휴대인터넷에서 고속 소프트 핸드오버를 위한 인증 프로토콜

류대현* · 최태완**

An Authentication Protocol for Fast Soft Handover in Portable Internet

Daehyun Ryu* · Taewan Choi**

이 논문은 2006년도 국립 진주산업대학교 애로기술개발과제의 지원에 의해 연구되었음

요 약

무선랜을 확장한 휴대인터넷은 그 셀 크기가 이동통신처럼 크고 중저속의 이동성을 지원하면서 연속적인 서비스를 제공할 수 있다. 휴대인터넷 국제 표준인 IEEE 802.16e에서는 단말과 기지국간 권한인증 및 키 교환을 위해서 PKMv2 프로토콜을 사용하고 있다. 본 논문에서는 단말의 이동에 따른 소프트 핸드오버가 발생할 경우 새로운 기지국과의 인증을 빠르게 수행할 수 있는 새로운 프로토콜을 제안한다. 기존의 소프트 핸드오버를 위한 권한인증 프로토콜에 비해 제안한 프로토콜은 무선구간의 메시지와 파라미터의 교환 횟수와 공개키 암호화와 서명 횟수 등을 줄임으로써 소프트 핸드오버 시 권한인증을 보다 효율적으로 수행할 수 있다. 또한, 외부 공격자의 도청을 방지하고 단말과 기지국의 가장공격에 대해서 안전성을 보장한다.

ABSTRACT

Portable Internet extended from wireless LAN has a large cell size, similar to a wireless mobile communication, and can provide the seamless service which offers middle-low speed mobility. IEEE 802.16e, the international standard of Portable Internet, uses PKMv2 protocol for authorization and key exchange between a MSS and a BS. This paper proposes a new protocol based on PKMv2, which can provide that MSS is able to do fast authorization with a new BS when soft handover is occurred in a MSS. Our protocol can carry out fast authorization because of reducing the number of messages and parameter exchange, public key encryption and signature in wireless network more than the previous works. It also prevents eavesdropping from an external attacker and keeps the security against impersonation attacks for both a MSS and a BS.

키워드

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

* 한세대학교 IT학부

** 진주산업대학교 메카트로닉스공학과

접수일자 : 2006. 5. 30

Ⅰ. 서 론

최근 국내에서는 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 있으며, 두 서비스의 장점을 고루 갖춘 서비스로써 휴대용 무선 단말기를 이용하여 언제, 어디서나 정지 및 중저속 이동 상태에서 고속 전송속도로 인터넷에 접속하여 다양한 정보와 컨텐츠를 얻거나 활용할 수 있는 서비스를 의미한다[1].

휴대인터넷의 국내 표준은 2004년 6월말에 TTA에서 정해졌고[2-4], 대부분 IEEE 802.16e[5]를 기반으로 하고 있으며, 국내 기술을 국제 표준으로 만들기 위해서 계속 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 연구로써 Mobile IPv6와 AAA(Authorization, Authentication and Accounting) 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 분석하고, 소프트 핸드오버 시 MSS가 계산해야 하는 연산량과 무선구간에서 전달해야하는 통신량을 최소화함으로써 빠른 소프트 핸드오버를 수행할 수 있는 인증 프로토콜을 제안하였다. 특히, 단말이 중첩된 기지국 셀 영역에 속하게 될 경우 잦은 셀 스위칭 및 재 인증으로 인한 지연 상황이 발생하게 되는데, 제안한 프로토콜은 이러한 환경에 적합하게 이용될 수 있는 장점이 있다.

본 논문은 2장에서 휴대인터넷 시스템 구조 및 서비스 절차에 대해서 살펴보고, 3장에서 IEEE 802.16e 표준에서 정의하고 있는 MSS와 BS간의 권한인증 및 키 교환 프로토콜인 PKMv2에 대해서 분석하며, 4장에서 MSS가 BS를 옮겨갈 경우, 빠른 소프트 핸드오버를 지원하기 위한 인증 프로토콜을 제안하고, 마지막으로 5장에서 결론을 맺는다.

Ⅱ. 시스템 구조 및 서비스 절차

2.1. 시스템 구조

휴대인터넷 시스템의 구조는 그림 1과 같이 MSS, BS, PAR(Packet Access Router)과 PAR들을 연결하는 백본(Backbone)망으로 구성된다. 백본망은 AAA 서버, HA(Home Agent) 서버, 관리 서버와 다른 특정 목적을 위한 서버들이 포함될 수 있다. MSS, BS, PAR과 백본망간의 상호 동작은 제어 메시지들이 정의하는 방식에 의해 구체화 된다[6,7].

