베이스 스테이션의 성능부하를 최소화하기 위한 WiMAX 보안 메커니즘

정윤수*, 김용태**, 박길철***, 이상호****

WiMAX Security Mechanism for Minimizing Performance load of Base Station

Yoon-Su Jeong*, Yong-Tae Kim**, Gil-Cheol Park***, Sang-Ho Lee****

본 연구는 지식경제부 지역혁신센터 사업인 민군겸용 보안공학 연구센터 지원으로 수행되었음

요 약

최근 IEEE 802.16 WiMAX에서는 인터넷 기반의 다양한 서비스와 애플리케이션의 빈번한 사용으로 인하여 저비용, 고효율의 특성을 가지는 이동 단말기의 사용이 일반화되고 있다. 이동 단말기의 사용이 일반화되면서 고속 인터넷 서비스의 보안 문제를 해결하기 위한 연구가 IEEE 802.16e 표준을 중심으로 연구되고 있다. 이 논문에서는 IEEE 802.16 WiMAX의 보안 요구사항을 충족하기 위해 IEEE 802.16e 표준에서 제공하는 기본 기능이외에 SS의 인증부하 및 보안공격(reply 공격과 man-in-the-middle 공격)에 안전한 보안 메커니즘을 제안한다. 제안된 메커니즘은 SS와 BS가 생성한 난수와 비밀값을 이용하여 TEK과 데이터 암호에 필요한 키 정보를 교환한다. 또한 SS의 초기 인증정보와 인증서를 이용하여 BS의 추가 인증 과정을 수행하지 않도록 하여 BS의 성능 부하를 줄인다.

ABSTRACT

Nowadays, usage of mobile unit which has a characteristic of low cost and high efficiency is being generalized because of frequent use of internet-based variable service and application in IEEE 802.16 WiMAX. A study for handling a security problem of high speed internet service is rising while the use of a mobile is being generalized. This paper suggests a security mechanism which provides safety from certification load of SS and a security attack as well as a basic function which is provided from IEEE 802.16e standard to satisfy security demand of IEEE802.16 WiMAX. The proposed mechanism exchangeskey material information for TEK and data code by using 난수(?) and secret value created by SS and BS, also reduces capacity load of BS not to perform an additional certificate procedure of BS by using the early certification information and certificate of SS.

키워드

WiMAX, PKM, 보안, 상호 인증 프로토콜

* 충북대학교 전자계산학과
** 한남대학교 멀티미디어학부 교수 (교신저자)
*** 한남대학교 멀티미디어학부 교수
**** 충북대학교 전기전자 컴퓨터공학부 교수

접수일자 2008. 05. 13

Ⅰ. 서 론

WiMAX(Worldwide Interoperability for Microwave Access)는 Wi-Fi의 한계로 지적되어온 제한된 커버리지 영역(AP당 약 30~200m 이내)과 전송 속도 개선, HotZone 내에서의 끊김없는 연결(seamless connection)을 통한 이동성 확보 등의 문제를 해결하기 위해 개발된 무선 광대역 접속 기술이다. 최근 IEEE 802.16e 표준이 2005년에 제정된 이후에 IEEE 802.16e 기반 네트워크의 보안 요구사항은 계속 증가하고 있다[1,3,4].

IEEE 802.16e의 Mobile WiMAX 환경에서는 사용자가 고정되어 있지 않고 네트워크간 이동이 수시로 이루어지기 때문에 이때마다 사용자를 인증하여 통신을 수행하기에는 베이스 스테이션과 ASN의 부하가 증가하는 문제점이 있다. Mobile WiMAX의 보안 문제점을 해결하기 위해서 IEEE 802.16e 표준에서는 SS(Subscriber Station)와 BS(Base Station) 사이의 안전한 통신을 지원하기 위해 기본(Primary), 동적(Dynamic) 그리고 고정(Static) SA의 보연연관(Security Association:SA)을 제공한다.

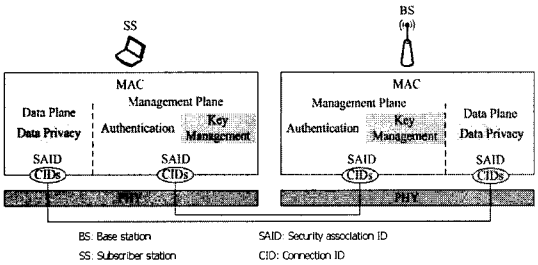

그림 1. IEEE 802.16 보안 협상
Fig 1. IEEE 802.16 Security Associations

그림 1의 SA는 SS와 BS 사이에 데이터 보안 협상을 위해 CID(Connection ID)와 SAID(Security Association ID)가 사용되지만 CID와 SAID만으로는 무선 환경에서 발생될 수 있는 보안공격에 안전하지 않다. 따라서 무선 보안 공격에 안전하기 위해서는 IEEE 802.16e 표준에서 제공하는 기본 보안기능이외에 보안 공격에 안전한 보안 메커니즘이 필요하다.

