논문 2010-47TC-1-4

안전한 모바일 와이맥스 네트워크를 위한 보안 구조 연구

(An Approach for Improving Mobile WiMAX Security - ROSMEX Architecture)

손 태 식*, 구 본 현*, 최 효 현**

(Taeshik Shon, Bonhyun Koo, and Hyo Hyun Choi)

요 약

IEEE 802.16-2004 표준은 MAC 계층 안에 PKM(Privacy Key Management)라 불리는 보안 부계층을 가지고 있다. 하지만, 몇몇 연구에서 IEEE 802.16-2004 표준의 취약성이 대두되었으며 IEEE 802.16 WG은 로밍과 핸드오프 기능을 가진 Mobile WiMAX라고 불리는 IEEE 802.16 개정 표준안을 발표하였다. 보안기능으로서 Mobile WiMAX는 PKMv2를 가지며 EAP 인증, AES 기반 암호화, CMAC/HMAC을 사용한 메시지 인증 등을 제공한다. 그러나 Mobile WiMAX 표준안의 보안 기능은 SS와 BS간 통신 보안에 초점을 맞추어서 네트워크 도메인간의 보안 문제나 핸드오버시 보안과 같은 네트워크 구조적 취약성을 여전히 가지고 있다. 따라서 본 논문에서는 현재 Mobile WiMAX 네트워크 환경의 보안 취약성을 네트워크 엔트리 과정, 네트워크 도메인간 통신 과정, 그리고 핸드 오프 과정으로 나누어 분석하였고, 이렇게 분석된 내용을 바탕으로 본 논문에서는 RObust and Secure MobilE WiMAX (ROSMEX)라 불리는 새로운 Mobile WiMAX 보안 구조를 제시하였다.

Abstract

The IEEE 802.16-2004 standard has a security sub-layer in the MAC layer called, Privacy Key Management (PKM). However, several researches have been published to address the security vulnerabilities of IEEE 802.16-2004. After the IEEE 802.16-2004 standard, a new advanced and revised standard was released as the IEEE 802.16e-2005 amendment which is foundation of Mobile WiMAX network supporting handoffs and roaming capabilities. PKMv2 in Mobile WiMAX includes EAP authentication, AES-based authenticated encryption, and CMAC or HMAC message protection. However, Mobile WiMAX still has a problem of security architecture such as a disclosure of security context in network entry, a lack of secure communication in network domain, and a necessity of efficient handover supporting mutual authentication because Mobile WiMAX security has mainly concentrated on between SS and BS communication. Based on the investigation results, we propose a novel mobile WiMAX security architecture, called RObust and Secure MobilE WiMAX (ROSMEX), to prevent the new security vulnerabilities.

Keywords : Mobile Broadband Access, Mobile WiMAX, Network Security

I. 서 론

현재 우리의 삶은 인터넷 기반의 다양한 서비스와 애플리케이션의 빈번한 사용으로 삶의 편의성을 증대시키는 방향으로 점점 더 나아가고 있다. 이러한 삶의 변화는 점점 더 빠른 속도, 저비용 고효율, 고속 이동성 및 광대역 통신 등과 같은 특성의 제공을 전제로 진행 중이다. 이와 같은 추세에 맞추어 IEEE 802.16 워킹 그룹은 저속이동성과 사용자들의 요구를 충족시키기 위한 IEEE 802.16 표준안을 2004년 제정하고 이로보터 다시 고속 이동성, 보안 기능 등이 보완된 IEEE 802.16e-2005 표준을 개정하였다. 이 표준안은 IEEE의 많은 산학 연구 단체는 물론이고 WiMAX(Worldwide

* 정회원, 삼성전자 Digital Media & Communication 연구소
(Samsung DMC)
** 정회원, 인하공업전문대학 컴퓨터정보과
(Inha Technical College)
접수일자: 2008년12월6일, 수정완료일: 2010년1월18일

Interoperability for Microwave Access) 포럼에 속한 많은 기업체의 지원 속에 상용화 시점이 점점 앞당겨지고 있다. IEEE 802.16 워킹 그룹이 주로 기술 개발 및 표준화에 중점을 두었다면, WiMAX 포럼은 IEEE 802.11과 Wi-Fi와의 관계처럼 필드 표준 정립을 위해 많은 기업체들과 함께 상호 운용성 및 호환성 테스트를 주도하여 Mobile WiMAX라는 사실상의 업계 표준안을 만들어냈다. 기본적으로 Mobile WiMAX는 IEEE 802.16e를 기반으로 하는 네트워크 구조와 시스템 프로파일을 의미하며 현재 광대역 데이터 전송, 고속 이동성 지원, 광역 커버리지, 그리고 고용량 제공 등 다양한 특성을 바탕으로 가장 유력한 4세대 통신의 후보로 떠오르고 있다.[1~4]

