# IEEE 802.16e/와이브로 망에서의 안전한 핸드오버 적용 방안*

조혜숙†, 전웅렬, 김승주, 원동호‡
성균관대학교 정보통신공학부 정보보호연구소

# Secure Handover Scheme in IEEE 802.16e/WiBro Networks

Heasuk Jo†, Woongryul Jeon, Seungjoo Kim, Dongho Won‡
Information Security Group, School of Information and Communication Engineering, Sungkunkwan University.

**요 약**

현재 국내 국책사업으로 추진 중인 와이브로(WiBro) 기술 규격이 포함되어 있는 휴대인터넷 표준 규격인 IEEE 802.16e는 IP기반으로, 이동성이 뛰어나고 고속전송 기능의 특징을 가지고 있다. 또한 기지국간의 핸드오버(Handover)를 지원함으로써 이동성을 지원한다. 그러나 이러한 핸드오버 기법에 있어서 Replay 공격, Man-in-the-Middle 공격, Stolen-Verifier 공격 등에 취약한 문제점이 드러나고 있다. 본 논문은 이러한 기존 핸드오버 기법의 취약점을 개선하기 위해서 사용자의 인증서와 Timestamp값을 통한 IEEE 802.16e/와이브로 망에서 안전한 핸드오버 적용 방안에 대해 제안한다.

## I. 서론

휴대인터넷이란 이동하면서도 초고속 인터넷을 이용할 수 있는 휴대 무선 인터넷을 지칭하는 것으로, 국내에서는 정보통신부, 한국정보통신기술협회(TTA)와 이동통신 업체들이 중심이 되어 2006년부터 상용 서비스하고 있다[1]. 이와 같은 서비스를 제공하기 위해 IEEE 802.16을 비롯하여 많은 규격들이 제공되고 있으며 국내에서는 IEEE 802.16을 기반으로 와이브로(Wireless Broadband Internet, WiBro)가 규격화 되고 있다[2].

휴대인터넷의 고속 데이터 전송의 특성상 안전한 핸드오버(Handover)를 위한 방안들이 제안되고 있다. 특히 사용자와 사용자에게 서비스를 제공하는 Base Station(Serving Base Station, SBS)과 핸드오버 할 Base Station(Target Base Station, TBS)사이에서 재전송 공격(replay attack)이나 전송 도중에 중요한 정보를 빼앗길(man-in-the-middle attack) 수 있는 취약점이 제기되고 있다. 이런 문제를 해결하기 위해 사용자의 인증서를 이용하거나 Base Station의 공개키를 이용하여 암호화 하여 데이터를 송수신하여 안전성을 보장한다[3,4].

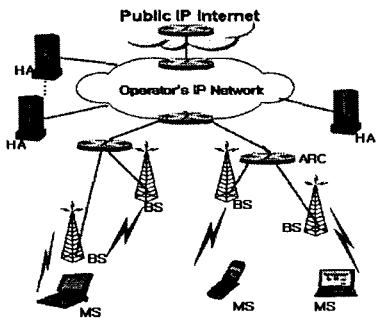


그림 1. WiBro Network 구조

† 주저자 : hsjo@security.re.kr
‡ 교신저자 : dhwon@security.re.kr
* 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터(ITRC) 육성·지원 사업의 연구 결과로 수행되었음.

본 논문에서는 기존 [3]의 핸드오버의 보안상 취약성으로 나타나는 도청 및 man-in-the-middle 공격을 개선하기 위해서 기존 Base Station에서 사용자를 인증하기 위해 사용했던 인증서를 사용함으로써 안전한 핸드오버 기법을 제안한다. 또, 제안기법은 Replay 공격이나 Stolen-Verifier 공격 등의 각종 공격으로부터 안전성을 지니면서, 보다 높은 효율을 가진다.

본 논문의 구성은 다음과 같다. 먼저, 2장에서는 기존에 제안된 기법에 대해서 알아보고 3장에서는 제안하는 IEEE 802.16e/와이브로 망에서의 핸드오버 기법에 대해 소개한다. 4장에서는 기존에 제안된 핸드오버 성능과 제시한 기법의 안전성과 성능을 분석하고, 5장에서는 논문의 결론에 대하여 기술한다.

## II. IEEE 802.16e의 인증 및 핸드오버 절차

이 장에서는 본 논문에서 사용할 용어들을 정의하고 IEEE 802.16e에서 Sen이 제안한 인증 및 핸드오버 절차에 대해 소개한다[3].

