DOI: 10.3745/KIPSTC.2009.16-C.2.257

WiMAX 초기 인증을 향상시킨 경량화된 PKM 상호 인증 프로토콜

정 윤 수[†] · 김 용 태[††] · 박 길 철[†††] · 이 상 호[††††]

요 약

최근 노트북, PDA와 같은 이동 단말기의 사용이 일반화되면서 고속 인터넷 서비스에 대한 요구가 점차 증가하고 있지만 IEEE 802.16e에서 제공하는 PKMv2만으로는 고속 인터넷 서비스의 완전한 보안을 제공하지 못하고 있다. 이 논문에서는 WiMAX 환경에서 동작되는 노드들의 안전한 고속 데이터 전송을 지원하기 위하여 PKMv2를 경량화한 상호 인증 프로토콜을 제안한다. 제안된 상호 인증 프로토콜은 네트워크내 사용자가 초기 인증을 수행한 후 네트워크 내에서 가입자와 베이스 스테이션 사이의 추가적인 인증과정을 수행하지 않고 안전하게 네트워크 내에서 통신할 수 있도록 하여 효율성을 향상시켰다. 또한 제안된 상호 인증 프로토콜에서는 인증서를 보호하기 위해서 노드 자신이 생성한 난수와 비밀값을 PRF() 함수에 적용하여 키를 생성함으로써 가입자와 베이스 스테이션 사이의 내부 공격(man-in-the-middle 공격과 reply 공격)에 안전성을 보장하고 있다.

키워드 : 와이맥스, 상호인증, PKM, 보안 공격

A Light-weight PKM Mutual Authentication Protocol for Improving Initial Authentication in WiMAX

Jeong Yoon Su[†] · Kim Yong Tae[††] · Park Gil Cheol[†††] · Lee Sang Ho[††††]

ABSTRACT

Now a days, as increased the use of mobile units like a laptop computer and PDA, the demand for high speed internet service is increasing. On the other hand, PKMv2 which is provided from IEEE 802.16e cannot support fully on the security of high speed internet service. This paper proposes light-weight mutual authentication protocol which solved security problem of PKMv2 related to integrity of mobile node for transmission of safe high speed data of mobile node operating in mobile WiMAX environment. Proposed mutual authentication protocol increases the efficiency as the user in network can move in network safely without additional procedure of authentication between subscriber and base station after user's initial authentication. Also, the proposed mutual authentication protocol is safe from the security attack (the man-in-the-middle attack and reply attack) between subscriber and base station by generating a key adopt to PRF() function using random number and secret value in order to secure certification.

Keywords : WiMAX, Mutual Authentication, PKM, Security Attack

1. 서 론

최근 노트북, PDA와 같은 이동 단말기의 사용이 일반화되면서 인터넷 기반의 다양한 서비스와 애플리케이션의 요구가 점차 증가하고 있다. 이와 같은 추세에 맞추어 IEEE 802.16 워킹 그룹은 저속 이동성과 사용자들의 요구를 충족시키기 위한 IEEE 802.16 표준안을 2004년에 제정한 후 고속 이동성, 보안 기능 등이 보완된 IEEE 802.16e-2005 표준을 개정하였다[1,2].

IEEE 802.16e 표준안이 2005년에 제정된 이후 IEEE 802.16e 기반에서 발생할 수 있는 보안 취약성 및 공격 가능성에 대한 많은 연구가 진행되었다[3,4,5]. IEEE 802.16e 표준을 기반으로 하는 이동 WiMAX(World wide Interoperability for Microwave Access)는 이동성을 지원하지 않는 IEEE 802.16 표준에 비하여 다양한 보안 기능을 지원하고 있으며 IEEE 802.16 표준과 IEEE 802.16e 표준을 모두 지원하는 PKMv1 (Privacy Key Management version 1)은 기본적인 키 관리 기능뿐 아니라 EAP 기반의 인증과 트래픽 암호화 등의 기

※ 본 연구는 지식경제부 지역혁신센터 사업인 민군겸용 보안공학 연구센터 지원으로 수행되었음
† 정 회 원 : 충북대학교 전자계산학과 박사
†† 정 회 원 : 한남대학교 멀티미디어학부 강의전담교수(교신저자)
††† 종신회원 : 한남대학교 멀티미디어학부 교수
†††† 종신회원 : 충북대학교 전기전자컴퓨터공학부 교수
논문접수 : 2008년 9월 3일
수 정 일 : 1차 2008년 11월 18일, 2차 2008년 12월 22일
심사완료 : 2009년 1월 3일

능을 가진다[4,6,7]. 그러나 PKMv1은 단방향 인증방식 문제, 재연공격 문제, DES 암호 알고리즘 문제 그리고 인증키 전송문제 등의 단점을 가지고 있다.

PKMv1의 문제점들을 개선하기 위해 PKMv2에서는 기지국과 단말 사이의 인증을 양방향으로 동작하는 상호 인증을 지원하고 있다. 이동 WiMAX 시스템에서는 가입자(Subscriber)의 이동성을 지원하지만 고정된 WiMAX 환경보다 이동 가입자가 네트워크에 진입할 때 더 큰 보안 문제가 발생되며, IEEE 802.16e에서 제공하는 PKMv2만을 이용해서는 이러한 보안 문제를 완전하게 해결하지 못하고 있다. 또한 PKMv2는 양방향 상호 인증을 통해 수행되는 인증 키 교환과정 중에서 Key-Request/Reply 교환 절차 과정에서 대역폭(bandwidth) 요청 코드가 충돌되는 것과 기지국과 여러 단만들 사이에 PKMv2 Key-Request/Reply 메시지를 교환하기 위한 불필요한 처리 시간이 소요되는 문제점이 발생한다[3,4]. 이러한 문제는 베이스 스테이션이 EAP 프로토콜에서 사용하는 필드 AAA-key를 사용하지 않고 MS가 EAP 전송 메시지(EAP-TLS에서 사용된 AP Success)를 수신했을 경우에 EAP 기반 권한 처리과정의 완벽한 시간을 알지 못하기 때문에 발생된다.

이 논문에서는 WiMAX 시스템에 초기 진입하려고 시도하는 노드들의 인증 부하를 줄이면서 무선 환경에서 발생하는 내부공격에 대해 안전한 경량화된 상호 인증 프로토콜을 제안한다. 제안된 상호 인증 프로토콜은 802.16 표준에서 제공하는 PKMv2의 양방향 상호인증을 향상시키기 위해 난수와 비밀값을 이용하여 인증서 내의 정보를 추출할 수 있도록 네트워크내 가입자와 베이스 스테이션 사이에서 초기 인증을 수행한다. 이때 기지국과 여러 단만들 사이에서 송·수신되는 Key-Request/Reply 메시지들의 불필요한 처리시간을 줄이기 위해서 제안 프로토콜은 가입자의 초기 인증정보와 인증서를 그대로 이용하여 WiMAX 시스템에 재접속하는 가입자가 베이스 스테이션과의 추가적인 인증 과정을 수행하지 않도록 하면서 WiMAX 서비스를 지원받기 위한 통신을 지원 받을 수 있도록 한다.