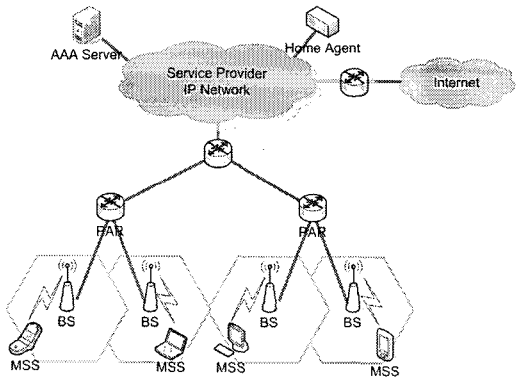

그림 1. 휴대인터넷 시스템 구성도
Fig. 1. System configuration diagram of portable Internet

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 플로우(flow)의 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[8]. 그림 2는 휴대인터넷에서 전체 서비스가 이루어지는 과정을 나타낸 것이다.

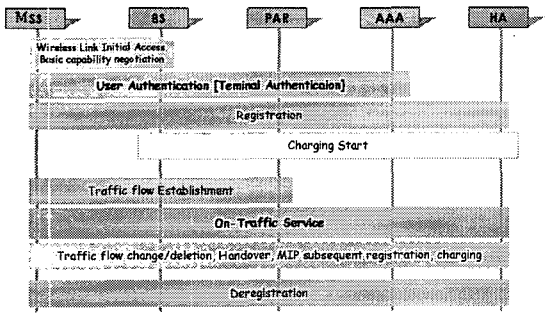

그림 2. 휴대인터넷 서비스 절차
Fig. 2. Service process of portable Internet

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 암호화 하는 과정으로 나눌 수 있다[7]. 이 장에서는 무선 구간에서의 사용자 인증과 키 교환 프로토콜에 대해서 살펴본다.

3.1. 표기

- CertManufacture(SS): 휴대인터넷 접속을 위한 MSS 장비 제조사 인증서.
- SS-R(SS-*Random*)/BS-R(BS-*Random*): MSS/BS가 난수 생성기를 사용하여 생성한 예측 불가능한 임의의 값.
- $Cert_{SS}$: MSS의 인증서, $Cert_{Manufacture(SS)}$에 의해 서명되어진 인증서.
- SecCap(Security Capabilities): MSS가 제공하는 암호화 슈트.
- pSAID(primary SAID): MSS와 BS 사이의 기본 연결 식별자.
- $Enc_{SS\_pk}(msg)$: MSS의 공개키(SS_pk)를 사용하여 RSA 알고리즘을 통해서 메시지 msg를 암호화.
- SAID-list: 보안 협상(SA: Security Association)을 위한 값의 배열로써 SAID, SA 타입, SA 암호화 슈트를 포함.
- AK-sNo(sequence Number) : AK의 순차 번호, AK가 갱신될 때 마다 1씩 증가. 12-bit.
- AK-lt(*lifetime*, 생명주기): AK가 만료될 시간. 32-bit.
- *pre*-AK: BS가 생성한 랜덤한 값으로 AK를 생성하기 위한 기본 key로써 사용.
- $Cert_{BS}$: BS의 인증서.
- $Sig_{BS\_sk}( )$: BS의 개인키로 메시지를 공개키 서명 알고리즘을 사용해서 서명한 값.
- SAID: MSS와 BS 사이의 보안상으로 안전한 링크의 기본 식별자.
- HMAC( ), OMAC( ): SHA1을 사용하여 계산한 메시지 무결성 검증 값.
- $Enc_{KEK}(msg)$: KEK(Key Encryption Key)를 사용하여 대칭키 알고리즘인 3DES나 AES-ECB로 msg를 암호화.
- SS-HMAC-*Addr*/ BS-HMAC-*Addr*: MSS/BS의 MAC 주소값.

3.2. PKMv2 권한인증 및 키 교환 프로토콜

PKMv2 권한인증 및 키 교환 프로토콜의 수행 절차는 그림 3과 같다. PKMv2 프로토콜은 권한인증을 위한 Authorization 절차와 키 교환을 위한 TEK Exchange 절차로 크게 구분할 수 있다[5,9,10].

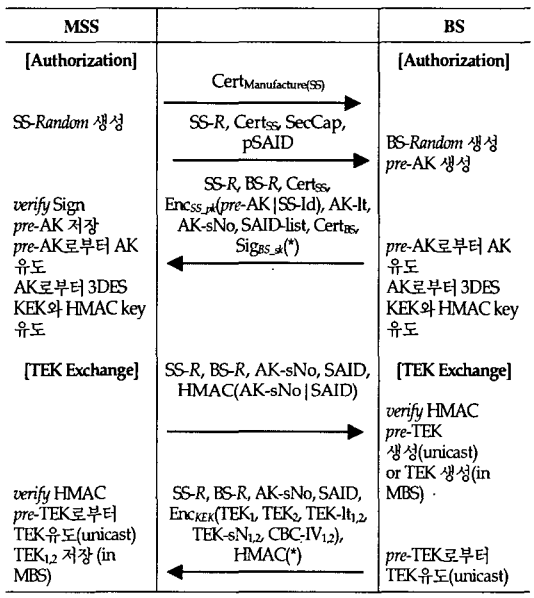

그림 3. PKMv2 권한인증 및 키 교환 프로토콜
Fig. 3. PKMv2 Authorization and TEK Exchange protocol

[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 구분하기 위한 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[11]로부터 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[12]으로 *pre*-AK를 암호화한 Enc_{SS_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(Traffic Encryption Key) 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[13]를 사용한다.