표 1. 용어정의

| 기 호 | 의 미 |
|---|---|
| SS | Subscriber Station |
| BS | Base Station |
| SBS | Serving Base Station |
| TBS | Target Base Station |
| BCID | Basic Connection ID |
| SAID | Security Association ID |
| AK | Authentication Key |
| SeqNo | AK의 일련번호 |
| Lifetime | AK의 사용기한 |

### 2.1 인증절차

우선 SS는 BS에게 인증을 요청하는 Message2를 보낸다. Message2에는 SS의 X.509 인증서가 포함되어 있다. BS는 SS로부터 받은 Message2를 통해 SS를 검증하고, 이후 SS와의 통신에서 사용할 암호 알고리즘과 프로토콜을 결정한 후, 여기에 사용할 비밀키 AK를 생성하여 SS에게 보낸다. 이러한 인증 절차는 아래와 같다.

Message 1. SS→BS : Cert(SS. Manufacturer)
Message 2. SS→BS : Cert(SS) | Capabilities | BCID
Message 3. BS→SS : $KU_{SS}$(AK) | SeqNo | Lifetime | SAIDList

Message 1에서 Cert(SS. Manufacturer)는 SS 기기에 대한 X.509 인증서를 의미한다. Capability는 SS가 지원하는 인증 및 암호 알고리즘을 나타내며, $KU_{SS}$는 SS의 공개키이다. $KU_{SS}$는 BS가 암호화 통신에 사용할 비밀키 AK를 SS에게 전달할 때 암호화 키로 사용된다.

### 2.2 핸드오버 절차

SBS로부터 TBS로의 Mobile Station(MSS)의 핸드오버 절차는 다음과 같다. 우선 SBS는 TBS에게 MSS의 핸드오버을 알린다. 이에 TBS는 SBS에게 응답을 하고, 응답을 받은 SBS는 MSS에게 핸드오버할 BS, 즉 TBS를 알려준다. 그러면 MSS는 TBS에게 인증을 요청하고 TBS는 MSS를 인증한 후 서로의 비밀키 new_AK를 나눠 갖고 SBS로부터의 핸드오버을 완료한다. 다음은 핸드오버 절차를 나타낸다.

Message 1. SBS→TBS: $T_1$, MSS, SK(MSS, $T_1$, RAK)
Message 2. TBS→SBS: $T_1$, $N_1$, SK($T_1$, $N_1$)
Message 3. SBS→MSS: $T_2$, $N_1$, Ready-to-Roam TBS, AK(TBS, RAK, $T_2$, $N_1$)
Message 4. MSS→TBS: $T_3$, $N_1$, Re-auth, RAK($R_3$, $N_1$)
Message 5. TBS→MSS: $T_3$, RAK(new-AK, $T_3$)

SK는 BS 간의 암호통신에 사용되는 Session Key이다. RAK는 Roaming AK이며 SBS와 MSS 사이의 AK로부터 도출된다. Tn과 $N_1$은 각각 Timestamp와 난수이다.

그러나 이 기법에서 SBS는 RAK를 알고 있기 때문에 TBS에서 MSS에게 전송하는 RAK(new-AK, $T_3$)을 악의적인 목적으로 복호화하여 추후 MSS와 TBS가 사용할 new_AK 키를

SBS가 획득할 수 있다는 취약성을 가진다.

## III. 안전한 핸드오버 방안 제안

본 논문에서 제안한 방법은 [3-5]의 핸드오버 방식과 유사하지만 SBS와 TBS 사이에 인증서를 발급하여 사용하는 것이 아니라 인증과정에서 이미 발급된 MS의 인증서를 사용하여 핸드오버를 수행한다. 그러므로 기존 [3]에서의 TBS가 MS에게 New_AK를 전송하는 과정에서 악의적인 SBS가 가지고 있던 RAK로 New_AK를 도청하는 것을 사전에 막을 수 있다. 다음은 핸드오버 시 보안 요구사항이다.

◆ 보안 요구사항

o 도청 공격에 안전해야 한다.

o 재전송 공격(replay attack)에 안전해야 한다.

o 중간자 공격(man-in-the-middle attack)에 안전해야 한다.

o Stolen-Verifier 공격에 안전해야 한다.