이 논문의 구성은 다음과 같다. 2장에서는 IEEE 802.16 표준과 WiMAX 보안에 대해서 분석한다. 3장에서는 WiMAX 환경에서 가입자와 베이스 스테이션간 안전한 통신을 제공하는 상호인증 프로토콜을 제시하고, 4장에서는 제안 프로토콜에 대한 효율성 및 안전성에 대하여 분석·평가한다. 마지막으로 5장에서는 이 연구의 결과를 요약하고 향후 연구에 대한 방향을 제시한다.

2. 관련연구

2.1 IEEE 802.16 표준

802.16 표준은 강력한 보안성을 가지고 있으며 음성이나 영상에 요구되는 QoS를 보장해준다[3]. IEEE 802.16a는 IEEE 802.16의 확장으로 2003년 1월에 완성되었으며. 이 표준은 2GHz에서 11GHz 사이의 밴드이고 LOS(Line-of-Sight)가 필요없고 point-to-multipoint 어플리케이션으로 DSL과 케이블 모뎀의 경쟁 관계에 있다. WiMAX는 75 Mbps까지 구현 가능하고 일반적인 4~6 마일(miles)의 셀 반경에서 30마일까지 커버가 가능하다. 하지만 최대 반경이 송신탑의 높이나 안테나 이동 그리고 전송 파워에 많은 영향을 받는다. IEEE 802.16a는 20MHz의 대역폭을 제공하는데 T1 수준의 60배 정도와 DLS의 100배 정도를 커버할 수 있다[8]. IEEE 802.16e는 현재 표준에 이동성의 특징을 부가하여 mobile air interfaces를 구현하고 이것은 PDA 같은 작은 단말기를 휴대하고 이동하며 무선 인터넷에 접속이 가능하도록 한다. 802.16e 표준은 1~3마일의 서비스 지역에 노트북이나 PDA같은 휴대용 기기들을 위한 로밍기능을 지원하고 있다. <표 1>은 802.16 시리즈의 여러 표준들(802.16, 802.16a, 802.16d, 802.16e)의 완성일, 채널상태, 주파수, 대역폭, 전송범위, 이동성 등의 특징 및 기능들을 비교하고 있다.

2.2 PKM 프로토콜

PKM 프로토콜은 기지국과 단말 사이에서 EAP 메시지를 전달하기 위해 사용되고 있으며, 초기에 제안된 PKMv1은 여러 가지 보안 문제점이 발견되어 현재는 PKMv2로 개정된 상황이다[4]. PKMv1은 단말이 망에 접속할 때 단말 자신의 MAC 주소 및 RSA 기반 공개키가 결합된 X.509 인증서를 사용한다. PKMv1의 문제점으로는 기지국이 단말을 인증하지만 단말이 기지국을 인증하지 않는 단방향 인증방식 문제, 정상적인 사용자와 기지국이 암호화된 통신을 하더라도

〈표 1〉 802.16 표준

표 준(Standard)	802.16	802.16a	802.16d	802.16e
완성일 (Completed)	Dec. 2001	Jan. 2003	Q3. 2004	Mid 2005
채널 상태 (Channel Conditions)	Line-of-sight Only	Non Line-of-sight	Non Line-of-sight	Non Line-of-sight
주파수 (Frequency)	10-66 GHz	Sub 11GHz	Sub 11GHz	2-6GHz
대역폭 (Throughput)	Up to 134Mbps (28MHz BW)	Up to75Mbps (20MHz BW)	Up to 75Mbps (20MHz BW)	Up to 30Mbps (10MHz BW)
전송범위 (Range)	Typical 1-3 miles	Typical 4-6 miles	Typical 4-6 miles	Typical 1-3 miles
이동성 (Mobility)	Fixed	Fixed	Fixed, Portable	Mobility, Regional roaming

통신내역을 캡처해 재전송하는 재연공격 문제, 전수공격에 의해 데이터가 노출될 수 있는 DES 암호 알고리즘 문제, 암호화되어 인증키가 직접 전송하는 인증키 전송 문제 등이 있다. PKMv2에서는 PKMv1의 문제점을 개선하기 위해 기지국과 단말 사이의 인증을 양방향 인증하는 방식을 사용하고 있다. PKMv2에서는 악의적인 공격자가 허위의 기지국으로 위장하는 것을 막을 수 있으며 인증 및 키 교환 단계에서 단말과 기지국은 난수를 생성하고 데이터에 포함시켜 통신하기 때문에 같은 통신내용이 전송될 확률이 낮아져 재연공격이 발생하기 어렵다. <표 2>는 PKMv1과 PKMv2를 인증속성, 인증방식, 인증내용, 인증키 교환, TEK 암호화, 데이터 암호화, 데이터 무결성 등의 속성으로 비교한 표이다[14].

PKM 프로토콜은 상위 인증 프로토콜인 EAP를 사용하여 기지국과 해당 단말 간에 인증키를 교환하는데 사용되며, 교환된 인증키는 패킷 데이터를 암호화하기 위한 트래픽 암호화키를 생성하는데 사용된다. 단말은 PKM 프로토콜을 사용하여 기지국으로부터 권한 검증 및 트래픽 키 정보등을 얻고 주기적인 재인증과 새로운 트래픽 암호화 키 정보들을 요청한다. MAC의 암호화 부계층의 암호화 프로토콜에서는 EAP-TLS 인증 프로토콜을 단말과 기지국 사이에 전달하기 위해 사용된다.

2004년 IEEE 802.16 표준이 발표된 이후 WiMAX 환경에서 발생 가능한 보안 문제점을 해결하기 위해서 PKMv1의 보안기능을 향상시킨 PKMv2 프로토콜을 사용하고 있지만 인증 키 교환과정 중에서 Key-Request/Reply 교환 절차를 통해 몇가지 문제점이 발생된다. 첫째는 단말들이 PKMv2 Key-Request 메시지를 전송하기 위해 사용되는 대역폭(bandwidth) 요청 코드가 충돌될 수 있는 문제점이고 둘째는 기지국과 여러 단말들 사이에 PKMv2 Key-Request/Reply 메시지를 교환하기 위한 불필요한 처리 시간이 소요되는 문제점이다. 이러한 PKMv2의 Key-Request/Reply 교환 절차의 문제점을 해결하기 위해서는 초기 인증 절차를 통해 인증된 인증 정보를 멀티캐스트 서비스, 브로드캐스트 서비스 또는 MBS(Multicast service, Broadcast Service)등에서 효율적인 그룹 트래픽 암호화 키 갱신 방법을 제공할 수 있어야 한다.