⑤ BS → MSS: 키 응답

BS는 AK로부터 유도한 3DES KEK(Key Encryption Key)를 사용하여 TEK를 암호화하여 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. 빠른 소프트 핸드오버를 위한 인증 프로토콜

4.1. 소프트 핸드오버

핸드오버란 셀 내에서 섹터 간에 이동을 하거나 한 셀에서 다른 셀로 이동해 갈 때 현재의 통화 채널을 자동적으로 전환해 주는 것을 말한다. 핸드오버를 위해서는 무선 레벨의 핸드오버 뿐만 아니라 네트워크 레벨의 핸드오버가 이루어져야 한다. 무선 레벨의 핸드오버는 이전의 접속점에서 새로운 접속점으로 무선 링크를 전환하는 것을 말하고, 네트워크 레벨의 핸드오버는 무선 레벨의 핸드오버를 지원하기 위해서 셀 버퍼링 및 연결 경로를 새롭게 재설정해 주는 것을 말한다.

핸드오버는 실행 과정 동안 이용되는 링크의 수에 따라 하드 핸드오버와 소프트 핸드오버로 구분된다. 하드 핸드오버는 이전 기지국에서 새로운 기지국으로 단말기의 액세스 포인트를 전환시키는 동안 단말은 하나의 액세스 포인트와만 통신한다. 따라서 액세스 포인트를 변환하는 과정에서 링크 스위칭으로 인해 짧은 시간동안 전송 중단이 발생하게 된다. 이와 같은 전송 중단시간을 최소화하여 사용자가 핸드오버 발생을 감지하지 못하도록 하는 것을 이음매 없는 핸드오버라 한다. 소프트 핸드오버 시 단말은 셀 스위칭 과정 동안 이전의 기지국과 핸드오

버 가능한 새로운 기지국들로부터 동시에 신호를 수신한다. 이동 단말기가 두 개 이상의 기지국과 연결되어 있는 동안 단말기는 현재 기지국에서 제공하는 것보다 나은 품질을 제공하는 기지국으로 핸드오버를 수행한다.

소프트 핸드오버의 일반적인 절차[14]는 다음과 같다.

① Scan 단계: MSS 주변에 있는 BS들에 대한 정보를 얻는 단계이다. 본 단계에서 얻어지는 정보는 접속 가능한 BS들의 리스트 및 각 BS의 전파 세기를 포함한다.

② Join 단계: MSS가 접속 가능한 BS들 중의 하나를 서전에 정해진 원칙에 의해서 선택한 후, 선택된 BS와 물리적으로 동기화 시킨다.

③ Authentication 단계: MSS가 접속하고자 하는 BS로 권한인증을 요청하는 단계이다.

④ Connection 단계: MSS가 새로운 BS로 통신 채널의 연결을 요청하는 단계이다.

⑤ Receive 단계: 요청을 받은 BS는 가능하다면 BS간 프로토콜을 이용하여 이전 BS에서 필요한 정보를 얻고 MSS에게 소프트 핸드오버 갱신 메시지를 전달한다.

4.2. 기존의 소프트 핸드오버를 위한 인증 프로토콜[9]

기존의 소프트 핸드오버를 위한 인증 프로토콜은 그림 4와 같다. 핸드오버의 절차를 마치고 MSS는 BS_2와 권한인증 절차를 완료하면 BS_2가 생성한 *pre*-AK로부터 유도한 AK를 공유하게 되고, AK로부터 KEK와 HMAC 키를 유도하게 된다. 다음으로 무선 구간 암호화를 위한 TEK Exchange 절차를 통해서 TEK, CBC-IV, *lifetime*, AK seqNo 등을 함께 교환하게 된다.

이 인증 프로토콜의 단점은 MSS가 BS_1과 통신하던 중 BS_2로 핸드오버 시, BS_2와 핸드오버를 위한 절차의 수행을 마치고 BS_2와 다시 새롭게 권한인증 및 키 교환 절차를 수행해야 하는 것이다. 여러 BS 셀 영역이 중첩된 지역에서 잦은 셀 스위칭이 발생하는 경우 MSS는 RSA 공개키 암호 알고리즘으로 암호화된 *pre*-AK의 복호화와 서명 검증을 수행해야 하므로 시간지연을 야기시킬 수 있다. 따라서 소프트 핸드오버 시 인증 및 키 교환에 소요되는 시간을 최소화하여 통신 채널이 끊기는 것을 막아야 하는 환경에는 적합하지 않다.

