韓國 컴퓨터情報學會 論文誌
第13卷 第7號, 2008. 12.

2008-13-7-3-6

Mobile WiMAX 환경에서 인터 네트워크간 가입자를 인증하기 위한 핸드오버 메커니즘

정 윤 수*, 김 용 태**, 김 재 홍***, 박 길 철****

A Handover Mechanism for Authenticate Subscriber between inter-network in Mobile WiMAX Environment

Yoon-Su Jeong*, Yong-Tae Kim**, Jae-Hong Kim***, Gil-Cheol Park****

요 약

최근 중저속 환경에서 인터넷서비스를 제공하는 WiMAX는 현재 Wi-Fi보다 그 기능 및 범위가 넓어지고 있다. 네트워크 범위가 넓어지면서 WiMAX는 가입자의 핸드오버시 발생할 수 있는 보안문제를 가입자 재인증 과정을 통해 해결하고 있지만 전력소모와 지연문제를 발생하면서 WiMAX 보안 문제가 추가적으로 발생되고 있다. 이 논문에서는 Mobile WiMAX에서 대두되고 있는 지연문제와 처리량 문제를 해결하기 위해 인터 도메인간 가입자의 재인증 처리절차를 간소화하면서 핸드오버상에 발생할 수 있는 보안 문제를 예방하는 핸드오버 메커니즘을 제안한다. 제안된 메커니즘은 유연성과 보안성을 향상시키기 위해 PKI 구조와 협력할 수 있고, 가입자의 끊김 없는 서비스 제공을 통해 네트워크 재진입 과정이나 재인증 과정을 최소화 할 수 있다. 실험 결과 제안기법은 기존 IEEE 802.16e 표준보다 이동 가입자 수에 따른 처리량이 9.5% 낮았고, 핸드오버시 발생하는 man-in-the-middle 공격과 reply 공격에 안전함을 증명하고 있다.

Abstract

Now a days, WiMAX which provides internet service with a middle and low speed serves more function and is wider than Wi-Fi. While they solve the security risks as subscribers do handover by subscriber's re-certification procedure as the Network range is getting wider, there are more security problems making the problems of electric-power consumption and delay. This paper suggests a handover mechanism which simplify the subscriber's re-certification procedure and

• 제1저자 : 정윤수 교신저자 : 김용태
• 접수일 : 2008. 9. 15, 심사일 : 2008. 9. 20, 심사완료일 : 2008. 12. 24.
* 충북대학교 전자계산학과 ** 한남대학교 멀티미디어학부 강의전담 교수 *** 영동대학교 컴퓨터공학과 교수
**** 한남대학교 멀티미디어학부 교수
※ 본 연구는 지식경제부 지역혁신센터 사업인 민군겸용 보안공학연구센터 지원으로 수행되었음

prevents a security problem as doing handover for solving the problem of delay and the rate of processing. The mechanism can cooperate with PKI structure to increase flexibility and security and minimize network re-entry procedure or re-certification procedure by providing continual service. As a result, the mechanism's throughput as the number of subscribers is lower than IEEE 802.16e and the mechanism proves that it is secure from the attack of man-in-the-middle and reply as doing handover.

▸ Keyword : 와이맥스(WiMAX), 인증(Authentication), 프로토콜(Protocol)

Ⅰ. 서 론

최근 노트북, PDA와 같은 이동 단말기의 사용이 일반화되면서 비디오 스트리밍, UCC(user Created Content)등과 같은 고속의 데이터 전송을 요구하는 멀티미디어 콘텐트들이 보급되어 이동성을 전재로 한 고속 인터넷 서비스에 대한 요구가 점차 증가하고 있다. 현재까지 개발된 기술중에 고속의 이동성을 보장하는 셀룰러 이동통신 시스템의 HSDPA는 고속의 데이터 전송을 할 수 있는 장점을 가지지만 높은 이용요금으로 사용자에게 부담이 되는 단점을 가지고 있다. WLAN은 이용 요금이 저가이지만 HSDPA에 비해 이동성이 보장되지 않는다[1].

Mobile WiMAX(Worldwide Interoperability for Microwave Access)는 기존 인터넷 서비스의 요구사항을 수용할 수 있으며 사용자의 이동으로 인하여 발생되는 핸드오버 시에도 사용자 트래픽에 대하여 서비스 품질을 끊임없이 제공할 수 있다. 그러나 Mobile WiMAX 시스템이 많은 보안 기능을 제공함에도 불구하고 Mobile WiMAX 네트워크는 여전히 몇몇 취약성을 가지고 있다. 그 중 첫째는 네트워크 진입 과정에서 MAC 관리 메시지들에 대한 보안부재로 인한 보안 context들의 노출이며, 둘째는 Mobile WiMAX의 ASN(Access Service Network), CSN(Connectivity Service Network) 간 통신시에 상이한 도메인간 보안 기능을 제공하는 문제이다. 마지막은 핸드오버 과정에서 시스템간에 이동성을 지원하기 위한 보안 문제가 있다[2,3,11].