2.2.1 PKMv1 보안 분석

PKMv1은 동작과정에 따라 단방향 인증방식, 재연공격, 암호 알고리즘 그리고 인증키 전송 등에서 보안 분석을 해보면 다음과 같다. 첫째, PKMv1에서는 기지국이 단말을 인증하지만, 단말이 기지국을 인증하지 않는 단방향 인증 방식을 사용하기 때문에 악의적인 공격자가 허위의 기지국을 정상적인 기지국으로 위장할 수 있다. 이때, 정상적인 단말이 접속요청을 하면 공격자가 생성한 임의의 인증키를 단말에 주고, 단말은 공격자를 통해 인터넷을 사용하고 공격자는 단말의 모든 트래픽을 도청하거나 데이터를 위·변조할 수 있다(단방향 인증방식). 둘째, 정상적인 사용자와 기지국이 암호화된 통신을 하더라도 공격자가 통신 내용을 캡처해 재전송하는 재연공격이 발생될 수 있다(재연공격). 셋째, PKMv1에서는 데이터 암호화를 위해 56bit DES 알고리즘을 사용하지만 DES 알고리즘은 전수공격에 의해 데이터가 노출될 수 있는 문제점이 있다(암호 알고리즘). 넷째, PKMv1에서 사용되는 인증키는 암호화되어 직접 단말에 전송지만 인증키로부터 데이터 암호화, 무결성 키가 생성되므로 인증키가 노출되면 큰 위협이 되는 문제점이 있다(인증키 전송).

2.2.2 PKMv2 보안 분석

PKMv2는 RSA 기반 인증방식과 EAP(Extensible Authe_ntication Protocol) 기반 인증방식을 지원한다. PKMv2 RSA 기반 인증방식은 PKMv1과 같은 RSA 기반의 공개키와 단말의 MAC 주소를 결합한 X.509 인증서를 사용하지만 기지국도 단말에 인증서를 제공하는 양방향 인증방식을 사용하며, 인증 시 메시지 무결성 보장을 위해 전자서명이 포함되고, 재연공격을 방지하기 위한 난수 등이 추가돼 PKMv1에서 예상됐던 취약성을 개선했다. 그러나 RSA 기반 인증방

〈표 2〉 PKMv1과 PKMv2 비교

구 분	PKMv1	PKMv2
인증 속성	-단방향 인증	-양방향 인증
인증 방식	-RSA 기반 인증	-RSA기반 인증 -EAP 기반 인증
인증 내용	-단말 인증	-단말/사용자 인증
인증키 교환	-기지국은 단말의 공개키로 암호화해 인증키를 직접 분배	-RSA 기반 : 기지국은 pre-PAK을 단말의 공개키로 암호화해 분배하고, pre-PAK으로부터 단말과 기지국은 인증키 자체 생성 -EAP 기반 : 인증서버는 AAA-key를 단말에 분배하고 AAA-key로부터 단말, 인증서버는 인증키 자체생성
TEK 암호화	-3DES	-3DES-EDE, RSA -AES-EBC/KEY-WRAP
데이터 암호화	-No Encryption -DES	-No Encryption -DES-CBC, 3DES, RSA -AES-CCM/CBC/CTR
데이터 무결성	-No MAC, HMAC	-No MAC, HMAC/CMAC

식은 권한처리과정에서 다음과 같은 문제점이 존재한다. 첫째, RSA 기반 권한 처리과정에서 권한 요청 메시지와 권한 응답 메시지는 EAP 기반 권한 처리과정의 EAP 전송 메시지와 동일한 등급을 가진다. 또한, 권한 요청/응답 메시지는 보안 자격, SAID, SA 명세서를 얻을 수 있지만 전송 메시지에서는 이러한 파라미터를 얻을 수 없다. 둘째, RSA 기반 권한 처리과정에 포함된 sequence 번호와 라임프타임은 AK sequence 번호와 AK 라이프타임이 아니다. 셋째, RSA 기반 권한 처리과정이 선택되었을 때 BS에서 MS로 MS의 인증 실패와 MS로부터 success/reject와 같은 BS의 인증 결과를 알리기 위한 메시지가 존재하지 않는다.

PKMv2 EAP 기반 인증방식은 IEEE802.1x 포트 기반의 가입자 인증 데이터 전송을 위한 표준 프로토콜로, EAP-MD5, EAP-TLS, EAP-AKA(Authentication and Key Agreement) 등 다양한 인증 프로토콜을 사용할 수 있으며, 사용자 인증 및 단말, 그리고 네트워크간 상호인증이 가능하다. 또한 AAA 인증 서버를 통해 인증을 수행하기 때문에 사용자가 증가해도 기지국에 오버헤드가 생기지 않는다는 장점이 있다. 그러나 EAP 기반 인증방식은 EAP 기반 권한처리 과정에서 다음과 같은 문제점이 있다. 첫째, 인증된 EAP 전송 메시지에서 사용된 키 연속 번호는 AK 연속 번호와 일치하지 않는다. 둘째, 베이스 스테이션은 EAP 프로토콜이 필드 AAA-key를 수행하지 않고 가입자가 EAP 전송 메시지(EAP-TLS에서 사용된 AP Success)를 수신했을 경우에 EAP 기반 권한 처리과정의 완벽한 시간을 알지 못한다. 베이스 스테이션과 가입자는 가입자가 이전 EAP전송 메시지를 수신하지 못했을 때 쌍마스터키(PMK)로부터 도출된 AK을 동시에 공유할 수 없기 때문이다.

2.3 WiMAX와 보안

WiMAX는 Wi-Fi의 한계로 지적되어온 제한된 커버리지 영역(AP(Acce가입자 Point)당 약 30~200m 이내)과 전송 속도 개선, HotZone 내에서의 끊임없는 연결(seamless connection)을 통한 이동성 확보 등의 문제를 해결하기 위해 개발된 무선 광대역 접속 기술이다[9,10]. WiMAX 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 기기간의 무선 통신에 활용되며, 백홀 네트워킹(backhaul networking)에도 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.

이동 WiMAX라는 이름으로 알려져 있는 802.16e 표준은 802.16-2004에 비해 이동성 문제를 개선하여 이동 중에도 최대 15Mbps의 속도로 데이터의 송·수신이 가능하다[11]. 이동 WiMAX는 셀간 이동을 원활하게 하는 핸드오프 기능을 지원하고, 지연(latency)을 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[12,13].

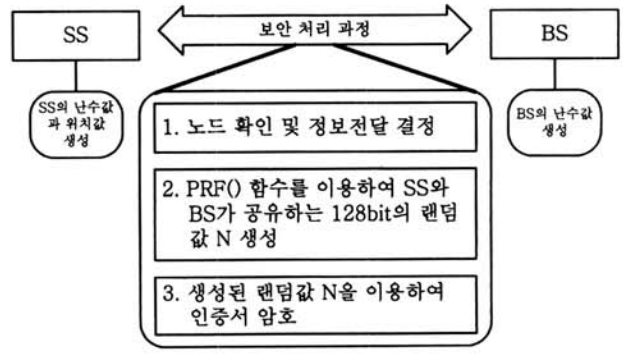
3. 경량화된 PKM 상호 인증 프로토콜

이 절에서는 IEEE 802.16e 표준에서 제공하는 PKMv2의 대역폭 요청 코드 충돌 문제와 Key-Request/Reply 교환 절차의 불필요한 처리시간 문제를 해결하기 위해서 인증된 인증정보를 노드 자신이 생성한 난수를 사용한다. Key-Request/Reply 교환 절차의 불필요한 처리시간 문제는 베이스 스테이션이 EAP 프로토콜에서 사용하는 필드 AAA-key를 수행하지 않아 가입자가 EAP 전송 메시지를 수신했을 경우에 EAP 기반 권한 처리과정의 완벽한 시간을 알지 못해서 베이스 스테이션과 가입자가 쌍마스터키(PMK)로부터 도출된 AK를 동시에 공유할 수 없게 때문에 제안 프로토콜에서는 초기 인증 과정이 끝난 후 가입자가 일정 시간이 지난 후에 WiMAX 시스템에 재접속할 경우 가입자는 초기 인증정보와 인증서를 이용하여 베이스 스테이션과의 추가적인 인증 과정을 수행하지 않고 WiMAX 서비스를 지원받기 위한 통신을 지원 받을 수 있도록 한다.