이 논문에서는 IEEE 802.16e 표준에서 제공하는 기본 보안 기능이외에 SS의 인증 부하를 줄이면서 무선 환경에서 발생하는 보안공격(reply 공격과 man-in-the-middle 공격)에 안전한 보안 메커니즘을 제안한다. 제안된 메커니즘은 SS와 BS가 생성한 난수와 비밀값을 이용하여 TEK과 데이터 암호에 필요한 키 정보를 교환한다. 또한 SS의 초기 인증 정보와 인증서를 이용하여 BS의 추가 인증 과정을 제거하여 BS의 성능 부하를 줄인다.

이 논문의 구성은 다음과 같다. 2장에서는 WiMAX와 PKM 프로토콜에 대해서 분석한다. 3장에서는 WiMEX 환경에서 발생되는 보안 공격유형에 대응하기 위해 *SS*와 *BS* 사이의 보안 메커니즘을 제시하고, 4장에서는 제안 프로토콜에 대한 효율성 및 안전성에 대하여 분석·평가한다. 마지막으로 5장에서는 이 논문의 결과를 요약하고 향후 연구에 대한 방향을 제시한다.

Ⅱ. 관련 연구

2.1 WiMAX

WiMAX는 Wi-Fi의 한계로 지적되어온 제한된 커버리지 영역(AP당 약 30~200m 이내)과 전송 속도 개선, HotZone 내에서의 끊김없는 연결을 통한 이동성 확보 등의 문제를 해결하기 위해 개발된 무선 광대역 접속 기술이다[2,6].

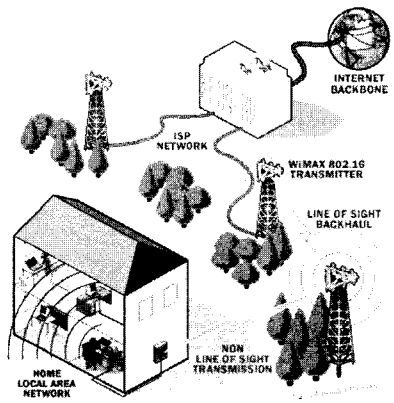

그림 2. WiMAX 환경
Fig 2. WiMAX Environment

그림 2의 WiMAX 환경에서 사용되는 기술은 크게 고정형 WiMAX 기술인 802.16-2004 표준과 이동형 기술인 802.16e 표준으로 분류할 수 있다. 802.16-2004 표준은 Fixed WiMAX라고도 불리며, WiMAX 포럼에서 WiMAX의 기반 기술로 선정되었다. 주로 고정 기기간

의 무선 통신에 활용되며, backhaul networking에도 적합하다. 802.16-2004 표준은 2004년 7월 장비 상호간 호환을 염두에 둔 표준안의 승인이 이루어진 후, 2005년 상반기 표준안을 따른 칩셋이 인증을 받아 Intel과 Fujisu 등에서 양산 체제를 갖추기 시작하였다.

Mobile WiMAX라는 이름으로 알려져 있는 802.16e 표준은 802.16-2004에 비해 이동성 문제를 개선하여 이동 중에도 최대 15Mbps의 속도로 데이터의 송・수신이 가능하다[10]. Mobile WiMAX는 셀 간 이동을 원활하게 하는 핸드오프 기능을 지원하고, latency를 50ms 미만으로 낮추어 VoIP와 같은 실시간 서비스도 품질의 저하 없이 제공할 수 있으며, 유연한 키 관리 기능을 이용하여 핸드오버 중 보안 기능을 유지할 수 있다. WiMAX 환경에서 PKM은 와이브로 표준에 명시된 인증 및 키 생성, 분배 프로토콜로 PKMv1과 보안성이 강화된 PKMv2가 있다. 이 기술은 망 접속을 위한 단말 및 네트워크간 인증, 암호화된 데이터 통신에 사용될 TEK(데이터 암호화 키) 교환이 가능하다. PKMv1은 기본적인 Key 관리 기능뿐 아니라 EAP 기반의 인증과 트래픽 암호화 등의 기능을 가진다[8,9]. IEEE 802.16e에서는 보다 강화된 Security Suite를 가진 PKMv2가 기본으로 사용된다.