최근 WiMAX의 보안문제가 대두되면서 WiMAX 표준에서 제공하는 여러 보안기법이외에 많은 연구자들이 WiMAX 보안관련 연구를 진행하고 있다. Kassb et al.은 사전 키 분배를 기반으로 802.11 네트워크를 위한 빠른 사전 인증 기법을 제안했다. 이 기법은 MS와 BS사이에서 사전 필요한 키 자료(material)와 EAP-TLS 단계를 줄임으로써 핸드오버 지연을 줄였다. 그러나 이 기법은 네트워크가 확장될 경우 man-in-the-middle과 같은 공격을 통해 이동 노드의 키 정보가 유출될 수 있는 문제점을 가지고 있다[4].

본 논문에서는 인터 도메인간 가입자가 이동이 필요할 경우 가입자와의 인증정보를 AAA 인증 서버와 함께 ASN간 상호인증을 통해 가입자가 끊김없이 네트워크를 핸드오버할 수 있도록 가입자를 재인증하는 핸드오버 메커니즘을 제안한다. 제안된 메커니즘은 기존 가입자가 소속된 네트워크의 1회 인증과정을 통해 네트워크간 이동시 ASN과 별도의 인증과정 없이 인증정보만을 가지고 통신할 수 있다. 특히, 기존 WiMAX 환경에서 발생할 수 있는 네트워크 도메인간 통신 문제를 해결하기 위해 제안 메커니즘에서는 홉-대-홉 인증을 수행한다.

이 논문의 구성은 다음과 같다. Ⅱ장에서는 WiMAX와 Mobile WiMAX에 대하여 분석한다. Ⅲ장에서는 Mobile WiMAX 환경에서 인터 도메인간 SS의 안전한 통신을 제공하는 상호인증 프로토콜을 제시하고, Ⅳ장에서는 제안 프로토콜에 대한 효율성 및 안전성에 대하여 분석·평가한다. 마지막으로 Ⅴ장에서는 본 연구의 결과를 요약하고 향후 연구에 대한 방향을 제시한다.

Ⅱ. 관련연구

2.1 Mobile WiMAX

WiMAX 기술은 크게 Fixed WiMAX와 Mobile WiMAX로 구분된다. Fixed WiMAX는 기존 무선인터넷 기술인 Wi-Fi의 커버리지와 속도를 개선하기 위해 개발한 기술로 IEE 802.16-2004를 기반으로 하고 있으며, Mobile WiMAX는 이동성을 추가한 IEEE 802.16e를 기반으로 개발된 기술이다[5,10]. Mobile WiMAX의 전체적인 환경은 (그림 1)과 같다.

특히, Mobile WiMAX는 Fixed WiMAX의 이동성 문제를 개선하여 이동 중에도 최대 30Mbps의 속도로 데이터를 주고받을 수 있고, 기지국간 이동을 원활하게 하는 핸드오버 기능을 지원하며, 핸드오버 지연시간을 50ms 미만으로 낮추

어 VoIP와 같은 실시간 서비스도 품질의 저하없이 제공할 수 있는 규격을 지원한다.

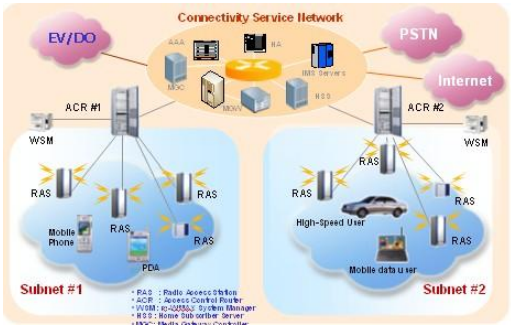

그림 1. Mobile WiMAX 환경
Fig 1. Mobile WiMAX Environment

2.2 Mobile WiMAX 핸드오버 기능

Mobile WiMAX가 핸드오버 기능에 의해 제공되는 핸드오버 형태는 MS 시작 핸드오버, 네트워크 시작 핸드오버, FBSS/MDHO가 있으며, 핸드오버 운영에 따라서 다음과 같이 분류된다[6].