3.1 개요

제안된 상호 인증 프로토콜은 가입자와 베이스 스테이션 사이의 경량화된 상호 인증 프로토콜을 보장하기 위해 노드 자신이 생성한 난수 값을 PRF() 함수에 적용하여 키를 생성한 후 생성된 키를 이용하여 인증서를 암호화한다.

제안 프로토콜의 전체 동작과정은 (그림 1)와 같다. (그림 1)의 보안처리 과정은 크게 3단계로 나누어진다. 1단계에서는 베이스 스테이션이 가입자를 확인하고 정보 전달을 결정하는 단계이며 2단계는 PRF() 함수를 이용하여 가입자와 베이스 스테이션이 공유하는 128 비트의 랜덤 값 N을 생성하는 단계이다. 마지막 3단계에서는 생성된 랜덤 값 N을 이용하여 베이스 스테이션과 가입자가 사용하는 인증서를 암



(그림 1) 제안 프로토콜의 전체 동작과정

호화한다. (그림 1)의 동작과정에서 가입자와 베이스 스테이션은 사전에 자신이 생성한 난수값을 생성하고 가입자는 자신의 위치값을 이용하여 베이스 스테이션에 등록하게 된다. 이 때, 가입자와 베이스 스테이션사이에서 송·수신되는 메시지는 PRF()함수를 통해 생성된 128bit 크기의 랜덤값을 이용하여 인증서를 암호화하여 상호인증을 수행할 수 있도록 한다. (그림 1)의 과정을 통해 제안 프로토콜은 무선 구간에서 발생할 수 있는 reply 공격과 man-in-the-middle 공격과 같은 공격에 안전하며 기존 공개키 암호방법에 비해 경량화된 계산이 가능하다.

3.2 용어정의

제안 프로토콜에서 사용하는 주요 용어를 정의하면 (표 3)와 같다.

3.3 가입자의 현재 위치 파악

제안 프로토콜의 초기 인증 과정을 수행하기 전에 가입자가 베이스 스테이션과 통신이 가능한 지를 파악하기 위해서 베이스 스테이션은 네트워크에 진입한 가입자에게 통신이 가능한지 주기적인 시간 간격을 통해 확인한다. 이러한 과정이 제안 프로토콜에서 필요한 이유는 제안 프로토콜이 위치기반 서비스(LBS, Location-Based Service)를 지원하는 이동 WiMAX 환경에서 동작하기 때문이다. 베이스 스테이션이 네트워크 범위내에 가입자가 존재하는지를 파악한 후에는 베이스 스테이션이 가입자의 위치 정보 D_{SS}를 요청하게 된다. 가입자의 위치 정보 D_{SS}는 초기 인증 과정에서 사용되는 메시지에 포함되며 이 정보를 통해 베이스 스테이션은 가입자의 현재 위치 정보를 파악할 수 있다. 가입자의 위치정보 D_{SS}에는 가입자의 인식정보, 가입자의 현재 위치 정보, 현재 소속된 베이스 스테이션의 정보, 가입자가 통신하고자 하는 베이스 스테이션의 네트워크 진입여부 정보 등이 포함된다.

〈표 3〉 파라미터

용어(Notaion)	설명(Definitions)
SS	가입자(Subscriber Station)
BS	베이스 스테이션(Base Station)
$E_{PU_A}(X)$	A의 공개키를 가고 X를 암호화
$S_{PR_A}(X)$	A의 개인키를 통해 메시지 X에 대한 시그너처 생성
D_{SS}	가입자의 위치정보
$Cert_x$	x의 인증서
ID_{SS}	가입자의 인식자
ID_{BS}	베이스 스테이션의 인식자
N_{SS}	가입자가 생성한 난수
N_{BS}	베이스 스테이션가 생성한 난수
K_{SS-BS}	가입자와 베이스 스테이션이 공유한 공유키
$prf()$	pseudo 랜덤 함수
$M_1 \| M_2$	M_1과 M_2의 연접(Concatenation)

3.4 초기 인증 프로토콜

이 절에서는 가입자가 네트워크에 진입할 경우 가입자의 인증을 위한 초기 인증 프로토콜을 제안하고 있다. 제안된 상호 인증 프로토콜은 네트워크내 사용자가 초기 인증을 수행한 후 네트워크 내에서 가입자와 베이스 스테이션 사이의 추가적인 인증과정을 수행하지 않고 안전하게 네트워크 내에서 통신할 수 있도록 하여 베이스 스테이션과 가입자가 쌍마스터키(PMK)로부터 도출된 AK를 동시에 공유할 수 있도록 하였으며, (그림 2)처럼 네트워크에 진입한 가입자와 베이스 스테이션 사이의 초기 인증 처리 과정을 12단계로 구분하였다. (그림 2)의 각 단계별 동작과정 및 특징들을 살펴보면 다음과 같다.

① 단계 1

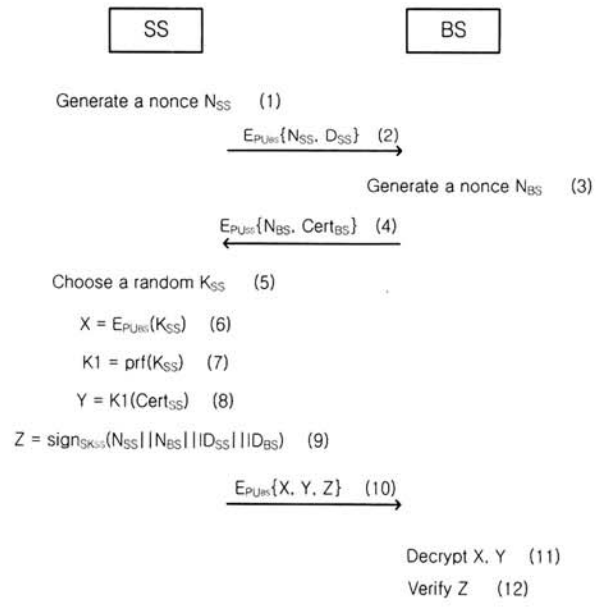
단계 1에서는 베이스 스테이션이 관리하는 네트워크에 가입자가 진입하게 되면 가입자는 replay 공격을 예방하기 위해 가입자 자신이 생성한 난수 N_{SS}을 먼저 생성한다.