이러한 뛰어난 통신 성능 외에도 보안 관점에서 Mobile WiMAX 는 PKMv2를 사용하여 기존 PKMv1 기반의 IEEE 802.16 표준보다 효율적인 보안 기능을 제공하지만, PKMv2의 제공만으로 모든 보안 요구사항을 만족시켰다고는 할 수 없다. 본 논문에서는 단순히 IEEE 802.16e의 PKMv2의 문제점이 아닌 Mobile WiMAX 네트워크 구조 관점에서 네트워크 진입 과정, 네트워크 도메인간 통신 과정, 그리고 핸드오버 과정 등 실제 Mobile WiMAX 네트워킹시 발생할 수 있는 보안 취약성을 진단한다[3~5].

본 논문의 구성은 다음과 같다. Ⅱ장에서는 Mobile WiMAX 보안 개요 및 알려진 보안 취약성에 대해서 설명한다. Ⅲ장에서는 Mobile WiMAX에 대한 새로운 보안 취약성을 소개하며 Ⅳ장에서는 새롭게 소개된 Mobile WiMAX 보안 취약성에 대한 대응 방안을 제시한다. Ⅴ장에서는 앞서의 보안 대응 방안에 대한 비교 검증 및 제안 방안을 종합한 보안 구조를 언급하며 Ⅵ장에서 본 논문의 결론 및 향후 연구 방향을 제시한다.

Ⅱ. 관련 연구

IEEE 802.16 표준안이 2004년에 제정된 이후로 IEEE 802.16기반 네트워크에 존재할 수 있는 보안 취약성 및 공격 가능성에 대해서 많은 연구가 수행되어져 왔다. Ⅱ장에서는 먼저 Mobile WiMAX 보안 개요에 대한 설명을 하고 그 후 이미 알려진 많은 연구에 나타난 보안 취약성과 그 공격 방법을 언급한다.

1. 모바일 와이맥스 보안

IEEE 802.16e-2005 표준을 기반으로 하는 Mobile WiMAX는 이동성을 지원하지 않는 IEEE802.16-2004 표준에 비하여 다양한 보안 기능을 지원한다. 기본적으로 양 표준안 모두가 지원하는 PKMv1은 기본적인 Key 관리 기능뿐 아니라 EAP기반의 인증과 트래픽 암호화 등의 기능을 가진다. IEEE 802.16e에서는 보다 강화된 Security Suite를 가진 PKMv2가 기본으로 사용된다. PKMv2는 HMAC(keyed-Hash Message Authentication Code)과 CMAC(Cipher-based Message Authentication Code)을 사용하는 메시지 인증 기능, EAP기반의 디바이스 및 사용자 인증 기능, 그리고 AES-CCM을 사용하는 기밀성 기능을 제공한다. 또한 WiMAX 포럼으로부터 진행된 [3~4]의 연구를 통해 PKMv2를 기반으로 하는 Mobile WiMAX의 주요 보안 기능은 앞서 IEEE 802.16e의 PKMv2가 가지고 있는 키 관리 기능, 디바이스 및 사용자 인증, 트래픽 암복호화, 제어 메시지 인증 기능은 물론이고, Hard Handover 및 IP 이동성 지원 등에 있어 도메인간 IPSec의 적용, AAA 서버와의 통신 보안을 위한 DIAMETER의 적용 등 부가적인 네트워크 전체에 대한 보안 기능을 일부 언급하고 있다. 있다. 특히 PKMv2 기반의 키관리 기능은 EAP 인증키, 메시지 인증키, 트래픽 암호화 키, AK(Authorization Key) 키교환 및 멀티/브로드캐스트 키 등 다양한 용도로 사용된다[16].

2. 알려진 취약성과 공격 가능성

Mobile WiMAX의 보안 구조는 부분적으로 일반적인 IEEE 802.11과 같은 무선 네트워크의 보안 기능을 근간으로 하고 있다. IEEE 802.11의 경우 그 개발 역사 및 다양한 용도로 현재 널리 사용되고 있어 다양한 보안 관련 연구가 이미 진행되어 왔으며 또한 몇몇 보안 취약성 등이 널리 알려져 있다[8~11]. 많은 연구 중에 John Bellardo와 Stefan Savage의 연구 [10]는 USENIX 학회에서 MAC과 identity 취약성을 이용한 DoS공격 가능성을 보여주었다. 이번 장에서는 현재 진행되어온 많은 연구들을 바탕으로 이미 알려진 IEEE 802.16d/e 표준의 몇 가지 보안 위협들을 살펴볼 것이다[12~14].