2.2 PKM

PKM(Privacy Key Management Protocol)은 재인증 과정동안 SS의 권한을 책임지고 키 정보를 수신/갱신하는 역할을 한다. 이 프로토콜은 PKM 서버로써 기능하는 BS로부터 SS가 키 정보를 요청하는 클라이언트/서버 모델과 비교된다. IEEE 802.16e 표준에서는 PKMv1을 확장한 PKMv2을 지원한다. PKMv2에서는 PKMv1의 기본적인 키(Key) 관리 기능뿐 아니라 EAP 기반의 인증과 트래픽 암호화 등의 기능을 가진다. 그러나 사용자의 이동으로 인하여 고정된 WiMAX 환경보다 네트워크에 진입하는데 더 큰 보안 문제가 발생되며, IEEE 802.16e에서 제공하는 PKMv2만을 이용해서는 보안 문제가 완전하게 해결되지 못하고 있다[5,11,12].

III. WiMEX 보안 메커니즘

이 장에서는 WiMEX 환경에서 발생될 수 있는 Man-in-the-Middle과 Reply/DoS 보안 공격유형에 대응하기 위한 SS와 BS간의 보안 메커니즘을 제안한다. 제안된 보안 메커니즘의 전체적인 동작 과정은 인증 과정, TEK 교환 과정 그리고 데이터 암호화 과정 등으로 구분된다. 인증 과정은 SS와 BS 사이에서 상호 인증을 통해 SS에게 권한을 부여하는 과정이며, TEK 교환과정은 SAID와 AK 일련 번호, TEK 파라미터 등을 이용하여 데이터 암호에 사용될 키를 생성하는 과정이다. 마지막으로 데이터 암호화 과정은 TEK 교환과정에서 생성된 키를 이용하여 암호화된 데이터를 통신하는 과정이다.

3.1 용어 정의

제안 프로토콜에서 사용하는 주요 용어는 표 1과 같다. 표 1은 제안 메커니즘에서 사용되고 있는 용어들을 정의하고 있다.

표 1. 제안 프로토콜의 주요 용어 정의
Table 1. Parameter of Proposed Protocol

Notaion	Definitions
DS	SS가 소속된 도메인 정보
SS	가입자
BS	베이스 스테이션
$E_{PU_A}(X)$	A의 공개키를 가지고 X를 암호화
$S_{PR_A}(X)$	A의 개인키를 통해 메시지 X에 대한 시그너처 생성
$Cert_x$	x의 인증서
ID_{SS}	$Cert_{ss}$의 인식자
ID_{BS}	$Cert_{BS}$의 인식자
SA	보안협력(Security Association)
$SAID$	보안협력 인식자
N_{SS}	SS의 난수
N_{BS}	BS의 난수
$prf()$	pseudo 랜덤 수
$M_1 \| M_2$	M_1과 M_2의 연접

3.2 인증과정

인증 과정은 PKM 프로토콜을 기반으로 SS와 BS가 생성한 임의의 난수를 이용하여 SS의 권한을 부여하는 과정이다. 제안 메커니즘의 인증 과정은 그림 3과 같다. 그림 3에서 SS와 BS의 인증 과정은 5단계로 구성된다.