$$\text{가입자 : Choose a nonce } N_{SS} \qquad \text{(식 1)}$$

② 단계 2

단계 2에서는 가입자가 생성한 난수 N_{SS}와 도메인 정보 D_{SS}를 베이스 스테이션의 공개키로 암호화한 후 베이스 스테이션에게 전달한다. 이 때, 도메인 정보 D_{SS}는 베이스 스테이션이 가입자의 도메인을 결정짓는 중요한 정보이며 가입자를 식별할 수 있는 식별자를 포함하고 있다. 이 정보는 베이스 스테이션이 도메인 정보 D_{SS}를 이용하여 이동 가입자와 고정 가입자를 구분짓고 이동 가입자의 이동성을 보장해 주는 역할을 한다.

$$\text{가입자} \rightarrow \text{베이스 스테이션} : E_{PU_{BS}}\{N_{SS}, D_{SS}\} \qquad \text{(식 2)}$$



(그림 2) 가입자와 베이스 스테이션 사이의 초기 인증 프로토콜

③ 단계 3

단계 3에서 베이스 스테이션은 수신한 도메인 정보 D_{SS}을 이용하여 서명된 공개키 인증서를 추출한다. 만약 도메인 정보 D_{SS}을 이용하여 가입자의 인증서 $Cert_{SS}$를 추출할 수 없다면 인증 프로토콜은 바로 종료하게 된다. 만약 베이스 스테이션이 가입자의 인증서 $Cert_{SS}$를 추출한다면 베이스 스테이션은 베이스 스테이션 자신이 생성한 난수 N_{BS}를 생성한다.

베이스 스테이션 : Check D_{SS} and Choose a nonce N_{BS} (식 3)

④ 단계 4

단계 4에서는 베이스 스테이션 자신이 생성한 난수 N_{BS}와 인증서 $Cert_{BS}$를 가입자에게 전달하기 위해서 가입자의 공개키를 이용하여 암호화한다.

가입자 ← 베이스 스테이션 : $E_{PU_{SS}}\{N_{BS}, Cert_{BS}\}$ (식 4)

⑤ 단계 5

단계 5에서 가입자는 베이스 스테이션의 공개키를 이용하여 베이스 스테이션에게 전달받은 N_{BS}와 $Cert_{BS}$을 검증한다. 검증이 완료되면 가입자는 자신이 생성한 임의의 키 K_{SS}을 선택한다.

가입자 : Choose a random K_{SS} (식 5)

⑥ 단계 6

단계 6에서 가입자는 베이스 스테이션 BS에게 전달받은 인증서 $Cert_{BS}$내에 포함된 베이스 스테이션의 공개키 PU_{BS} 정보를 사용하여 가입자가 임의로 생성한 키 K_{SS}을 암호화한 후 X 값으로 치환한다.

가입자 : $X = E_{PU_{BS}}(K_{SS})$ (식 6)

⑦ 단계 7

단계 7에서 가입자는 단계 5에서 생성한 키 K_{SS}를 $pseudo$ 랜덤 함수 $prf()$에 적용한 후 그 결과값을 $K1$으로 치환한다.

가입자 : $K1 = prf(K_{SS})$ (식 7)

⑧ 단계 8

단계 8에서 가입자는 $K1$을 이용하여 가입자의 인증서 $Cert_{SS}$을 암호화한 후 Y 값으로 치환한다. 특히, 이 단계에서 사용되는 $K1$은 가입자가 생성한 키 K_{SS} 대신 $AES-128$과 같은 대칭 암호를 통해 인증서 $Cert_{SS}$을 암호화한다.

가입자 : $Y = K1(Cert_{SS})$ (식 8)

⑨ 단계 9

단계 9에서 가입자는 가입자 자신의 개인키 SK_{SS}을 사용하여 메시지 $N_{SS}||N_{BS}||ID_{SS}||ID_{BS}$을 서명한 후 Z값으로 치환한다. 서명된 값에 사용된 파라미터 중 ID_{SS}와 ID_{BS}는 가입자와 베이스 스테이션을 구분짓는 인식자로 사용되며 || 는 메시지 간의 연접을 의미한다. 단계 9에서 가입자와 베이스 스테이션의 인식자를 난수(N_{SS},N_{BS})와 같이 연접하는 이유는 가입자와 베이스 스테이션사이에서 발생하기 쉬운 replay 공격을 예방하기 위해서이다.

가입자 : $Z = sign_{SK_{SS}}(N_{SS}||N_{BS}||ID_{SS}||ID_{BS})$ (식 9)

⑩ 단계 10

단계 10에서 가입자는 자신이 생성한 X, Y, Z를 베이스 스테이션의 공개키 PU_{BS}로 암호화하여 베이스 스테이션에게 전달한다. 이 때, 공격자가 전달되는 정보를 가로채기 하더라도 가입자와 베이스 스테이션이 생성한 일회성 난수(N_{SS}, N_{BS})를 공격자가 알지 못하기 때문에 가로채기 공격에 안전할 수 있다.

가입자 → 베이스 스테이션 : $E_{PU_{BS}}$(X, Y, Z) (식 10)

⑪ 단계 11

단계 11에서 베이스 스테이션은 가입자가 전달한 정보를 베이스 스테이션의 개인키 PR_{BS}를 이용하여 복호한 한 후 X 정보에서 자신의 개인키 SK_{BS}를 사용하여 비밀키 K_{SS}을 복호화한다. 베이스 스테이션은 비밀키 K_{SS}를 복호화한 후 비밀키 K_{SS}를 $pseudo$ 랜덤 함수 $prf()$에 적용하여 가입자의 인증서를 복호화하기 위한 $K1$을 생성한다.

베이스 스테이션 : Decrypt X, Y (식 11)

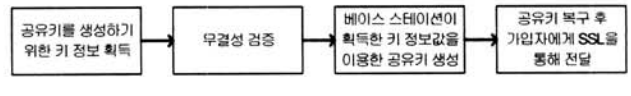
⑫ 단계 12

단계 12에서 베이스 스테이션은 자신의 공개키를 이용하여 가입자를 인증한 후 서명 $sign_{SK_{SS}}(N_{SS}||N_{BS}||ID_{SS}||ID_{BS})$을 검증한다. 검증이 모두 끝나면 가입자는 난수 값과 비밀키 k를 기반으로 공유키 K_{SS-BS}(= h(k, N_{SS}, X, Y, Z))를 추출하여 베이스 스테이션과 통신을 수행한다.

베이스 스테이션 : $Verify$ Z (식 12)

3.5 인증 정보 갱신

이 절에서는 가입자와 베이스 스테이션 사이에 공유된 공유키 K_{SS-BS}를 가입자가 분실하였거나 키 라이프타임을 초과한 경우 인증 정보를 갱신하기 위한 과정을 기술한다. (그림 3)은 공유키 K_{SS-BS}를 생성하기 위한 인증 정보 과정의 전체적인 동작 흐름도를 나타내고 있다. 인증 정보 갱신은 크게 4가지 과정으로 구성된다.