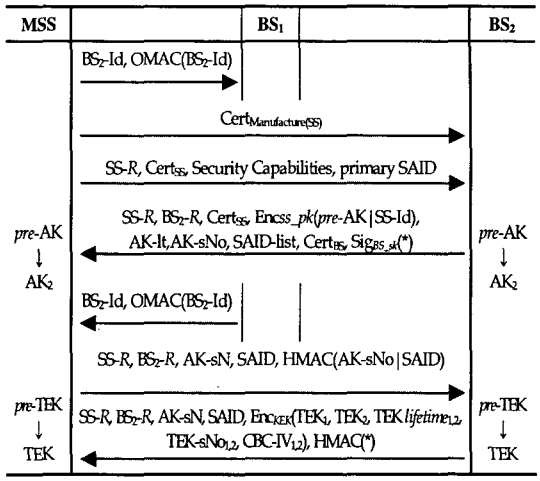

그림 4. 소프트 핸드오버를 위한 기본 인증 및 키 교환 프로토콜

Fig. 4. Basic authorization and TEK Exchange for soft handover

4.3. 빠른 소프트 핸드오버를 위한 인증 프로토콜

이 절에서는 기존의 소프트 핸드오버를 위한 권한인증 및 키 교환 프로토콜의 단점을 보완하여 효율적으로 권한인증 및 키 교환 절차를 수행할 수 있는 프로토콜을 제안한다. 제안하는 프로토콜은 기존의 권한인증 절차에서 MSS와 BS2와의 RSA 공개키 암호화·복호화 및 서명생성·검증으로 인한 오버헤드를 줄이기 위해서 MSS와 BS2 간의 인증을 BS1과 BS2와의 인증으로 대체함으로써 MSS가 수행해야 하는 공개키 암호 연산을 없애고, 또한 무선구간에서 MSS의 전송량을 줄임으로써 소프트 핸드오버 과정에서 인증 및 키 교환을 빠르게 수행할 수 있도록 하였다. 제안한 프로토콜은 IEEE 802.16e/D5[9]의 프로토콜 구조를 크게 변화시키지 않으면서 효율적으로 핸드오버를 수행할 수 있는 프로토콜을 설계하는데 중점을 두었다.

4.3.1 가정

PKI를 사용하는 무선 네트워크 사용자의 증가는 CRL 검색을 위해서 많은 시간이 소비되며, 인증에 필요한 시간 또한 증가하게 된다. 따라서 휴대인터넷에서는 MSS의 인증 시 CRL 검색에 소요되는 인증시간을 최대한 줄여야 한다. MSS의 소프트 핸드오버 시 MSS와 새로운 BS와의 메시지 전달횟수 줄이기 위해, 이것을 설치 과정에서 이미 인증을 수행한 BS간의 메시지 전달로 대체한다. BS와

비교해서 상대적으로 계산 능력이 떨어지는 MSS는 핸드오버 시 인증과정에서 생기는 부담을 최대한 줄임으로써 소프트 핸드오버에 드는 부담을 줄일 수 있다.

- BS는 설치 시 이웃하고 있는 BS들과 완전 인증을 통해서 상호인증 과정을 수행한다.

이 과정을 통해서 각 BS는 인접한 BS에 대한 정보와 공개키를 획득하고 이를 저장하게 된다. BS는 가입과 탈퇴가 빈번한 MSS와는 달리 구성의 변화가 자주 있지 않기 때문에 BS를 설치 시 주변의 BS들을 인식하는 과정에서 상호 인증을 수행하는 것이 MSS의 소프트 핸드오버 과정에서의 인증을 보다 효율적으로 제공할 수 있다. 각 BS간 CRL 검증도 BS의 설치 시 수행하게 되며 이후의 새로운 CRL에 등록되는 BS의 인증서의 경우는 AAA 서버에서 해당 BS의 주변 BS에게 통보하게 된다.

- BS간의 상호인증을 통해서 CRL 검색 과정을 생략한다.

MSS의 초기 인증 과정에서는 BS가 인증서와 CRL을 검색해야 하지만, 소프트 핸드오버 과정 중 인증에서는 각 BS간의 상호인증을 통해서 CRL 검색 과정을 생략하게 된다. 이때 생략된 CRL 검색 과정을 보완하기 위해서 AAA 서버는 OCSP를 통해서 MSS 인증서의 CRL 정보를 주기적으로 확인하고 CRL 변경사항이 생기면 해당 MSS에게 서비스를 제공하고 있는 BS에게 MSS의 인증 무효를 통보한다. 따라서 MSS의 소프트 핸드오버 시 인증과정에서 CRL 검색에 소요되는 시간만큼 MSS에게 빠른 소프트 핸드오버를 제공할 수 있다.

- 최소 AK *lifetime*을 사용하고 AK seqNo는 초기화한다.

AK *lifetime*은 IEEE 802.16e에서 1일~70일로 되어 있으며, 7일을 기본 값으로 사용하지만, 소프트 핸드오버를 위한 권한인증에서는 최소 AK *lifetime*인 1일을 사용한다. AK seqNo는 최초의 AK 설정 시와 마찬가지로 0으로 초기화한다. 그러므로 BS가 MSS에게 전송하는 권한인증 응답 메시지의 파라미터로 포함하지 않는다.