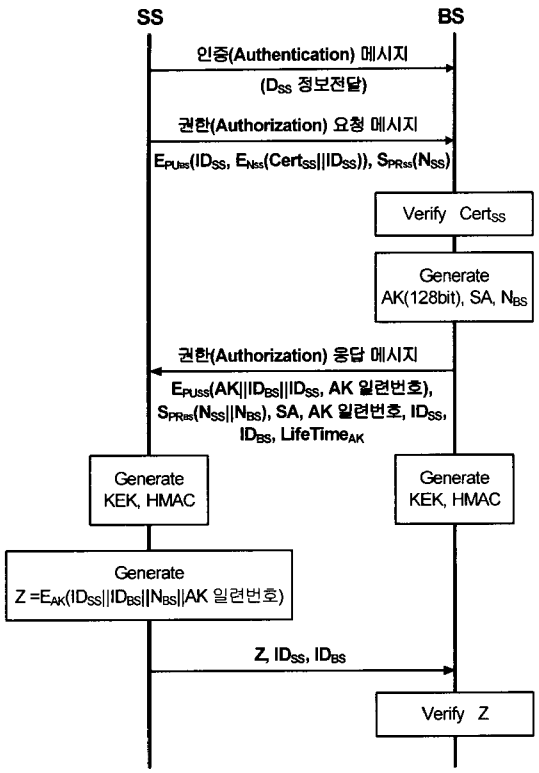

그림 3. 제안 메커니즘의 인증과정
Fig 3. Authentication Process of Proposed Mechanism

① 단계 1

SS는 D_{SS} 정보를 인증(Authentication) 메시지를 통해 BS에게 전달한 후 바로 권한(Authorization) 요청 메시지를 BS에게 전달한다. 이 때, BS에게 전달된 메시지는 식 (1)과 같다. 식 (1)에서는 SS의 ID, SS의 CID_{SS}, N_{SS}로 암호화한 $E_{N_{SS}}(Cert_{SS}\|SAID_{SS})$등을 BS의 공개키로 암호화한 메시지와 SS의 시그너처 값 $S_{PR_{SS}}(N_{SS}\|ID_{SS})$, $Cert_{SS}$, CID_{SS} 등이 생성된다.

$$E_{PU_{BS}}(ID_{SS}, CID_{SS}, E_{N_{SS}}(Cert_{SS}\|SAID_{SS})),\ S_{PR_{SS}}(N_{SS}\|ID_{SS}), Cert_{SS}, CID_{SS} \quad \text{식 (1)}$$

② 단계 2

BS는 전달받은 권한 요청 메시지를 통해 SS의 인증서를 추출하여 D_{SS} 정보와 비교하여 SS를 검증한다. 인증 메시지와 권한 요청 메시지를 통해 BS는 $Cert_{BS}$, N_{BS} 그리고 128비트 크기를 가지는 $AK(Authority\ Key)$를 생성한다.

$$Verify\ Cert_{SS} \quad \text{식 (2)}$$

$$Generate\ Cert_{BS}, N_{BS}, AK \quad \text{식 (3)}$$

③ 단계 3

BS는 SS의 ID를 판변한 후, primary SA의 속성과 ID를 SS가 액세스 할 수 있도록 SA를 메시지에 포함시킨 후. BS가 생성한 AK, AK 일련번호, $Life\ Time_{AK}$ 정보, 인증서 $Cert_{BS}$ 등의 식 (4)를 SS에게 전달한다.

$$E_{PU_{SS}}(AK\|ID_{BS}\|ID_{SS}\|CID_{BS}, E_{N_{BS}}(Cert_{BS}\|SAID_{BS}\|AK\ 일련번호), S_{PR_{BS}}(N_{SS}\|N_{BS}\|SAID_{BS}), Cert_{BS}, SA, AK\ 일련번호, CID_{BS}, Life\ Time_{AK} \quad \text{식 (4)}$$

④ 단계 4

SS는 전달받은 AK로부터 KEK와 메시지 인증키(HMAC_KEY_D와 HMAC_KEY_O)를 계산한다. 이 과정은 TEK 교환 과정에 필요하며 SS는 TEK 정보를 추가적으로 수신하기 위해 BS에게 부여받은 권한 상태를 유지한다. 이 과정은 $Life\ Time_{AK}$ 만기 전에 권한 요청 메시지를 BS에게 보내어 AK를 주기적으로 갱신하기 위해 필요하다. SS는 AK 키를 이용하여 BS에게 Z, ID_{SS}, ID_{BS}를 전달한다.

⑤ 단계 5

BS는 전달받은 Z를 AK를 이용하여 복호화한 후 단계 3에서 SS에게 전달한 N_{BS}를 검증한다. SS와 BS 사이에서 SS의 재권한 과정은 SS의 초기 권한 정보를 기반으로 수행되며 SS의 재권한 과정을 위해서는 단계 1의 과정을 필수적으로 수행해야 한다.

3.3 TEK 교환 과정

이 과정은 SS의 인증 과정이 끝난 후 인증 과정에서 생성한 키 정보를 이용하여 TEK 키를 교환하는 과정이다. TEK 교환 과정은 그림 4처럼 2가지 단계로 구성된다.