### 3.1 핸드오버 요청 단계

핸드오버 요청 단계는 빠른 핸드오버를 지원하기 위한 단계이다. 만약 TBS가 MS의 QoS를 지원해주지 못할 경우를 감안하여 Per_Auth를 사용한다. 다음은 핸드오버 요청 단계에 대한 설명이다.

**MS → SBS : HO_REQ, TBS_Info**
**SBS → TBS : HO_REQ**
**TBS → SBS : HO_RSP | QoS, Per_Auth**
**SBS → MS : HO_RSP | Per_Auth**

MS는 핸드오버 할 수 있는 TBS (TBS_Info)와 함께 핸드오버 요청 메시지(HO_REQ)를 SBS에게 전송한다. SBS는 다시 TBS에게 요청 메시지(HO_REQ)를 전송하고, 이를 수신한 TBS는 핸드오버 준비를 한다. 그리고 제공할 수 있는 QoS와 핸드오버 응답 메시지를 SBS에게 전송한다. SBS는 수신한 TBS의 QoS를 확인하고 MS에게 제공해야할 QoS와 비교하여 적합 또는 부적합 여부를 확인 후 MS에게 통보한다. 이때 Per_Auth는 TBS가 MS에게 적합한 QoS를 지원에 따른 과금 문제가 있기 때문에 본 논문에서는 적합, 부적합으로 나타낸다.

### 3.2 키 획득 단계

SBS에서 TBS의 QoS 적합 여부를 판단하고 적합할 경우 사전에 MS의 인증 절차에서 받은 인증서 Cert(MS)와 $T_i$, 그리고 무결성을 보장하기 위해 BS 간에 사전 공유하고 있는 비밀키를 이용하여 암호화 $E_{BS}$(Cert(MS), $T_i$)한 것을 TBS에게 전송한다. $T_i$는 SBS의 시간정보인 Timestamp 이다.

**SBS → TBS : $T_i$ | Cert(MS) | $E_{BS}$(Cert(MS), $T_i$)**
**TBS → SBS : $T_i$ | $N_i$ | $E_{PK_{MS}}$(HO_AK) | $E_{BS}$($T_i$ | $N_i$ | $E_{PK_{MS}}$(HO_AK))**
**SBS → MS : $T_{i+1}$ | $N_i$ | $E_{PK_{MS}}$(HO_AK) | Ready_TBS | AK($T_{i+1}$ | $N_i$ | $E_{PK_{MS}}$(HO_AK))**
**TBS → MS : UL_MAP, DL_MAP**
**MS → TBS : $T_{i+2}$ | $N_i$ | REQ_HO | HO_AK($T_{i+2}$ | $N_i$,)**
**MS → TBS : $T_{i+2}$ | HO_AK($T_{i+2}$ | New_AK)**

TBS는 받은 $T_i$의 유효성을 확인하고 TBS의 비밀키로 암호화된 데이터를 복호화하여 무결성 여부를 확인한다. 그리고 난수 $N_i$ 를 생성하고 MS 인증서의 공개키 $PK_{MS}$를 사용하여 핸드오버 인증키인 HO_AK(HandOver_Authentication Key)를 암호화 $E_{PK_{MS}}$(HO_AK) 한다. 생성한 값들과 TBS의 비밀키로 암호화한 $E_{BS}$($T_i$ | $N_i$ | $E_{PK_{MS}}$(HO_AK)) 데이터를 SBS에게 전송한다.

SBS는 수신한 $T_i$, $N_i$,의 유효성과 데이터를 복호화해서 그 무결성을 확인한다. 그리고 $T_{i+1}$, $N_i$, $E_{PK_{MS}}$(HO_AK), Ready_TBS와 인증키 AK로 열거한 데이터를 암호화 하여 MS에게 전송한다.

이렇게 준비된 상태에서 TBS는 데이터를 송수신 하기 위한 UP_Link 정보(UL_MAP)와, DOWN_Link 정보(DL_MAP)를 MS에게 전송한다.

MS는 개인키로 $E_{PK_{MS}}$(HO_AK)를 복호화하여

HO_AK를 얻는다. 그리고 TBS와 새로운 AK (New_AK)를 공유하기 위해, 요청 메시지 HO_REQ와 $T_{i+2}$, $N_i$ 를 HO_AK로 암호화 한 값과 $T_{i+2}$, $N_i$를 UP_Link 정보에 따라 TBS에게 전송한다.