4.3.2 제안 프로토콜

소프트 핸드오버 절차를 수행하고 BS_1에서 BS_2로 셀 스위칭이 이루어지기 전에 MSS는 BS_2와 권한인증 및 키 교환을 수행해야 한다. 소프트 핸드오버 과정에서 MSS와 BS_2와의 인증을 빠르게 수행하기 위해서 그림 5와 같이 MSS와 BS_2는 PKMv2의 절차를 새롭게 수행하지 않는다. BS_1과 BS_2의 인증 결과를 통해서 MSS와 BS_2는 상호인증을 수행한다.

[권한인증(Authorization) 과정]

① MSS → BS_1: 권한인증 요청

MSS는 소프트 핸드오버 프로시저를 통해서 BS_1보다 나은 품질을 제공하는 BS를 결정하고 해당 BS로 권한인증을 요청한다.

② BS_1: AK_1로부터 *pre*-AK 유도

BS_1은 MSS와의 pairwise key인 AK로부터 *pre*-AK를 유도한다. *pre*-AK는 MSS와 BS_2가 공유하게 될 AK_2를 유도하는데 사용한다.

pre-AK = HMAC-SHA1(AK_1, SS-*R* | BS_1-*R* | SS-MAC-*Addr* | BS_1-MAC-*Addr* | 160)

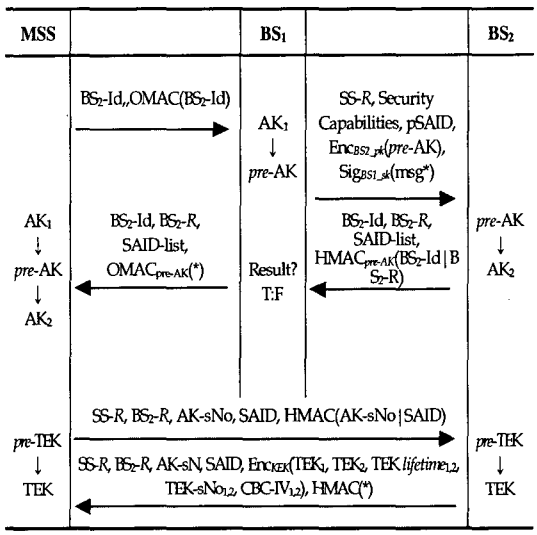

그림 5. 빠른 소프트 핸드오버를 위한 인증 및 키 교환 프로토콜

Fig. 5. Authorization and TEK Exchange for fast soft handover

③ BS_1 → BS_2: MSS 권한인증 요청

BS_1과 BS_2는 사전에 서로간의 인증서를 교환한 상태이며 주기적으로 CRL 검증을 수행하기 때문에 MSS가 BS_2의 셀 영역으로 이동하면, BS_1과 BS_2는 서로의 X.509

인증서를 교환하지 않는다. Replay Attack과 동일한 AK의 생성을 방지하기 위해서 MSS는 SS-*Random*을 포함해서 권한인증 요청 메시지를 전송한다. MSS의 암호화 제공능력인 Security Capability, BS_2와의 연결을 구분하기 위한 pSAID에 BS_1이 AK_1으로부터 유도한 *pre*-AK를 RSA 공개키 암호 암고리즘을 사용해서 BS_1의 개인키로 암호화하고 BS_2의 개인키를 사용하여 계산한 메시지 전체에 대한 서명 값을 첨부하여 보낸다.

④ $BS_2 \rightarrow BS_1$: MSS 권한인증 응답

BS_2는 MSS 권한인증 요청 메시지를 통해서 MSS의 권한인증을 검증한다. BS_2는 BS_1의 권한인증 요청으로부터 *pre*-AK를 복호화 함으로써 AK_2를 유도하기 위한 준비를 마친다. 응답 메시지에는 BS_2의 ID와 Replay Attack과 동일한 AK의 생성을 방지하기 위한 MSS의 SS-*Random*과 BS_2-*Random*을 포함하고, 응답 메시지 전체를 *pre*-AK를 키로 하는 HMAC을 계산하여 첨부함으로써 BS_2를 인증하기 위한 정보를 포함한다.

⑤ BS_1: BS_2 권한인증 확인

MSS 권한인증 응답 메시지로부터 BS_2의 ID와 SS-*Random* 값을 확인하고 HMAC을 계산함으로써 BS_1과 BS_2간 상호인증을 마친다. BS_1은 인증 결과에 따라서 권한인증 응답 메시지나 권한인증 거절 메시지를 전송하게 된다. 권한인증 거절 메시지는 BS_2-Id와 HMAC을 포함한다.

⑥ $BS_1 \rightarrow$ MSS: 권한인증 응답

BS_1은 BS_2의 BS_2-*Random*과 BS_2의 보안 협상을 위한 값인 SAID, SA 타입, SA 암호화 슈트를 포함하는 SAID-list와 메시지에 대한 무결성 검증을 위해서 *pre*-AK가 키인 HMAC을 계산하여 첨부한다.

권한인증 과정을 마치면 MSS와 BS_2는 아래의 키 유도 함수를 통해서 AK_2를 공유하게 된다.