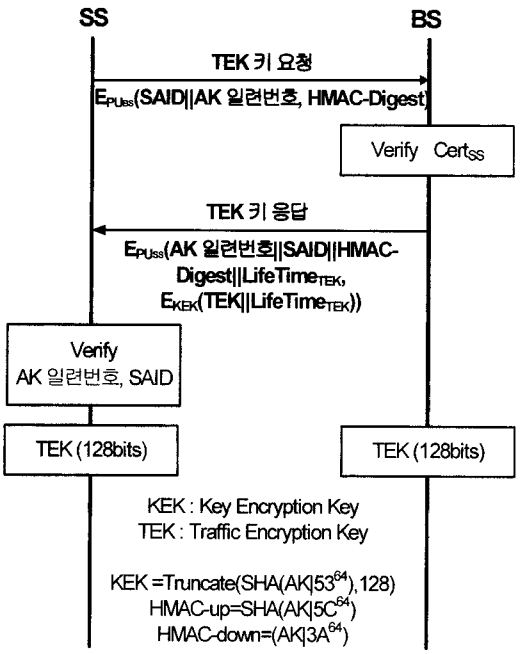

그림 4. 제안 메커니즘의 데이터 키 교환
Fig 4. Data Key Exchange of Proposed Mechanism

① 단계 1

SS는 *SAID*를 이용하여 *TEK*과 관련된 키 정보를 얻기 위해 *BS*에게 식 (5)와 같은 키 요청 메시지를 전달한다.

$$E_{PU_{BS}}(SAID \| AK \text{ 일련번호}, HMAC\text{-}Digest) \quad \text{식 (5)}$$

식 (5)와 같은 *TEK* 키 요청 메시지는 *TEK* 키 갱신을 위해 주기적으로 *BS*에게 전달한다. 전달되는 키 요청 메시지에는 데이터 암호화를 위해 사용되는 *SAID*, *AK* 일련번호, *HMAC-Digest* 등이 포함된다. *SS*는 *BS*가 특정 *TEK* 키 정보를 버리거나 새로운 *TEK* 키를 요청하려고 할 때 $Life\ Time_{TEK}$ 기간동안 키를 사용한다. 만일 *TEK* 키 정보없이 *SS*가 데이터를 암호화하려고 한다면 *BS*는 사용된 키 *TEK* 키 정보를 체크한다.

② 단계 2

*BS*는 새로운 키 정보를 얻기 위해 키 응답 메시지에 *TEK* 파라미터(이전에 사용된 TEK과 새로 갱신한 TEK), SAID, HMAC-Digest 등을 식 (6)과 같이 *SS*에게 전달한다.

$$E_{PU_{SS}}(AK \text{ 일련번호} \| SAID \| HMAC\text{-}Digest \| Life\ Time_{TEK}, E_{KEK}(TEK \| Life\ Time_{TEK})) \quad \text{식 (6)}$$

*SS*에게 전달되는 식 (6)은 *TEK*과 *TEK*의 타당성을 입증하기위한 정보로써 $Life\ Time_{TEK}$동안 *SS*와 *BS* 사이에서 송·수신된다. *BS*와 *SS*가 이전에 사용한 *TEK* 키는 *BS*가 *SS*에게 전달하기 위한 데이터를 암호화할 때 사용되며 식 (6)과 같이 새로 생성된 *TEK*는 *SS*가 *BS*에게 전달할 데이터 트래픽을 암호화하기 위해 사용된다. *BS*는 키 요청 메시지를 체크한 후 *HMAC-Digest*가 타당한지와 *BS*에게 전달받은 *SAID*가 *SS*의 *SA*와 일치하는지를 검사한다. 만일 타당성이 검증받지 못하면 *SS*는 AK 일련번호, *SAID*, *HMAC-Digest*, *TEK* 파라미터 등을 다시 *BS*에게 키 요청 메시지를 통해 응답한다. 이 메시지는 *BS*가 *SS*를 신뢰할 수 있을 뿐만 아니라 메시지가 변경되지 않았는지를 보장한다.

3.4 데이터 암호화 과정

제안 메커니즘의 마지막 과정인 데이터 암호화 과정은 *SS* 권한 부여 과정과 TEK 교환 과정이 수행된 후 데이터 스트림(MAC PDU)를 암호화하여 *SS*와 *BS*사이에서 송·수신하는 과정이다. 이 과정에서는 TEK 교환 과정에서 생성된 키를 이용하여 데이터를 암호화한다. 그러나 이 과정에서 MAC 헤더는 데이터 스트림을 포함하지 않아 데이터 스트림을 직접적으로 포워드하지 못하며 데이터 스트림의 CRC 체크섬 또한 비암호화되어 있다. 데이터 스트림의 암호화 과정은 DES나 AES에 의해 수행되며 TEK 암호화는 128비트의 EDE 모드의 3DES와 128비트의 ECB 모드의 RSA와 AES를 사용한다.

Ⅳ. 평가

이 절에서는 제안 기법의 성능을 평가하기 위해 IEEE 802.16e 표준에서 지원하고 있는 알고리즘을 제안 기법에 적용하였을 때 나타나는 처리량, 이동 속도에 따른 지연시간 등과 공격 유형에 따른 보안 평가를 수행한다.