먼저 Auth-Invalid 취약성을 살펴보면, Key Reply 또는 Key Reject 메시지 인증이 실패하는 경우 Auth Invalid 이벤트가 SS(Subscriber Station) 내부적으로 생성된다. 또는 BS(Base Station)로부터 SS에게 Auth

Invalid 메시지 수신되는 경우에 Auth Invalid 메시지 전달에 의해서도 Auth Invalid 이벤트가 생성 될 수 있다. 만일 SS가 비인증된 MAC 코드를 가진 Key Request 메시지를 보낸다면, BS는 Auth Invalid로서 Key Request 요청에 응답한다. 그러므로 SS가 Auth Invalid 메시지를 받았을 때 SS의 state machine은 Authorized 상태에서 Reauth Wait상태로 전환 될 것이다. 그리고 SS는 BS로부터 새로운 명령을 받을 때까지 대기 상태로 들어가게 된다. 만일 SS가 BS로부터 새로운 명령을 받기 전에 Reauth Wait 타이머가 종료된다면 SS는 Reauth Request를 다시 요청하게 된다. 또한 SS가 Reauth 상태에 있는 동안 SS는 Auth Reject 메시지를 받을 수 있게 되고 만일 이렇게 되면 SS는 Permanent Authorization Failure 상태에 빠지게 될 수도 있다. SS가 그런 메시지를 받을 수 있다면, 공격자는 SS를 Silent state로 전환시키고 모든 사용자 트래픽을 중단 시킬 수 있게 된다. 이 방법은 공격자가 Authorization 상태 머신을 조정할 수 있다는 것을 보여주는 하나의 취약점이 되겠다. 이러한 공격은 Auth Invalid 메시지가 PKM identifier 및 HMAC/CMAC 인증 코드를 지원하지 않기 때문에 가능하다.

또한 Rogue BS로 알려진 보안 취약성의 경우, SS는 위조된 BS에 의해서 공격당할 가능성을 가지고 있다. 즉, SS는 위조된 BS에 대한 접속을 실제 BS로 간주하게 될 수 있고, 그러므로 위조된 BS는 SS의 모든 정보를 중간에서 가로 챌 수 있게 된다. 다시 말해서 Rogue BS 공격의 일반적인 무선 네트워크 환경에서 널리 알려진 Man-in-the-Middle 공격의 하나로서 볼 수 있다. PKMv1을 사용하는 IEEE 802.16에서 Auth Request 메시지는 단지 SS 인증에 대한 인증 정보만을 포함하며 BS 인증 정보를 가지지 않기 때문에 SS와 BS간 통신 설정 과정에서 보안 프로토콜 측면에서 BS의 정당성을 인증하는 부가적인 방법을 찾을 수 없다. 그러므로 SS-BS 인증과정의 Auth 관련 메시지들을 스니핑 함으로써 Rogue BS가 실제 BS인양 가장하는 공격이 가능함이 알려져 있다. 그러나 PKMv2가 적용된 IEEE 802.16e기반의 Mobile WiMAX의 경우 SS-BS인증과정에서 상호 인증 기능을 기본으로 적용되기 때문에 Rogue BS 취약성은 제거 될 수 있다. 이외에도 RNG-RSP 공격, RNG-CMD DoS 공격, Auth-Reject, EAP 관련 여러 공격들이 존재함이 알려져 있다[12~14].

III. 모바일 와이맥스의 취약성

앞서의 많은 연구들로부터 IEEE 802.16e의 보안 기능 및 Mobile WiMAX 시스템에 대한 기본적인 이해를 구할 수 있었다. 하지만 IEEE 802.16e 기반의 Mobile WiMAX 시스템이 많은 보안 기능을 제공함에도 불구하고 Mobile WiMAX 네트워크는 여전히 몇몇 취약성을 가지고 있다. 그 중의 하나는 네트워크 진입 과정에서 MAC 관리 메시지들에 대한 보안 부재로 인한 security context들의 노출이며, 또 하나는 Mobile WiMAX의 ASN(Access Service Network), CSN (Connectivity Service Network)간 통신시에 상이한 도메인간 보안 기능을 제공하는 문제이다. 또한 Hand-over 과정의 보안 문제는 어떤 시스템이던지 간에 이동성을 지원하게 되면 항상 지적이 되어 오고 있는 문제이다.