AK_2 = HMAC-SHA1(*pre*-AK, SS-*R* | BS_2-*R* | SS-MAC-*Addr* | BS_2-MAC-*Addr* |160)

[암호화 키 교환(TEK Exchange) 과정]

TEK 교환 과정은 PKMv2 권한인증 프로토콜의 절차를 동일하게 수행한다. 이러한 TEK 교환과정으로 MSS와 BS_2는 data SA를 만들고 TEK와 MAC 키는 각각 트래픽의 기밀성과 무결성을 제공하기 위해 사용된다.

4.4. 효율성과 안전성

이 절에서는 기존 프로토콜과 제안한 프로토콜의 효율성과 안전성을 각각 분석한다. 제안한 프로토콜이 기존 프로토콜과 비교해서 Forward Secrecy에 대한 안전성은 약하지만, 소프트 핸드오버 발생 시 기존 프로토콜보다 훨씬 효율적으로 권한인증 및 키 교환을 수행할 수 있는 장점이 있다.

4.4.1 효율성 분석

빠른 핸드오버를 수행하기 위해서는 계산능력이 제한된 MSS의 계산량이 적어야 한다. 만약 MSS에서 수행해야 하는 연산량이 증가하면 MSS의 계산지연으로 인해서 소프트핸드오버가 늦어질 수 있다. 또한 BS간 유선구간에서 보다 MSS와 BS간 무선구간의 데이터전송 속도가 훨씬 느리기 때문에 무선구간에 전송되는 메시지의 횟수와 통신량 또한 적어야 한다. 만약 무선구간의 통신량이 증가하면 MSS가 처리해야 하는 데이터량이 많아지게 되므로 MSS의 데이터 처리 지연으로 인해 핸드오버 수행이 지연될 수 있다. 또한 유선에서보다 무선에서의 데이터 손실율이 더 높기 때문에 전송오류로 인한 지연이 증가할 수 있다.

제안한 프로토콜은 기존의 프로토콜의 단점을 보완하여 위에서 언급한 요구사항에 적합하게 설계되었다. 제안한 프로토콜은 MSS와 새로운 BS_2와의 직접적인 권한인증 대신에 MSS와 인증된 BS_1과 새로운 BS_2가 권한인증을 수행한다. 따라서 MSS와 BS_2와의 메시지 교환 횟수가 감소하였고 무선구간에서의 공개키 암호 알고리즘을 사용한 암호화 및 서명 계산을 제거하였다. BS간 인증에서는 인증서의 교환이 필요 없으며 인증서의 유효성 검사도 주기적으로 수행하게 되기 때문에 CRL 검증에 드는 시간을 줄일 수 있다. 결과적으로 MSS와 BS_2간 PKMv2를 사용해서 새롭게 권한인증을 수행할 때 보다 빠르게 권한인증을 수행할 수 있다.

기존의 PKMv2 사용해서 새롭게 권한인증을 수행하는 프로토콜과 제안한 프로토콜의 효율성을 전달 메시지(Msg) 수와 암호화(Enc-A:Asymmetric Encryption, S:Symmetric Encryption) 수, 공개키 서명(Sign), Hash 및 HMAC (Hash) 계산 수에 따른 비교를 표 1에 간단하게 정리하였다.

• 전체 메시지 전송은 유, 무선 구간 전체 7번의 전송에서 6번으로 줄였으며 특히, MSS와 BS_2간의 무선구간에 메시지 전송을 5번에서 2번으로 줄였다.

표 1. 기존 프로토콜과 효율성 비교
Table 1. Comparison of performance with previous protocol

구분 / 프로토콜	MSS–BS_1				BS_1–BS_2				MSS–BS_2			
	Msg	Enc (A/S)	Sign	Hash	Msg	Enc (A/S)	Sign	Hash	Msg	Enc (A/S)	Sign	Hash
기존 프로토콜	2	0/0	0	2	0	0/0	0	0	5	1/1	1	4
제안 프로토콜	2	0/0	0	2	2	1/0	1	1	2	0/1	0	2

• 암호화의 경우 기존 프로토콜은 MSS와 BS_2 사이에 RSA 공개키 암호를 사용하여 *pre*-AK를 전달하게 되므로 암·복호화에 많은 시간이 소요되는데 반해, 제안한 프로토콜에서는 RSA 공개키 암호를 BS_1과 BS_2간에 *pre*-AK의 전달을 위해서 사용하기 때문에 MSS보다 상대적으로 계산 능력이 뛰어난 BS에서 보다 빠르게 암·복호화를 수행할 수 있다.

• 기존 프로토콜은 BS_2의 인증을 위해서 서명 계산이 사용되었는데, 제안한 프로토콜에서는 BS_2의 인증을 위해서 서명 대신 공유하고 있는 *pre*-AK를 이용하여 HMAC을 계산하게 되고 이를 이용해 인증을 수행함으로써 계산에 소요되는 시간을 줄였다.