4.1 실험 환경

WiMAX 환경에서 제안 프로토콜의 타당성을 검증하기 위해 NS-2을 이용하여 실험 모델을 구현하였다.

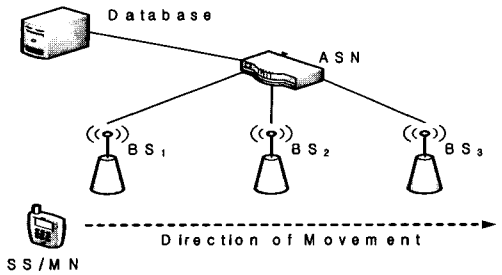

그림 5. 실험 환경
Fig 5. Experiment Environment

제안 프로토콜의 실험 환경은 그림 5와 같다. BS는 Mobile WiMAX상에서 500m 범위 내에서 SS/MN과 통신이 이루어진다. 그림 5에서 SS/MN의 최대 수는 200으로 하며 시간에 따른 패킷 지연 시간과 트래픽 처리량을 중심으로 성능 실험을 수행한다[7]. 제안 프로토콜에서 사용하는 SS/MN의 트래픽 모델은 CBR 모델을 사용한다.

4.2 성능 평가

그림 6은 WiMAX 환경에서 전송되는 서로 다른 패킷 사이즈를 IEEE 802.16e 표준에서 지원하는 AES, DES, 3DES 알고리즘을 이용하여 제안 메커니즘의 네트워크 처리량을 나타내고 있다.

그림 6에서 제안 기법에 적용된 알고리즘 중 암호 동작과정이 높은 3DES가 다른 알고리즘보다 가장 많은 네트워크 처리량을 보이고 있으며 DES가 가장 적은 처리량을 나타낸다. 그리고 AES 알고리즘은 3DES 알고리즘보다 2% 낮은 처리량을 나타내며 DES 알고리즘보다는 높은 처리량을 나타낸다.

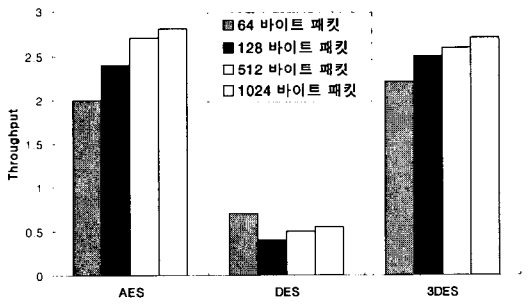

그림 6. WiMAX환경에서 알고리즘에 따른 네트워크 처리량
Fig 6. Network Throu호put through Algorithm in WiMAX Environment

그림 7는 *BS*들 사이에서 *SS*의 이동 속도에 따른 평균 이동 지연 시간을 나타낸다. 그림 4에서 평균 속도를 10km/h, 20km/h, 30km/h, 40km/h, 50km/h, 60km/h로 구분하여 실험한 결과 제안 프로토콜이 IEEE 802.16 표준보다 전체적으로 5.5% 향상되었다. 이 같은 결과는 제안 메커니즘의 *BS*에서 동작되는 성능 부하를 줄였기 때문이다.

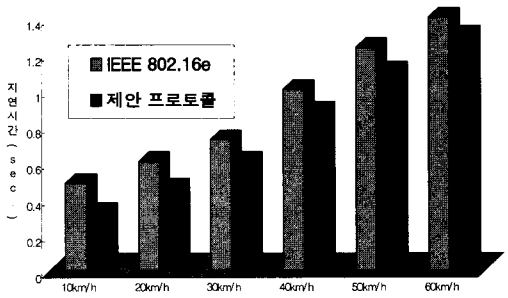

그림 7. 이동 속도에 따른 평균 지연시간
Fig 7. Average Delay Time Through Mobile Speed

4.3 보안 평가

이 절에서는 *SS*와 *BS*사이에서 동작되는 인증 구문과 키 정보 교환 구문의 안전성을 평가한다.