① Serving HO Function

핸드오버에 관련된 시그널링 절차와 핸드오버 결정을 위한 전체적인 운용을 제어하는 HO 기능이다. 이 기능은 핸드오버를 위한 메시지를 필요시 릴레이 HO 기능을 통해서 타겟 HO 기능에 전송하며, 결과를 MS에 전송하는 기능을 수행한다.

② Relaying HO Function

서빙 HO 기능과 타겟 HO 기능 사이에 위치하여 핸드오버에 관련된 제어 메시지를 중재하는 HO 기능이다. 이 기능은 핸드오버 메시지의 내용을 갱신할 수 있으며 핸드오버 결정에 영향을 줄 수 있다.

③ Target HO Function

핸드오버를 위한 목적지로 선택되었거나 잠재적인 목적지로 선택된 HO 기능이다.

2.3 Mobile WiMAX의 사전인증 기법

Mobile WiMAX에서 Kassab는 사전적 키 분배를 기반으로 802.11 네트워크를 위한 빠른 사전 인증 기법을 제안했다[9]. 이 기법은 MS와 BS사이에 사전 계산된 키 정보와 EAP-TLS의 단계를 줄임으로써 핸드오버 지연을 줄이고 있다. 사전 인증 기법은 IAPP 캐싱을 이용한 PKD(Pro-active Key Distribution)와 4 방향 핸드쉐이크를 사용하는 PKD가 있다.

PKD는 MS와 AP사이의 PMK의 사전 계산을 사용한다[8]. PKD의 처리방법은 AAA 서버를 가지고 동작된다. MS가 이웃 지역으로 로밍할 때 PMK는 더 이상 적용하지 않는다. IAPP에서 캐싱을 이용하는 방법은 PTK(Pairwise Transient Key)와 TIME_AUTH 값이 협력되기 위해서 이웃 AP들에게 IAPP 교환을 실행한다[9]. 이 기법은 단지 한 번만 그룹 키 핸드쉐이크가 실행된다. 또 다른 기법은 4방향 핸드쉐이크 방법으로 PTK 이웃 처리과정이 사전 인증 과정으로 동작된다. 따라서 핸드오버 동안 MS는 인증을 끝내기 위해 새로운 AP와 함께 그룹 키 핸드쉐이크 교환을 실행한다.

III. 인터 네트워크간 상호인증 프로토콜

이 장에서는 가입자가 다른 네트워크로 이동할 경우 추가적인 인증절차 없이 가입자와 ASN이 가지고 있는 가입자의 인증정보를 바탕으로 통신을 끊김없이 사용할 수 있는 상호인증 프로토콜을 제안한다.

3.1 네트워크 모델

이 절에서는 인터 네트워크간 상호 인증을 수행하기 위하여 IEEE 802.16e 표준에서 지정한 EAP 방법을 SS(Subscriber Station)와 BS(Base Station) 사이에 적용한 제안기법의 네트워크 구조를 (그림 2)에서 보여주고 있다.

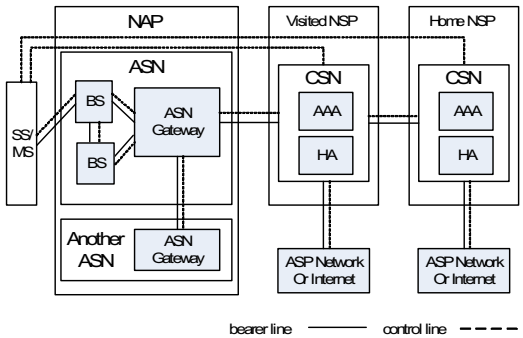

그림 2. Mobile WiMAX 네트워크 구조
Fig 2. Mobile WiMAX Network Structure

(그림 2)은 제안 프로토콜이 적용되는 Mobile WiMAX 네트워크 모델을 보여주고 있다. (그림 2)에서처럼 네트워크는 크게 SS/MS(Subscriber Station/ Mobile Station), NAP(Network Access Provider)의 ASN(Access Service

Network) 그리고 NSP(Network Service Provider)의 CSN(Connectivity Service Network) 등의 3개 부분으로 나누어진다.

ASN은 Mobile WiMAX 가입자에게 무선 접속을 제공하기 위해 필요한 네트워크 기능으로 정의되며 Mobile WiMAX에서 정의하고 있는 ASN 프로파일에 따라서 BS와 ASN으로 나누어진다. CSN은 WiMAX 가입자에게 IP 연결 서비스를 제공하기 위한 네트워크 기능들의 집합으로 정의된다. (그림 2)의 네트워크 구조는 서로 다른 BS(Base Station)의 ASN간 SS/MN이 인증할 수 있도록 X.509 인증서를 사용한다.