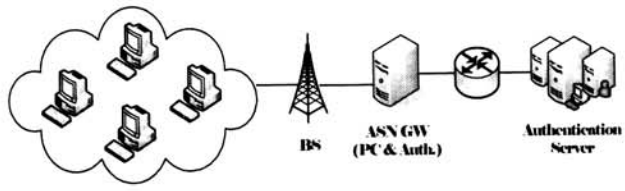
(그림 3) 키 복구 과정의 동작 흐름도

- 단계 1 : 베이스 스테이션은 적법한 과정을 통하여 무선 인증 및 키 설립 프로토콜에서 전송되는 가입자의 N_{SS}, D_{SS}를 획득한다.
- 단계 2 : 베이스 스테이션은 적법한 과정을 통하여 가입자와 비밀리에 공유하고 있는 X, Y, Z를 획득하고 획득한 X, Y, Z의 무결성을 검증한다.
- 단계 3 : 베이스 스테이션은 획득한 값들을 이용하여 $X(=E_{PU_{ss}}(K_{SS}))$, $Y(=K1(Cert_{SS}))$, $Z(=sign_{SK_{ss}}(N_{SS}||N_{BS}||ID_{SS}||ID_{BS}))$ 를 차례로 계산한다.
- 단계 4 : 베이스 스테이션은 공유키 $K_{SS-BS}=h(k, N_{SS}, X, Y, Z)$을 복구하여 가입자에게 전달한다.

(그림 3)의 인증 정보 갱신 과정이 끝난 후 가입자와 베이스 스테이션 사이에서는 송·수신되는 메시지를 암호화하기 위해 흡 간 공유된 공유키를 사용한다. 기존 PKM 프로토콜에서는 네트워크 생명주기동안 사용되는 공유키를 변경하지 않고 사용할 경우 악의적인 노드에 의해 내부 보안 공격에 매우 취약하기 때문에 제안 프로토콜에서는 가입자가 베이스 스테이션이 관리하는 네트워크에 진입하거나 탈퇴하려고 하는 가입자가 발생할 경우 인증키를 정기적으로 갱신하도록 한다. 제안 프로토콜에서 사용되는 가입자의 키 K_{SS}는 기본적으로 인증 프로토콜의 초기 키 생성과 가입자 추가의 경우에만 이용된다. 제안 프로토콜에서 사용되는 키 K_{SS} 만으로는 WiMAX 환경에서 쉽게 발생되는 중간 노드의 악의적인 공격을 막기는 어렵다. 중간 노드의 악의적인 공격을 막기 위해서 제안 프로토콜에서는 초기 키 생성과정 이후에 네트워크 상황과 가입자의 권한 등급에 따라 정기적인 시간간격(t)을 할당하여 가입자의 키를 새로 갱신하도록 한다. 가입자의 권한 등급은 베이스 스테이션의 권한 등급 정책에 따라 수행되고 데이터베이스에 저장되어 있는 가입자의 정보를 통해 가입자의 권한 등급을 파악한다. 또한 가입자의 서비스 사용 유·무에 따라 베이스 스테이션이 가입자의 권한 등급을 유지 관리한다. 이 과정은 가입자와 베이스 스테이션 사이에 통신 오버헤드를 발생할 수 있는 문제점이 있지만 전체 네트워크 상황과 가입자의 권한 등급에 맞게 시간간격을 조절하기 때문에 기존 네트워크보다 네트워크 관리 효율성과 성능 향상을 가져올 수 있다.

4. 평 가

이 절에서는 제안 프로토콜의 성능을 평가하기 위해 IEEE 802.16e 표준에서 지원하고 있는 DES와 AES의 알고리즘을 제안 프로토콜에 적용하였을 때 나타나는 노드수 증가에 따른 인증서버의 인증 지연시간, 노드수 증가에 따른 인증처리시간 그리고 노드수 증가에 따른 인증 서버의 처리량 등의 성능평가와 가입자와 베이스 스테이션 사이에서 가장 많이 발생되는 내부 공격에 따른 보안 평가로 수행한다.



(그림 4) 실험환경

4.1 실험환경

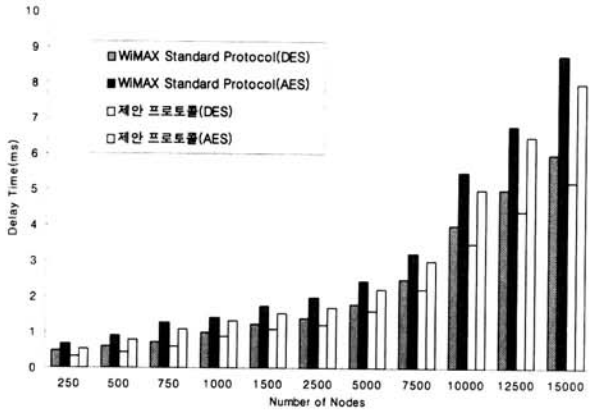
WiMAX 환경에서 제안 프로토콜의 타당성을 검증하기 위해서 NS-2 시뮬레이터를 이용하여 (그림 4)와 같은 실험 모델을 구현하여 제안 프로토콜의 처리과정이 기존 프로토콜에 비해 경량화 되었음을 비교 평가할 수 있도록 실험하였다. 베이스 스테이션의 통신 범위는 500m 범위이며 이 범위내에서 베이스 스테이션은 가입자와 통신이 이루어진다. 실험에 사용된 가입자의 최대 수는 15,000 명으로 하며 성능 실험에 사용되는 성능평가 항목은 [8]처럼 알고리즘에 따른 네트워크 처리량, 노드수 증가에 따른 인증서버의 인증 지연시간, 노드수 증가에 따른 인증처리시간 그리고 노드수 증가에 따른 인증 서버의 처리량 등으로 평가한다. 베이스 스테이션과 단말간은 Air interface이며 단말대 단말은 16e spec에서처럼 P2P가 지원하지 않는다.

4.2 성능평가

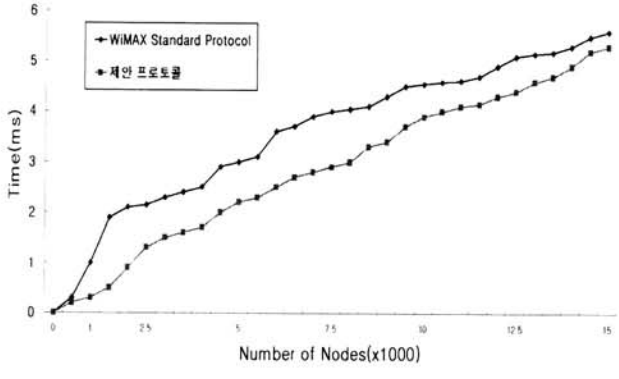
제안 프로토콜의 가입자는 데이터 전달에 서로 다른 패킷 크기를 사용하기 때문에 WiMAX 환경에서 사용되는 서로 다른 패킷 사이즈를 지원하여야 한다. (그림 5)은 제안 프로토콜에 적용된 DES와 AES 암호 알고리즘을 WiMAX 표준 프로토콜과 제안 프로토콜에 적용한 후 노드 수 증가에 따른 인증 지연 시간을 비교 평가하고 있다. (그림 5)의 결과 노드 수가 증가함에 따라 암호 알고리즘과 상관없이 인증 지연 시간이 모두 비례적으로 증가하였으며 WiMAX 표준 프로토콜과 제안 프로토콜의 노드 수가 10,000 명이 넘었을 경우에 인증 지연 시간이 급격하게 증가한 결과가 나타났다. 그리고, DES를 WiMAX 표준 프로토콜과 제안 프로토콜에 적용한 결과 제안 프로토콜이 WiMAX 표준 프로토콜에 비해 4.5%의 인증 지연 시간이 적게 소요되었지만 제안 프로토콜에 AES를 적용한 경우 DES를 적용한 WIMAX 표준보다 8.8% 많은 인증 지연 시간이 필요하였다. 이러한 결과는 인증 메시지에 사용되는 암호 알고리즘과 인증 처리