① SS 인증 구문과정

SS 인증 과정에서는 무선 환경에서 발생할 수 있는 Man-in-the-Middle 공격, 위조 공격, replay 공격 그리고 Dos 공격 등이 발생될 수 있다. 특히 WiMAX 환경에서는 이러한 공격들이 *SS*와 *BS* 사이에서 이루어지며 WiMAX에서 지원하는 PKMv2는 상호 인증의 보안 부족으로 인해 이러한 공격이 자주 발생된다. 제안 메커니즘의 *SS* 인증 구문에서는 *SS*와 *BS*의 상호 인증을 지원하기 위해 *SS*와 *BS* 자신이 생성한 인증서를 메시지에 포함하도록 하고 있다. 그러나 WiMAX 통신과정에서는 위조 공격과 Man-in-the-Middle 등에 의해 *BS*가 인증이 되지 않는 경우가 발생된다. 위조 공격의 경우, 공격자는 *SS*와 *BS* 사이에 위치하여 *SS*를 인증하기 위해 *SS*를 위조하고 *AK*를 *SS*에게 전달함으로써 세션을 초기화 할 수 있다. Man-in-the -Middle 공격의 경우, 공격자는 자신이 생성한 AK을 획득하여 권한 응답 메시지를 생성하고 공격한 SS의 통신과정에서 제어할 수 있다. 이러한 결과는 *SS*가 권한 구문 메시지를 신뢰할 수 있는 *BS*로부

터 생성된 것인지를 판단할 수 없기 때문이다. 제안 메커니즘에서는 이러한 문제점을 해결하기 위해 SS와 BS의 상호인증과정에서 SS와 BS 자신이 생성한 임의의 ID와 난수를 수신한다.

또한, 제안 메커니즘에서는 reply/dos 공격에 대응하기 위해 SS의 시그너처와 함께 타임스탬프의 권한 요청 메시지를 제공한다. 이렇게 추가된 파라미터들은 제안 메커니즘에서 메시지 인증을 보장하는데 사용된다. 메시지에 사용된 시그너처는 메시지 내 중요 정보를 예방하기 위해 SS의 개인키를 사용한다. BS 인증은 BS의 인증서가 권한 응답 메시지에 추가되면서 수행한다. 권한 응답 메시지내에 수신된 타임스탬프는 SS를 보장하기 위해 메시지에 추가되어야 한다. 권한 응답 메시지내 BS의 추가적인 시그너처는 초기 메시지 인증과 부인방지를 위해 사용된다.

SS와 BS의 무결성을 보장하기 위해서 제안 메커니즘에서는 SS와 BS 자신이 생성한 난수를 권한 요청 메시지와 권한 응답 메시지에 사용한다. 그러나 BS는 권한 요청 메시지가 이미 이전에 보낸 메시지인지를 판별하지 못하기 때문에 replay 공격에 노출되기 쉽다. 제안 메커니즘에서는 replay 공격에 노출되는 것을 막기 위해 BS는 pre-AK를 AK로 변경하여 SS게 보낸다. SS와 BS는 pre-AK로부터 AK를 추출할 수 있다. 제안 메커니즘에서는 pre-AK가 타협되는 것을 막기 위해 BS는 $Life\,Time_{AK}$를 생성하여 SS에게 전달하여 $Life\,Time_{AK}$는 주기적으로 갱신되기 때문에 공격자가 동일한 알고리즘으로 AK를 추출하더라도 공격자는 AK를 사용할 수 없다.

② 키 교환 구문 과정

인증 과정이 수행된 후 SS는 데이터 암호화를 위해 BS에게 키 정보(TEKs)를 요청한다. 이 정보는 주기적으로 $SAID$ 중에 하나를 참조하여 키 요청 메시지를 보낸다. 키 교환 구문 과정에서 발생할 수 있는 응답 공격은 2비트 길이를 가지는 TEK의 키 연속 변호에 의해 가능하다. 연속적인 번호는 키 응답 메시지내의 TEK 파라미터에 포함된다. 제안 메커니즘에서 이러한 공격을 예방하기 위해 키 교환 과정에 $Life\,Time_{AK}$를 포함하여 공격자가 TEK 메시지를 캡처하여 데이터 트래픽을 복호화하기 위해 필요한 정보를 획득할 수 있는 시간을 제한하고 있다.

V. 결 론

WiMAX는 X.509 인증서, SA, 암호방법, Encapsulation 프로토콜과 같은 서로 다른 구성요소를 사용하여 무선 전송을 안전하게 하는 보안 구조를 제공한다. 그러나 무선 환경에서 이루어지는 인증과 키 교환 구문에는 몇몇 보안 취약점을 내포하고 있다. 이 논문에서는 IEEE 802.16e 표준에서 제공하는 기본 보안 기능이외에 SS의 인증 부하를 줄이면서 무선 환경에서 발생하는 보안공격(reply 공격과 man-in-the-middle 공격)에 안전한 보안 메커니즘을 제안했다. 제안된 메커니즘은 SS와 BS가 생성한 난수와 비밀값을 이용하여 TEK과 데이터 암호에 필요한 키 정보를 교환하고 SS의 초기 인증정보와 인증서를 이용하여 BS의 추가 인증 과정을 제거하여 BS의 성능 부하를 줄였다. 향후 연구에서는 무선 환경에서 발생할 수 있는 여러 보안 공격에 안전한 보안 구조 및 정책 연구를 수행할 계획이다.