3.2 용어 정의

제안 프로토콜에서 사용하는 주요 용어를 정의하면 (표 1)와 같다. (표 1)에서 사용된 용어는 타원곡선 암호에 사용되는 파라미터들과 노드들의 좌표값에 해당하는 용어들이다.

표 1. 파라미터
Table 1. Parameter

Notaion	Definitions
PU_A	A의 공개키
PR_A	A의 개인키
$E_{PU_A}(X)$	A의 공개키를 가지고 X를 암호화
$D_{PR_A}(X)$	A의 개인키를 가지고 X를 복호화
$S_{PR_A}(X)$	A의 개인키를 통해 메시지 X에 대한 시그너처 생성
$V_{PU_A}(X,S)$	A의 공개키를 통해 시그너처 S와 일치하는 메시지 X를 검증
$C(X)$	X의 인증서
AL	ASN 리스트 정보
$E_{X\|Y\_AK}(M)$	X와 Y의 공유된 인증키로 메시지 X를 암/복호화
R_A	A에 의해 생성된 Pseudo 랜덤 수
ID_A	A의 인식자
$H()$	One-way 해쉬 함수
$M_1 \| M_2$	Concatenation of M_1 and M_2

3.3 네트워크간 핸드오프 인증 프로토콜

이 절에서는 네트워크간 가입자가 핸드오프할 경우 가입자와 베이스 스테이션사이에 사전에 상호인증이 수행된 것으로 가정한다. 제안 프로토콜은 특정 지역의 BS와 상호인증을 수행한 가입자가 다른 네트워크에 위치한 BS과 통신의 끊김없이 통신을 원활하게 수행하기 위해서 이전 BS과 상호인증 과정을 통해 얻은 인증정보를 BS을 통해 전달하여 가입자가 네트워크간 안전한 핸드오프를 수행할 수 있도록 한다.

제안 메커니즘에서 제안하고 있는 인증 과정은 네트워크간 가입자가 핸드오버 할 경우 발생하며 이 과정의 세부적인 인증 처리절차는 (그림 3)와 같다.

- 단계 1 : $SS/MN \rightarrow BS_1$
  SS/MN는 SS/MN이 생성한 난수(N_{SS}), SS의 인증서($C(SS)$), BS_1의 개인키로 생성한 SS의 시그너처($S_{PR_{ASN}}(SS)$)를 BS_1에게 전송한다.
- 단계 2 : $BS_1 \rightarrow ASN$
  BS_1은 SS/MN에게 전달받은 정보를 확인한 후 BS_1의 인증서를 포함하여 ASN의 공개키로 암호한 후 ASN에게 전달한다.
- 단계 3 : $ASN \rightarrow AAA\ \ Authentication\ \ Server$
  ASN는 SS/MN의 정보를 AAA 인증서버에게 검색 요청한다.
- 단계 4 : $AAA\ \ Authentication\ \ Server \rightarrow ASN$
  AAA 인증서버는 SS/MN의 인증정보를 검색한 후 SS/MN 정보에 대한 랜덤 수 R을 생성하여 ASN에게 전달한다.
- 단계 5 : $BS \rightarrow BS_1$
  ASN는 AAA 인증서버에게 전달받은 랜덤 수 R과 인증키 AK을 SS/MN의 공개키로 암호화한 후 ASN의 인증서를 BS_1에게 전달한다.
- 단계 6 : $BS_1 \rightarrow SS/MN$
  BS_1은 BS에게 전달받은 정보를 복호화한 후 BS_1의 인증서와 ASN의 리스트 정보를 SS/MN의 공개키를 이용하여 SS/MN에게 전달한다.
- 단계 7 : $SS/MN \rightarrow BS_1$
  SS/MN은 전달받은 N_{SS}값과 기존 N_{SS}값을 비교한 후 BS_1에게 전달받은 ASN의 리스트 정보를 이용하여 주위의 액세스 서비스가 가능한 네트워크를 검색한다. 검색된 ASN이 발견되면 ASN의 인증서에 ASN과 일치하는 공개키 정보를 포함시킨 후 BS_1에게 $SSID$, R, $N_{SS}^{'}$, $N_{BS}^{'}$등과 같은 정보를 보낸다.
- 단계 8 : $BS_1 \rightarrow BS_2$
  BS_1은 SS/MN에게 전달받은 ASN 리스트 정보를 이용하