• Hash 및 HMAC의 계산의 경우 기존 프로토콜은 전체적으로 6번의 해쉬 및 HMAC의 계산이 필요하지만 제안한 프로토콜은 5번의 해쉬 및 HMAC의 계산만 필요하며 MSS와 BS_2간의 무선구간에서는 TEK 교환과정에서 필요한 2번의 HMAC 계산만 필요하다.

4.4.2 안전성 정의

암호 프로토콜의 안전성을 증명하기 위해서는 먼저 프로토콜이 어떠한 공격에 대해서 안전해야 하는지에 대한 공격유형을 정의하고, 프로토콜이 만족해야 하는 안전성을 정의하여야 한다. 공격 유형은 공격자의 능력에 따라 수동적 공격과 능동적 공격으로 나뉜다. 수동적 공격 유형에서 공격자는 단지 프로토콜에 참여하는 정당한 사용자들의 통신내용을 도청함으로써 공격을 수행하고, 능동적 공격 유형에서 공격자는 도청뿐만 아니라 전송되는 메시지를 위·변조, 삭제 하거나 새로운 메시지를 삽입하여 공격을 수행한다. 이 절에서는 일반적으로 키 교환 프로토콜에 요구되는 안전성을 정의한 후 기존의 프로토콜과 제안한 프로토콜이 정의된 안전성을 만족하는지 비교·분석한다.

정의 1. *Impersonation Attack*: 공격자가 정당한 사용자를 위장하여 프로토콜에 참여하여 상대방과 같은 키를 공유할 수 없을 때 가장공격에 안전하다고 한다.

정의 2. *Known-key Security*: 정당한 사용자 A와 B가 키 교환 프로토콜을 수행하여 공유한 세션키가 노출되었을 때, 그 세션 이외의 세션에서 A와 B가 공유한 세션키에 대한 정보를 얻을 수 없을 때 Known-key security를 만족한다고 한다.

정의 3. *Forward Secrecy*: 정당한 사용자 A와 B의 long-term 비밀키가 노출되었을 경우 그 비밀키로부터 이전에 A와 B가 공유한 세션키를 계산할 수 없을 때 Forward secrecy를 만족한다고 한다.

- *Half forward Secrecy*: 한 사용자의 long-term 비밀키만 노출되었을 경우 이전 세션키를 계산할 수 없을 때 Half forward secrecy를 만족한다고 한다.

4.4.3 안전성 비교·분석

본 논문에서는 공격자가 능동적 공격자이고, 공격자는 프로토콜의 구성원이 아니라고 가정한다. 제안한 프로토콜과 기존 프로토콜의 안전성은 표 2와 같다.

• Impersonation Attack에 대한 안전성

기존 프로토콜에서 MSS와 BS의 인증은 각각 RSA 공개키 시스템에 의해서 수행된다. 즉, 공격자가 BS로 가장하여 MSS와 세션키를 공유하려면 BS의 서명값을 위조해야 한다. 그리고 공격자가 MSS를 가장하여 BS와 세션키를 공유하려면 그림 4의 네 번째 플로우의 Enc_{SS_pk}(*pre*-AK | SS-Id)로부터 *pre*-AK를 계산해야 한다.

표 2. 기존 프로토콜과 안전성 비교
Table 2. Comparison of stability with previous protocol

공격유형 / 프로토콜	Impersonation Attack	Known-key Security	Forward Secrecy
기존 프로토콜	안전	안전	Half
제안 프로토콜	안전	안전	불안전

제안한 프로토콜에서 MSS가 BS_2로 핸드오버시 MSS에 대한 인증은 결국 BS_1을 통해서 이루어지기 때문에 공격자가 BS_2에게 MSS로 가장하여 키를 공유하려면 BS_1의 서명값을 위조해야 한다. 그리고 공격자가 BS_2로 가장하여 MSS와 세션키를 공유하려면 그림 5의 두 번째 플로우의 Enc_{BS2_pk}(*pre*-AK)로부터 *pre*-AK를 계산해야 한다. 제안한 프로토콜과 기존 프로토콜에서 Impersonation Attack에 대한 안전성은 모두 RSA 공개키 시스템에 기반한다.

- Known-key Security에 대한 안전성

기존 프로토콜과 제안한 프로토콜의 경우, 만약 어떤 세션의 세션키 TEK가 노출된다 하더라도 그 이외의 세션에 대한 세션키 값들은 계산할 수 없다. 다른 세션의 세션키값을 계산하려면 그 세션에 해당하는 *pre*-AK를 계산해야만 한다. 따라서 노출된 TEK만 이용해서 노출되지 않은 세션키를 계산하는 것은 불가능하다.

- Forward Secrecy에 대한 안전성

기존의 프로토콜과 제안한 프로토콜에서 MSS의 long-term 비밀키는 RSA 암호시스템의 비밀키 *SS_sk*이고, BS의 long-term 비밀키는 RSA 서명 시스템의 서명키 *BS_sk*이다. 기존의 프로토콜의 경우, 만약 MSS long-term 비밀키만 노출된다면 이전 세션의 메시지들을 저장하고 있는 공격자는 Enc*ss_pk*(pre-AK|SS-Id)로부터 이전 세션의 *pre*-AK를 계산할 수 있고, 이 값으로부터 이전 세션키 값을 유도할 수 있다. 만약 BS long-term 비밀키만 노출된다면 이전 세션의 메시지들을 저장하고 있는 공격자라 할지라도 이전 세션의 *pre*-AK를 계산할 수 없으므로 결국 세션키 값을 계산할 수 없다. 따라서 기존 프로토콜은 Half forward secrecy를 만족한다.