참고문헌

[1] X. Sen, M. Maqtthews, H. Chin-Tser, "Security Issues in Pricacy and Key Management protocols of IEEE 802.16", Department of Computer Science and Engineering - University of Sourth Carolina Columbia, SC 29208, USA:www.cse.sc.edu/~huanget/acmse06cr.pdf#search=%22acmse06cr.pdf%22.

[2] S. Wattanachai, "Security Architecture of the IEEE 802.16 Standard for Mesh Networks", Department of computer and Systems Sciences Stockholm University/Royal Institute of Technology, 2006: www.dsv.su.se/research/seclab/pages/pdf-files/2006-x-360.pdf#search=%222006-x-360.pdf%22.

[3] A. Arkou야-Vafea, "Security of IEEE 802.16. Master of Information and Communication Systems Security" Department of Computer and Systems - Science Royal Institute of Technology, 2006: www.dsv.su.se/research/seclab/pages/pdf-files/2006-x-332.pdf.

[4] D. Johnston, J. Walker, "Overview of IEEE 802.16 Security", Published by IEEE Computer Society, 2004:mia.ece.uic.edu/~pages/WWW/Bubbles/segment

/WiMax_Security.pdf#search=%22WiMax_Security.pdf%22.

[5] M. Barbeau, "WiMAX/802.16 Threat Analysis", School of Computer Science Carleton University 1125 Colonel By Drive. Ottawa, Ontario, Canada, 2005 www.scs. carleton.ca/~barbeau/Publications/2005/iq2-barbeau.pdf#search=%22iq2-barbeau.pdf%22.

[6] Frank Ohrtmann: Wimax Handbook. Building 802.16 Wireless Networks - McGraw-Hill Communicaitons, 2005.

[7] WiMAX Forum(2006) : Mobile WiMAX: The Best Personal Broadband Experience.

[8] J. Bellardo and S. savage, "802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions", Presented at 11th USENIX Security Symposium, 2003.

[9] M. Barbeau, "WiMAX/802.16 threat analysis", in Proceedings of ACM Q2SWinet'05, Montreal, Quebec, Canada, Oct 13, 2005.

[10] D. Gollmann, Computer Security(2nd ed.), West Sussex, Wiley, 2006.

[11] M. Schumacher, E. B. Fernandez, D. Hybertson, F. Buschmann, and P. Sommerlad, "Security Patterns: Integrating Security and Systems Engineering", Wiley, Chichester, W. Sussex, England, 2006.

[12] E. Yang, H. Zhou, L.Zhang, and J. Feng, "An improved security scheme in WMAN based on IEEE Standard 802.16", Wireless Communication, Networking and Mobile Computing, Vol. 2, pp. 1191-1194, Sep. 2005.

저자소개

정 윤 수 (Yoon-Su Jeong)

1998. 청주대학교 전자계산학과 학사
2000. 충북대학교 대학원 전자계산학과 석사
2008. 충북대학교 대학원 전자계산학과 박사
2008.3 ~ 현재 충북대 및 한남대 시간강사
※관심분야 : 센서 보안, 암호이론, 정보보호, Network Security, 이동통신보안

김 용 태 (Yong-Tae Kim)

1984. 한남대학교 계산통계학과 학사.
1988. 숭실대학교 전자계산학과 석사.
1995. 충북대학교 전산학과 박사수료.
2002. 12. ~2005.2 (주)가림정보기술 이사
2006.3 ~ 현재 한남대학교 멀티미디어 학부 강의전담교수
※관심분야 : 멀티미디어, 모바일 웹서비스, Real-time Multimedia Communication

박 길 철 (Gil-Cheol Park)

1983. 한남대학교 전자계산학과 학사.
1986. 숭실대학교 전자계산학과 석사.
1998. 성균관대학교 전자계산학과 박사.
2006. UTAS, Australia 교환교수
1998. 8. ~ 현재 한남대학교 멀티미디어학부 교수
2005. 2. 한국정보기술학회 이사 멀티미디어 분과 위원장
※관심분야 : multimedia and mobile communication, network security

이 상 호 (Sang-Ho Lee)

1976. 숭실대학교 전자계산학과 학사.
1981. 숭실대학교 전자계산학과 석사.
1989. 숭실대학교 전자계산학과 박사.
1981. 3. ~ 현재 충북대학교 전기전자 컴퓨터공학부 교수
※관심분야 : 네트워크보안, Protocol Engineering Network Management,