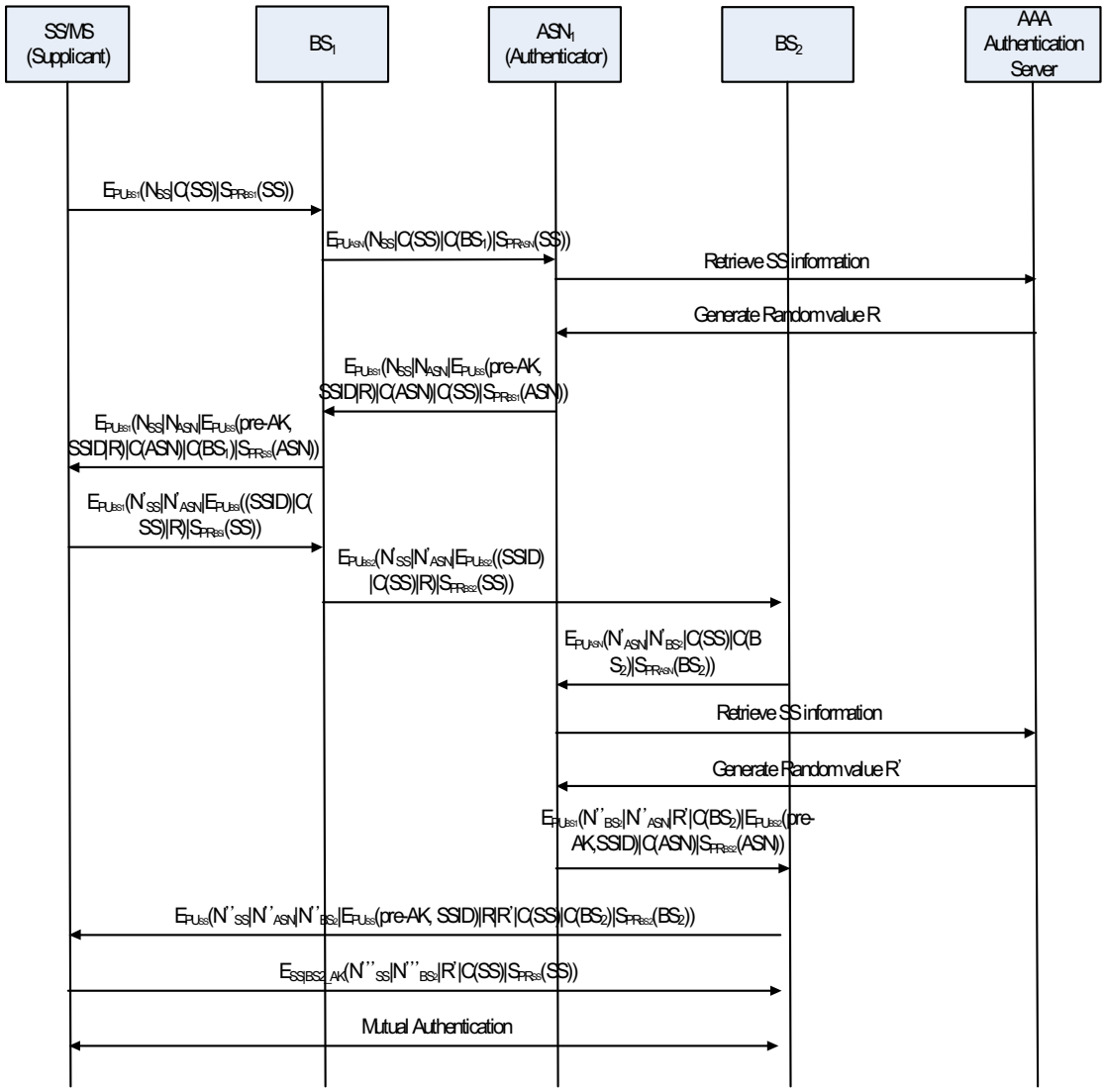

그림 3. 제안 프로토콜의 흐름도
Fig 3. The Flow of the Proposed Scheme

여 선택된 BS_2에게 SS/MN의 정보를 그대로 전달한다. 이 때, SS/MN이 AAA 서버에게 전달받은 랜덤 값 R과 인증서를 이용하여 man-in-the-middle 공격을 예방할 수 있다.

- 단계 9 : $BS_2 \rightarrow BS$

  BS_2는 SS/MS의 정보와 함께 BS_2의 인증서를 BS에게 전달한다.

