAC-SHA1(*pre*-TEK, SS-*R* | BS-*R* | SS-MAC-*Addr* | BS-MAC-*Addr* | seqNo | 160)

IV. 결 론

휴대인터넷은 기존의 무선랜을 확장하여 이동통신처럼 셀 크기가 크고 중저속의 이동성을 지원하면서 이음매 없는 서비스를 제공할 수 있는 구조를 갖고 있다. 인접한 기지국으로 셀 스위칭이 발생하게 되는 소프트 핸드오버를 위한 인증은 빠르고 안전하게 단말기를 인증해야 한다. TTA 휴대인터넷 표준이나 IEEE 802.16e에서는 소프트 핸드오버를 위한 인증 프로토콜을 명확하게 정의하고 있지 않다. 본 논문에서는 IEEE 802.16e의 이동단말과 기지국간의 권한인증을 위한 PKMv2 프로토콜을 바탕으로 셀 스위칭이 발생할 경

우 권한인증 및 키 교환을 빠르게 수행할 수 있는 프로토콜을 제안하였다.

제안한 빠른 소프트 핸드오버를 위한 권한인증 및 키 교환 프로토콜은 무선 구간에서 전송되는 통신량을 크게 줄였으며, 무선 구간에서 전달되는 공개키 암호화 및 서명을 줄임으로써 권한인증에 소요되는 시간을 감소시킬 수 있다. 또한 무선 구간에서 수행했던 인증서 검증을 이웃한 기지국간 주기적으로 수행함으로써 소프트 핸드오버가 발생할 경우 인증서 검증에 소요되는 시간을 줄였다.

뿐만 아니라, 외부 공격자에 대해서 기존의 프로토콜과 동일한 안전성을 제공하며, 단말과 새로운 기지국간 상호인증을 제공하고 외부 공격자에 대해서 수동적 공격에 대해서 안전성을 보장하며, MSS 가장공격 및 BS 가장공격에 대해서 안전하다. 다만, 단말이 소프트 핸드오버를 통해서 이웃한 기지국으로 이동하게 될 경우 내부 공격자(현재의 BS)의 가장공격에 취약점이 있다는 단점이 있다.

휴대인터넷의 경우 중저속의 이동성을 지원하기 때문에 소프트 핸드오버가 발생할 경우 이음매 없는 서비스를 제공해야만 사용자가 불편함을 느끼지 못할 것이다. 특히, 사용자가 중첩된 기지국의 셀 영역에 위치할 경우 제안한 프로토콜을 통해서 핸드오버 프로시저의 수행 후 인증 및 키 교환에 소요되는 시간을 줄여줌으로써 휴대인터넷 사용자에게 효율적이고 안정적인 이동 서비스를 제공해 줄 것으로 기대된다.

참 고 문 헌

[1] IEEE Std 802.16d/Draft5, "Draft IEEE Standard for Local and Metropolitan Area Networks - Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems.", *IEEE 802.16 Draft*, 2004.05.

[2] IEEE Std 802.16e/Draft5, "Draft IEEE Standard for Local and Metropolitan Area Networks - Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems.", *IEEE 802.16 Draft*, 2004.09.

[3] D. Johnston, J. Walker, "Overview of IEEE 802.16 Security", *IEEE Computer Society*, 2004.05.

[4] D. Eastlake 3rd, S. Crocker, J. Schiller, "Randomness Recommendations for Security", *IETF RFC1750*, 1994.12.

[5] RSA Cryptography Standard, "RSA Public Key Cryptography Standard #1 v. 2.0", *RSA Laboratories*, 1998.10.

[6] H. Krawczyk, M. Bellare, R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", *IETF RFC2104*, 1997.02.

[7] TTA 표준, "2.3GHz 휴대인터넷 표준, 매체접근제어 계층", *TTAS_KO-06_0065*, 2004.06.25.

[8] TTA 표준, "2.3GHz 휴대인터넷 서비스 및 네트워크 요구사항", *TTAR-0017*, 2004.08.10.

[9] TTA 표준, "2.3GHz 휴대인터넷 네트워크 참조모델", *TTAR-0018*, 2004.08.10.

[10] 송석일, 김영일, 김영진, "초고속 휴대용 인터넷 기술", *전자통신 동향분석 제18권 제6호*, 2003.12.

[11] 양정록, 김영일, 안지환, "휴대인터넷 기술동향", *SK TR 제14권 1호*, 2004.02.

[12] 강충구, "휴대인터넷 서비스 및 네트워크", *TTA 저널 93호*, 2004.06.

[13] 추연성, 이동훈, 류대현 외 3명, "휴대인터넷에서 사용자 인증 및 키 교환 프로토콜", *WISC 2004*, pp. 675-691, 2004.09.

[14] 박재홍, "Mobile IP 적용 기술", *SK TR 제14권 5호*, pp. 767-774, 2004.10