〈표 4〉 성능 평가 환경변수

환경 변수	값
베이스 스테이션의 통신 범위	500 m
가입자 수	15,000 명
암호 알고리즘	DES, AES
패킷 사이즈	1024 바이트
시뮬레이션 동작시간	1 시간



(그림 5) 노드 수 증가와 암호 알고리즘에 따른 인증 지연시간

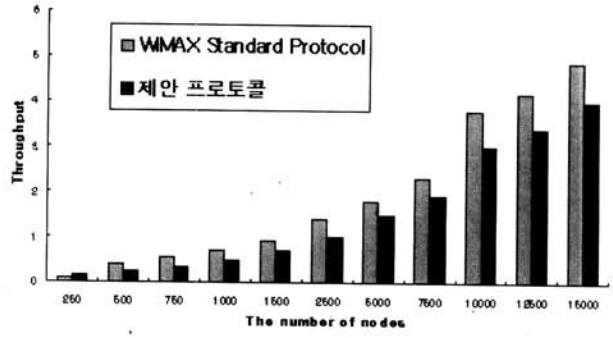


(그림 6) 노드 수에 따른 인증 처리시간

절차에 따라 차이를 나타났으며, 제안 프로토콜에서 초기 인증정보와 인증서를 이용하여 베이스 스테이션과의 추가적인 인증 과정을 수행하지 않아 WiMAX 표준 프로토콜보다 노드 수 증가에 비해 인증 지연 시간이 낮게 나타났다.

(그림 6)은 초기 인증 처리과정을 원하는 노드들 증가에 따른 인증서버의 인증 처리시간을 보여주고 있다. (그림 6)의 결과처럼 WiMAX 표준 프로토콜과 제안 프로토콜은 노드 수가 15,000명까지 증가할수록 인증 처리시간 또한 비례적으로 증가하였다. 그러나 (그림 6)에서 WiMAX 표준 프로토콜은 노드수가 1,000명, 6,000명, 12,000명 일때 인증처리 시간이 급격하게 증가한 반면 제안 프로토콜에서는 1,500명, 7,500명, 14,000명 일 때 인증처리 시간이 급격하게 증가하는 현상이 나타났다. 이 같은 결과는 제안 프로토콜이 추가적인 인증처리 절차를 거치지 않도록 인증서의 정보를 이용하였기 때문에 동일 인증 처리시간을 기준으로 WiMAX 표준 프로토콜보다 제안 프로토콜이 더 많은 노드 수를 처리할 수 있는 결과를 얻었다. (그림 6)의 결과 제안 프로토콜은 WiMAX 표준 프로토콜보다 노드 증가수에 따른 인증 처리 시간이 평균 7.8%% 낮게 나타났다.

(그림 7)은 노드 수 증가에 따른 인증 서버의 처리량 변화를 보여주고 있다. (그림 7)처럼 WiMAX 표준 프로토콜과 제안 프로토콜에서는 노드의 수가 증가할수록 처리량이 비례적으로 증가하고 있으며 7,500명에서 10,000명으로 증가



(그림 7) 노드 수에 따른 인증 서버의 처리량

할 때 WiMAX 표준 프로토콜과 제안 프로토콜의 처리량이 큰 폭으로 증가하였다. 이 결과의 원인은 서버의 오버헤드가 증가하여 나타나는 현상이며 이러한 결과를 해결하기 위해서는 서버의 성능을 향상시키던가 인증서버가 처리하는 서버의 처리량을 분산시켜야 한다. 그리고 (그림 7)의 결과처럼 제안 프로토콜은 WiMAX 표준 프로토콜보다 인증서버의 인증 처리시간이 짧게 소요되어 제안 프로토콜의 인증서버 처리량이 WiMAX 표준 프로토콜보다 평균 18% 낮게 나타났다.

4.3 보안 평가

제안된 상호 인증 프로토콜은 초기에 Identity를 위한 전달 과정과 실제 인증 과정을 수행하는 과정에서 상호인증의 처리절차가 증가하여 통신 오버헤드가 증가하는 단점을 가지고 있으나, 전체적인 오버헤드 측면에서 보면 IEEE 802.16e 표준과 차이가 없었으며 보안 관점에서 보면 공격자로부터 공격당한 노드에 의한 공격이나 위장 공격에 대해서 가입자와 베이스 스테이션 사이에 제안된 상호 인증 프로토콜을 적용함으로써 기존 WiMAX 표준 프로토콜에서 제공하는 보안성보다 한 단계 높은 보안성을 제공한다. WiMAX 환경에서 공격자는 무선 구간의 트래픽을 가로채 사용자 ID와 재인증 ID 등의 메시지를 이용하여 서버에 접속을 시도한다. 제안 프로토콜에서는 ID 메시지에 대한 응답으로 난수값이 전송되기 때문에 이전 인증 과정에서 전송된 메시지 그대로 전송될 수 없으므로 제안 프로토콜에서는 재사용 공격을 막을 수 있다. 공격자가 사용자로 위장하여 EAP-Success 및 EAP-Start 메시지를 기지국에 전송하여 서비스 이용을 방해할 경우 기지국에게 많은 연결 요청 패킷을 전송하여 사용자의 기지국 접속을 방해할 수 있다. 제안 프로토콜에서는 가입자 자신이 생성한 X, Y, Z를 베이스 스테이션의 공개키 PU_{BS}로 암호화하여 베이스 스테이션에게 전달하기 때문에 공격자가 전달되는 정보를 가로채기 하더라도 가입자와 베이스 스테이션이 생성한 일회성 난수(N_{SS}, N_{BS})를 공격자가 알지 못하기 때문에 가로채기 공격에 안전할 수 있다. Main-in-the Middle 공격은 사용자와 인증 서버 간의 트래픽을 중간에서 가로채는 방식이다. 제안 프로토콜은 상호인증을 제공하기 때문에 공격자의 개입을 방지할 수 있고, 인증 과정 후 생성된 키에 의해 안전한 채널이 형성되므로

Impersonation 공격에 의한 데이터 수집도 막을 수 있다. 그리고 재인증 과정 때마다 인증 키가 갱신되므로 공격자는 키 정보를 알더라도 사용할 수는 없다. 이동성을 가지는 가입자와 베이스 스테이션 사이는 무선 구간이므로 공격자는 이 무선 구간에서 전송되는 데이터에 대해 도청이 가능하다. 이를 막기 위해서는 무선 구간에 전송되는 데이터는 암호화되어야 하며 암호화하는 키도 주기적으로 갱신되어야 한다. 제안 프로토콜에서는 키 사용기간이 만료되기 이전에 재인증을 시도하고 이를 통해 키를 갱신하게 되며, 인증 과정 이후에는 인증과정에서 생성된 키로 데이터를 암호화하여 전송하게 된다.