- 단계 10 : $BS \rightarrow AAA\ \ Authentication\ \ Server$

  SS/MN의 정보를 전달받은 ASN는 $AAA\ \ Authentication\ \ Server$에게 SS/MN의 인증 정보를 요청한다.

- 단계 11 : $AAA\ \ Authentication\ \ Server \rightarrow ASN$

  SS/MN의 인증 정보를 $AAA\ \ Authentication\ \ Server$에서 검색한 후 SS/MN의 정보를 이용하여 랜덤 수 R을 생성하여 ASN에게 전달한다.

- 단계 12 : $BS \rightarrow BS_2$

  ASN는 AAA 인증서버로부터 전달받은 랜덤 수 R과 인증키 AK을 SS/MN의 공개키로 암호화한 후 ASN의 인증서를 BS_2에게 전달한다.

- 단계 13 : $BS_2 \rightarrow SS/MN$

  BS_2은 BS에게 전달받은 정보를 복호화한 후 BS_2의 인증서와 ASN의 리스트 정보를 포함시킨 후 SS/MN의 공개키를 이용하여 SS/MN에게 전달한다.

- 단계 14 : $SS/MN \rightarrow BS_2$

  SS/MN은 난수 값 N_{SS}''', N_{ASN_i}'''을 BS_2에게 전달하여 BS_2이 SS/MN에게 전달한 난수 값과 비교한다.

- 단계 15 : $SS/MN \leftrightarrow BS_2$

  다른 기지국으로 이동한 SS/MN은 BS_1으로부터 전달받은 정보를 이용하여 BS_2과 함께 상호인증을 위한 키를 생성한 후 상호인증 키를 이용하여 데이터를 전달한다.

Ⅳ. 평가

4.1 보안 평가

제안 메커니즘에서는 SS/MN과 ASN 사이에서 발생하는 재전송 공격을 예방하기 위해 홉-대-홉 인증을 통해 인증서와 랜덤수를 사용하여 인증을 수행하였으며, AAA구조에서 SS/MN의 인증과 권한 기능을 수행할 수 있도록 SS/MN이 ASN 리스트를 활용하였다. 제안기법에서 BS와 ASN이 MN을 인식하고 인증하기 위해 서명기법을 인증키와 함께 사용하였다. SS/MN의 신뢰적인 핸드오버 동작은 SS/MN의 요청에 의해 AAA 인증서버에게 인증정보를 검증받은 후에 네트워크간 핸드오버가 동작되고 있기 때문에 MN과 ASN, ASN과 BS 사이에서 이루어지는 repay 공격을 예방할 수 있다. 또한, SS/MN, ASN, BS에서 사용하고 있는 파라미터들의 기밀성을 보장하기 위해 제안 메커니즘에서는 keying material 정보를 사용하였다. keying material 정보를 사용하는 목적은 SS/MN과 ASN 사이에서 기밀성 있는 데이터를 교환하는 역할이다. BS는 SS/MN과 ASN에 대한 일정 크기의 관리 목록을 유지하면서 목록에 저장되지 않은 SS/MN이 인증 요청을 할 경우 SS/MN의 인증 요청을 거부한다. 또한, 제안 프로토콜에서는 인증정보와 서명 기법을 함께 사용하여 Mobile WiMAX에서 발생할 수 있는 제3자의 악의적인 redirect 및 DoS공격을 방지할 수 있다.

4.2 성능 평가

4.2.1 실험환경

이 절에서는 Mobile WiMAX환경에서 제안 프로토콜의 타당성을 검증하기 위해서 NS-2을 이용하여 실험 모델을 구현하였다.

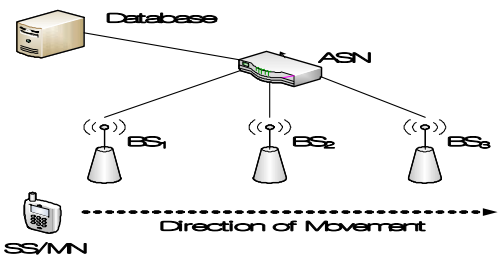

그림 4. 실험 시나리오
Fig 4. Simulated Scenario

제안 프로토콜의 실험 시나리오는 (그림 4)과 같다. BS는 Mobile WiMAX상에서 500m 범위내에서 SS/MN과 통신이 이루어진다. (그림 4)에서 SS/MN의 최대 수는 200으로 하며 시간에 따른 패킷 지연시간과 트래픽 처리량을 중심으로 성능 실험을 수행한다[7]. 제안 프로토콜에서 사용하는 SS/MN의 트래픽 모델은 CBR 모델을 사용한다.