제안한 프로토콜의 경우, 만약 MSS long-term 비밀키만 노출된다면 MSS가 BS와 처음 키 교환을 수행할 때의 세션에 대한 메시지들을 저장하고 있는 공격자는 Enc*ss_pk*(*pre*-AK | SS-Id)로부터 처음 세션의 *pre*-AK를 계산할 수 있고, 이 값으로부터 세션키 값을 유도할 수 있다. 만약 BS long-term 비밀키만 노출된다면 이전 세션의 메시지들을 저장하고 있는 공격자는 이전 세션의 *pre*-AK를 계산할 수 있고, 이 값으로부터 이전 세션키 값을 유도할 수 있다. 따라서 제안한 프로토콜은 Forward Secrecy를 만족하지 않는다.

***Remark*:** 기존 프로토콜의 경우, 수동적 공격자에 대해서 MSS와 BS2간에 공유되는 pre-AK의 기밀성에 대한 안전성은 RSA 암호 알고리즘의 안전성에 기반한다. 제안한 프로토콜의 경우, MSS와 BS2간의 pre-AK는 MSS와 BS1간의 AK1으로부터 유도된다. 즉, MSS와 BS2간의 권한인증 과정에서 BS2가 생성해야 하는 pre-AK는 MSS와 BS1과의 AK1으로부터 BS1이 HMAC-SHA1() 함수를 통해서 유도한다. 이때 MSS는 BS1 및 BS2와 서로 다른 AK를 공유하게 된다. 그러므로 제안 프로토콜에서 수동적 공격자 대한 pre-AK의 안전성은 해쉬함수의 안전성에 기반한다.

V. 결 론

휴대인터넷은 기존의 무선랜을 확장하여 이동통신처럼 셀 크기가 크고 중저속의 이동성을 지원하면서 이음매 없는 서비스를 제공할 수 있는 구조를 가지고 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 경우 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 취약하다는 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.

참고문헌

[1] 송석일, 김영일, 김영진, "초고속 휴대용 인터넷 기술," *전자통신 동향분석*, 제18권 제6호, Dec. 2003.

[2] TTA 표준, '2.3GHz 휴대인터넷 표준, 매체접근제어계층', *TTAS_KO*-06_0065, 2004.06.25.

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

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

[5] D. Johnston, J. Walker, 'Overview of IEEE 802.16 Security', *IEEE Computer Society*, Jun 2004.

[6] 강충구, "휴대인터넷 서비스 및 네트워크," *TTA 저널*, 93호, Jun 2004.

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

[8] 양정록, 김영일, 안지환, "휴대인터넷 기술동향," *SK TR*, 제14권 1호, Feb. 2004.

[9] 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, Jun 2004.

[10] 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, Sep. 2004.

[11] D. Eastlake 3rd, S. Crocker, J. Schiller, 'Randomness Recommendations for Security', *IETF* RFC1750, Dec. 1994.

[12] RSA Cryptography Standard, 'RSA Public Key Cryptography Standard #1 v. 2.0', RSA Laboratories, Oct. 1998.

[13] H. Krawczyk, M. Bellare, R. Canetti, 'HMAC: Keyed-Hashing for Message Authentication', *IETF* RFC2104, Feb. 1997.

[14] 박재홍, "Mobile IP 적용 기술," *SK TR*, 제14권 5호, pp. 767-774, Oct. 2004.

저자소개

류 대 현(Daehyun Ryu)

1997년 부산대학교 전자공학과 (공학박사)
1985년 부산대학교 전자공학과 (공학석사)
1983년 부산대학교 전기기계공학과 (공학사)
1987년 2월~1998년 2월 한국전자통신연구원 선임연구원
1998년 3월~현재 한세대학교 IT학부 부교수
※관심분야 : 정보보호, 컴퓨터비젼 및 영상처리, 유비쿼터스 컴퓨팅 등

최 태 완(Taewan Choi)

1996년 부산대학교 전자공학과 (공학박사)
1985년 부산대학교 전자공학과 (공학석사)
1983년 동아대학교 전자공학과(공학사)
1984년 12월~1991년 2월 (주)LG전자 디지털어플라이언스 연구소 선임연구원
1991년 3월~1993년 2월 부산대학교 전자공학과 조교
1993년 3월~1997년 2월 부산대학교 전자공학과 시간강사
1996년 3월~1997년 2월 (주)하나정보기술 부설연구소 기술이사
1997년 3월~현재 국립 진주산업대학교 메카트로닉스 공학과 부교수
※관심분야 : 컴퓨터비젼 및 영상처리, 신경회로망, 패턴인식 등