TBS는 $T_{i+2}$의 유효성과 저장된 $N_i$와 일치하는지 검증하고 New_AK를 $T_{i+2}$ 와 함께 HO_AK로 암호화하여 전송한다.

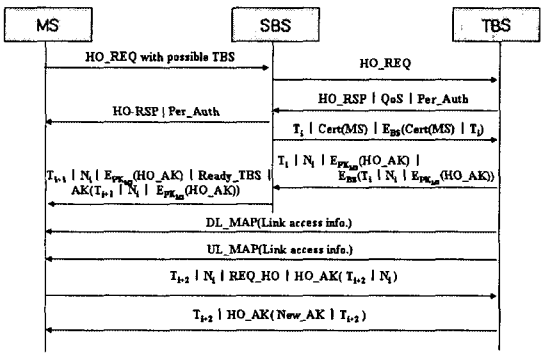


그림 2. 제안 핸드오버 기법

## IV. 제안 기법의 안전성 및 효율성 분석

이 절에서는 제안한 IEEE 802.16e/와이브로 망에서 안전한 Handover 방안에 대한 안정성과 효율성에 대해서 분석한다.

■ Replay 공격

공격자가 사용했던 정보를 재사용 했을때 BS 이나 MS에서는 서로 송수신한 Timestamp 또는 난수 N의 유효성 검증을 통하여 공격 여부를 판명 함으로써 Replay 공격을 막을 수 있다.

■ Man-in-the-Middle 공격

본 논문에서 제안한 기법의 특징은 MS의 발급된 인증서를 활용하는 것이다. 기존 논문[3]에서 SBS가 악의적인 목적으로 New_AK를 획득할 수 있는 취약성을 MS의 공개키를 이용하여 방지한다. 이는 TSB에서 MS의 공개키로 HO_AK를 암호화함으로써 SBS가 그 정보를 알 수 없게 하고 또한 MS의 개인키로만 복호화 됨으로 HO_AK 및 New_AK의 기밀성이 보장된다.

■ Stolen-Verifier 공격

사전에 BS 간에 안전하게 비밀키를 공유하고 있지만 만약 이 비밀키가 노출된다 하더라도 HO_AK는 MS의 공개키로 암호화되어 있어 이를 유추하지 못한다.

## V. 결론

본 논문은 최근 이슈화 되고 있는 IEEE 802.16e/와이브로 망에서 안전한 핸드오버 적용 방안에 대해서 제안하였다. 이는 기존 [3]의 핸드오버 보안상 취약점을 지적하고 이를 해결하기 위해 인증서를 사용한 핸드오버 기법으로 취약점을 개선하였다. 다시말해 SBS는 MS의 인증과정에서 받은 인증서를 TBS에게 전송하여 재사용함으로써 MS의 공개키를 이용해 핸드오버 시 안전하게 새로운 인증키(New_AK)를 MS와 TBS 사이에 공유 할 수 있다. 또한 Timestamp와 난수 N은 매번 다른 값을 전송함으로써 위조가 불가능하고 송신자의 데이터 작성 시각과 그 이후의 데이터 수정 여부를 체크할 수 있고, 난수의 경우 MSS가 TBS에게 자신이 정당한 MSS라는 것을 입증하기 위해 사용된다. 그리고 Replay 공격이나 Man-in-the-middle 공격 등의 각종 공격으로부터 안전도를 지니면서, 보다 높은 효율을 가진다.

본 논문은 [3-5]의 특징을 살리고 보안점을 개선한 핸드오버 방식은 국내의 WiBro 시장 및 국외 시장에서 효율적으로 사용 될 수 있을 것이다.

## [참고문헌]

[1] 이지영, "휴대인터넷 기술," ITA, 2006

[2] 이건백, 이현우, 류원, 조진성, "WiBro와 이기종 무선망 연동 및 고속 핸드오프 방안," 한국컴퓨터종합학술대회, 2005 논문집, Vol.32, No1.

[3] Sen Xu, Manton Matthews, Chin-Tser Huang, "Security Issues in Privacy and Key Management Protocols of IEEE 802.16," ACMSE'06, March, 2006

[4] Itzik Kitroser, "IEEE 802.16e handoff draft", IEEE C802.16e-03/20rl, 2003

[5] David Johnston, Jesse Walker, "Overview of IEEE 802.16 Security," IEEE Security & Privacy, May/June 2004