4.2.2 실험결과

(그림 5)는 Mobile WiMAX 표준에서 제공하는 핸드오버 규격과 제안 프로토콜의 패킷지연시간을 비교평가하고 있다. (그림 5)의 결과에서처럼 패킷 지연시간은 핸드오버 처리시간에 따라 지연시간의 차이를 보이고 있다. 특히 실험 결과 제안 프로토콜이 IEEE 802.16 표준보다 지연시간이 일정하며 패킷 손실 및 지연시간도 IEEE 802.16 표준 보다 11% 향상을 보이고 있다.

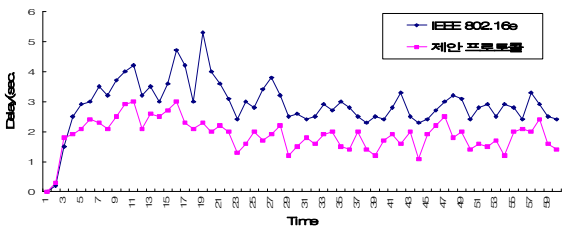

그림 5. 패킷 지연시간
Fig 5. Packet Delay Time

(그림 6)은 SS/MN의 이동 속도에 따른 평균 이동 지연시간을 보여주고 있다. (그림 6)처럼 SS/MN의 평균 속도를

10km/h, 30km/h, 50km/h로 구분하여 실험한 결과 제안 프로토콜이 IEEE 802.16 표준보다 7% 향상된 결과를 보이고 있다.

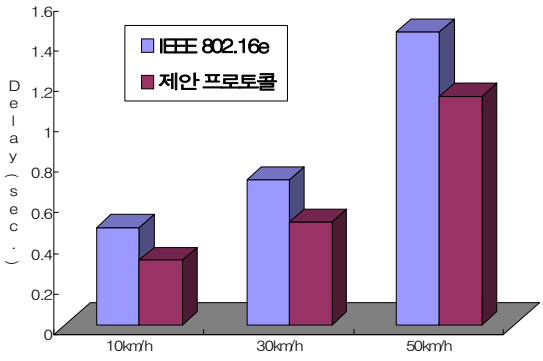

그림 6. 이동 속도에 따른 평균 지연시간
Fig 6. Average Delay Time through Mobile Speed

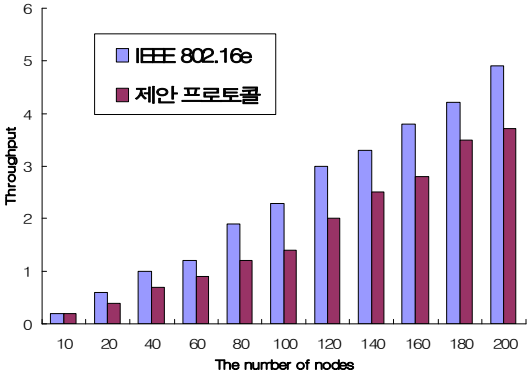

그림 7. SS/MN 수에 따른 처리량
Fig 7. Throughput through the SS/MN

(그림 7)은 도메인간 이동하려고 하는 SS/MN수에 따른 처리량을 보여주고 있다. IEEE 802.16e 표준에서는 도메인간 이동하려고 하는 노드수가 평균 20, 80, 120일 경우 ASN과 BS의 병목현상으로 인해 처리량이 급격하게 늘어나는 현상이 발생하였으며, 제안 프로토콜에서는 노드의 추가인증 처리절차없이 수행되기 때문에 노드 증가에 따른 처리량이 IEEE 802.16e보다 처리량이 일정비율로 증가하고 있다.

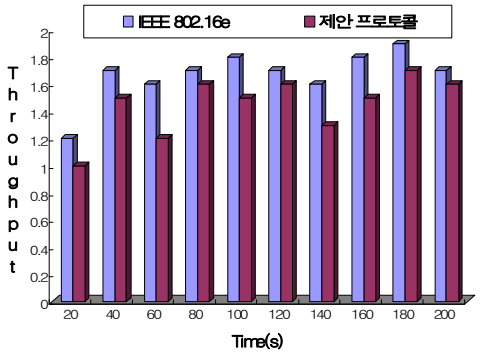

그림 8. 이동 시간에 따른 처리량
Fig 8. Throughput through Mobile Time

(그림 8)은 도메인간 이동하려고 하는 SS/MN의 이동시간을 매 20초 간격으로 분석한 결과이다. (그림 8)의 분석결과 IEEE 802.16e와 제안 프로토콜의 처리량이 20초, 60초, 140초에서 감소하였으며, 이 부분에서 핸드오버가 발생할 때 인증정보를 유지하면서 핸드오버를 하는 경우 제안 프로토콜이 기존 IEEE 802.16e 표준보다 11% 향상된 결과를 얻을 수 있었다.