5. 결 론

WiMAX는 기존 이동통신 시스템에 비해 월등한 성능, 낮은 지연 시간, all-IP 핵심망 연동 가능, 그리고 진보된 QoS 및 보안 기능을 제공한다. 그러나 이와 같은 많은 장점에도 불구하고 대역폭(bandwidth) 요청 코드 충돌과 기지국과 여러 단만들 사이에 PKMv2 Key-Request/Reply 메시지를 교환하기 위한 불필요한 처리 시간이 소요되는 문제점을 가지고 있다. 이 논문에서는 WiMAX 시스템에 초기 진입하려고 시도하는 노드들의 인증 부하를 줄이면서 무선 환경에서 발생하는 내부공격에 대해 안전한 경량화된 상호 인증 프로토콜을 제안했다. 제안된 상호 인증 프로토콜은 802.16 표준에서 제공하는 PKMv2의 양방향 상호인증을 향상시키기 위해 난수와 비밀값을 이용하여 인증서 내의 정보를 추출할 수 있도록 네트워크내 가입자와 베이스 스테이션 사이에서 초기 인증을 수행하도록 하였다. 제안 프로토콜은 WiMAX 표준 프로토콜과 노드수 증가에 따른 인증서버의 인증 지연시간, 노드수 증가에 따른 인증처리시간 그리고 노드수 증가에 따른 인증 서버의 처리량 등에서 평가되었으며, 노드수 증가에 다른 인증서버의 인증 지연시간에서는 제안 프로토콜과 WiMAX 표준 프로토콜이 DES를 사용하였을 경우 제안 프로토콜이 WiMAX 표준 프로토콜에 비해 4.5%의 인증 지연 시간이 적게 소요되었지만 제안 프로토콜에 AES를 적용한 경우 DES를 적용한 WIMAX 표준보다 8.8% 많은 인증 지연 시간이 필요하였다. 그리고 노드수 증가에 따른 인증처리사간에서는 제안 프로토콜이 WiMAX 표준 프로토콜보다 평균 7.8%% 낮게 나타났다. 마지막으로 노드 수에 따른 인증 서버의 처리량에서는 WiMAX 표준 프로토콜과 제안 프로토콜 모두 노드 수가 증가할수록 처리량이 비례적으로 증가하였으며 7,500명에서 10,000명으로 가입자가 증가할 때 WiMAX 표준 프로토콜과 제안 프로토콜의 처리량이 큰 폭으로 증가하였다. 향후 연구에서는 다른 통신망과 연동하는 WiMAX 환경에서 발생되는 다양한 보안 공격에 안전한 네트워크 간 핸드오프 통신 프로토콜에 대한 연구를 수행할 계획이다.

참 고 문 헌

[1] A. Ghosh, D. R. J. Wolter, G. Andrews, and R. Chen, "Broadband Wireless Access with WiMax/802.16: Current Performance Benchmarks and Future Potential", IEEE Communications Magazines, Vol.43, Issue2, pp.129-136. Feb., 2005.

[2] IEEE 802.16e-2005, "Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems", 2006.

[3] D. Johnston and J. Walker, "Overview of IEEE 802.16 Security", IEEE Security & Privacy, 2004.

[4] S. Xu and C.-T. Huang, "Attacks on PKM protocols of IEEE 802.16 and its later versions", Proceedings of the 3rd International Symposium on Wireless Comunication Systems (ISWCS 2006), Sep., 2006.

[5] S. Xu, M. Mattews and C.-T. Huang, "Security issues in privacy and key management protocols of IEEE 802.16", Proceedings of the 44th ACM Southeast Conference (ACMSE 2006), Mar., 2006.

[6] IETF RFC 4285, "Authentication Protocol for Mobile IPv6", 2006.

[7] WiMAX Forum NWG, "Stage-3: Detailed Protocol and Procedures", 2007.

[8] T. Janevski, "Traffic analysis and design of wireless IP networks", Artech House, pp.186-190, 2003.

[9] TTAS.KO-06.0065R1, "2.3GHz 휴대인터넷 표준 매체접근제어 계층", 2004년.

[10] 김대익, 이상호, 김영진, "WiBro/Mobile WiMAX 이동성 기술", 한국정보과학회, 제25권, 제4호, 2007년 4월, pp.5-14.

[11] D. Sweeney, "WiMax Operator Manual: building 802.16 Wireless Networks", Apress, 2005.

[12] A. Mishra, M. Shin, and W. Arbaugh, "pro-active Key Distribution using neighbor Graphs", IEEE Wireless Communication, Vol.11, Feb., 2004.

[13] 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.

[14] KISA, "와이브로 인증, 키 관리 기술동향", 정보보호뉴스, 2006년 6월.

[15] D. Johnston and J. Walker, "Overview of IEEE 802.16 security," IEEE Security & Privacy, Vol.2, No.3, pp.40-88, May/June, 2004.

[16] S. Xu, M. M. Matthews, and C.-T. Huang, "Security issues in privacy and key management protocols of IEEE 802.16," in ACM Southeast Regional Conference, R. Menezes, Ed. ACM, pp.113-118, 2006.

[17] M. Barbeau, "Wimax/802.16 threat analysis," in Q2SWinet '05: Proceedings of the 1st ACM international workshop on Quality of service & security in wireless and mobile networks. New York, NY, USA: ACM Press, pp.8-15, 2005.

정 윤 수

e-mail : bukmunro@gmail.com

1998년 2월 청주대학교 전자계산학과 (이학사)

2000년 2월 충북대학교 전자계산학과 (이학석사)

2008년 2월 충부대학교 전자계산학과 (이학박사)

1998년 9월~2000년 8월 충북대학교 전자계산소

관심분야 : 정보보호, 암호이론, Network Security, 이동통신보안, 전자상거래보안

김 용 태

e-mail : ky7762@hannam.ac.kr

1998년 숭실대학교 전자계산학과(석사)

2008년 충북대학교 전산학과(이학박사)

2002년~2006년 가림정보기술 이사

2006년 3월~현 재 한남대학교 멀티미디어학부 강의전담교수

관심분야 : 모바일 웹서비스, 정보보안, 센서 웹, 모바일 통신보안, 멀티미디어

박 길 철

e-mail : gcpark@hannam.ac.kr

1986년 숭실대학교 전자계산학과(석사)

1998년 성균관대학교 전자계산학과(박사)

2006년 UTAS, Australia 교환교수

1998년 8월~현 재 한남대학교 멀티미디어학부 교수

관심분야 : multimedia and mobile communication, network security

이 상 호

e-mail : shlee@chungbuk.ac.kr

1976년 숭실대학교 전자계산학과

1981년 숭실대학교 전자계산학과(석사)

1989년 숭실대학교 전자계산학과(박사)

1976년 1월~1979년 5월 한국전력 전자계산소

1981년 6월~현 재 충북대학교 전기전자컴퓨터공학부 교수

관심분야 : Protocol Engineering, Network Security, Network Management, Network Architecture