V. 결론

본 논문에서는 가입자가 네트워크간 이동할 경우 재인증과정 없이 핸드오버 프로토콜의 효율성을 향상시키면서 안전성을 보완한 인터 도메인간 가입자의 상호인증을 수행하는 핸드오버 메커니즘을 제안했다. 제안된 프로토콜에서는 이전 인증정보를 핸드오버동안 유지하면서 지연시간과 처리량을 줄일 수 있었다. 또한, IEEE 802.16e 표준과 비교 분석한 결과, 안전성 측면에서는 최신 Mobile WiMAX에서 발생되는 재전송공격, 제3자의 악의적인 redirect 공격 및 DoS 공격에 안전한 결과를 얻었고, 효율성 측면에서는 제안 프롤코콜이 IEEE 802.16e 표준보다 패킷 손실 및 지연도가 11%의 향상되었으며 SS/MN의 이동 속도에 따른 평균 지연시간도 7% 향상된 결과를 얻을 수 있었다. 향후 연구에서는 Mobile WiMAX 환경에서 자주 발생되는 여러 보안 공격에 안전한 메커니즘 연구를 수행할 계획이다.

참고문헌

〔1〕 A. Ghosh, D. R. Wolter, J. G. Andrews and R. Chen, "Broadband Wireless Access with WiMax/802.16: Current Performance Benchmarks and Future Potential", IEEE Communications Magazines, vol. 43, issue 2, pp. 129~136. Feb. 2005.

〔2〕 TTAS.KO-06.0065R1, "2.3GHz 휴대인터넷 표준 매체접근 제어 계층", 2004.

〔3〕 IEEE 802.16e-2005, "Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems", 2006.

〔4〕 IETF RFC 4285, "Authentication Protocol for Mobile IPv6", 2006.

〔5〕 WiMAX Forum NWG, "Stage-3: Detailed Protocol and Procedures", 2007.

〔6〕 김대익, 이상호, 김영진, "WiBro/Mobile WiMAX 이동성 기술", 한국정보과학회, vol. 25, No. 04, pp. 5~14. 2007. 04.

〔7〕 T. Janevski, "Traffic analysis and design of wireless IP networks", Artech House, pp. 186~190, 2003.

〔8〕 A. Mishra, M. Shin and W. Arbaugh, "pro-active Key Distribution using neighbor Graphs", IEEE Wireless Communication, vol. 11, Feb 2004."

〔9〕 M. Kassb, A. Belghith, J. M. Bonnin and S. Sassi, "Fast Pre-Authentication Based on Proactive Key Distribution for 802.11 Infrastructure Networks", In Proceedings of the 1st ACM workshop on Wireless multimedia networking and performance modeling, pp. 46-53, 2005.

〔10〕 D. Sweeney, "WiMax Operator Manual: building 802.16 Wireless Networks", Apress, 2005.

〔11〕 D. Johnston and J. Walker, "Overview of IEEE 802.16 Security", IEEE Security & Privacy, 2004.

저 자 소 개

정 윤 수

2000년 2월 : 충북대학교 대학원 전자계산학 이학석사

2008년 2월 : 충북대학교 대학원 전자계산학 박사

관심분야: 센서 보안, 암호이론, 정보보호, Network Security, 이동통신보안

김 용 태

1984년 한남대학교 계산통계학과

1988년 숭실대학교 대학원 전자계산학과 공학석사

2008년 2월 충북대학교 대학원 전자계산학과 이학박사

2006.3 ~ 현재 한남대학교 멀티미디어학부 강의전담교수

관심분야: 모바일 웹서비스, 정보보안, 센서 웹, 모바일 통신 보안, 멀티미디어

김 재 홍

1994년 인하대학교 대학원 전자계산공학과 졸업(박사)

1995년~현재 영동대학교 컴퓨터공학과 교수

관심분야 : 멀티미디어 데이터베이스, 지리정보시스템, 저장관리자

박 길 철

1983년 한남대학교 계산통계학과

1986년 숭실대학교 대학원 전자계산학과 공학석사

1998년 성균관대학교 대학원 정보통신공학과 공학박사

2006년 UTAS, Australia교환교수

1998년 8월~ 현재 한남대학교 멀티미디어학부 교수

(관심분야) multimedia and mobile communication, network security