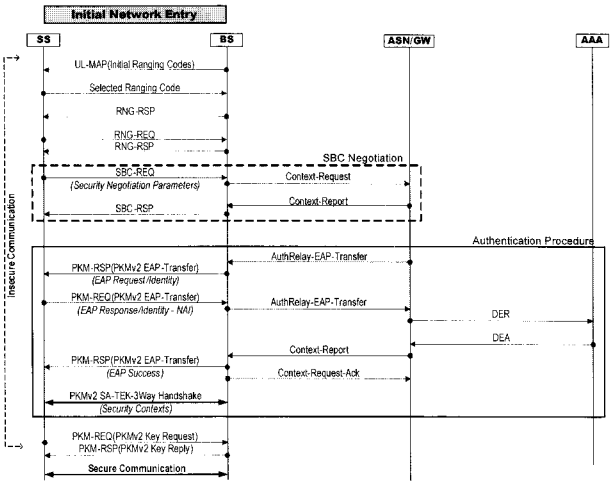


그림 1. 초기 네트워크 진입 과정
Fig. 1. An Overview of Initial Network Entry Procedure.

3.1. 초기 네트워크 진입 취약성

IEEE 802.16e-2005 표준안에 따르면, Mobile WiMAX 네트워크에 진입한 SS는 BS와 초기 Ranging 과정, SBC(SS Basic Capability) 협상 과정, PKM 인증 과정, 그리고 등록(Registration) 과정을 거쳐 실제 Mobile WiMAX 네트워크를 시작하게 된다. 앞서 열거된 과정들은 그림 1에서와 같이 도식화 될 수 있다. 이러한 초기 네트워크 진입 과정은 SS가 Mobile WiMAX에 최초로 접속하여 통신 과정을 수행하는 과정으로서 Mobile WiMAX의 첫 번째 관문이라는 점에서 매우 중요한 의미를 지니게 된다. 그러므로 이러한

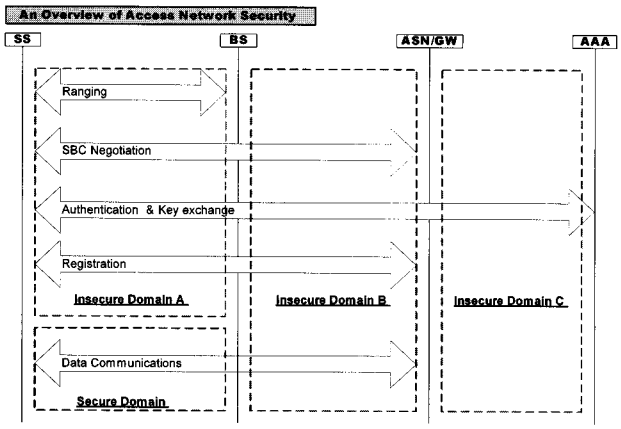


그림 2. 액세스 네트워크 보안 구조
Fig. 2. An Overview of Access Network Security.

초기 네트워크 진입 과정은 네트워크를 구성하는 물리적인 파라미터 설정으로부터 시작해서 다양한 성능 팩터들 그리고 보안 관련 여러 context들을 협상하고 설정하게 된다. 하지만, SBC 협상과정과 PKM 인증 과정에서 사용되는 여러 파라미터를 포함하고 있는 MAC 관리 메시지들은 이러한 네트워크 진입 과정을 이끄는 중간 과정이기 때문에 특별한 보호 수단 없이 평문 상태의 메시지 교환으로 그들의 정보를 노출 시키게 되는 문제점을 안고 있다. 이때 SBC 협상과정은 PKM version support, Authorization policy support, MAC code mode, 그리고 PN Window size와 같은 정보를 교환하게 된다. 여기서 authorization policy support나 MAC code mode 등은 공격자에게 노출되었을 경우 시스템 침해를 위한 공격의 단초를 제공해 줄 가능성을 가지고 있다. 또한 PKM인증 과정은 Dobule-EAP를 쓰지 않을경우엔 PKM 인증 페이즈의 모든 메시지들이 노출 될 수 있다. 다시 말해서 Mobile WiMAX는 HMAC/CMAC을 사용하는 메시지 인증기능과 AES-CCM을 사용하는 트래픽 암호화 기능을 가지고 있지만, 이러한 PKMv2 기반의 보안 기능들은 통신을 요청한 SS가 초기 네트워크 진입 과정을 모두 정상적으로 끝마쳐야만 적용 가능하므로 실제적인 초기 네트워크 진입 과정의 다양한 파라미터 협상과정에는 근본적으로 적용이 불가능하다는 문제점을 내포하고 있다. 그러므로 Mobile WiMAX의 근간이 될 수 있는 초기 네트워크 진입 과정의 보안 취약성은 간단하게는 chicken-egg problem으로 보일 수 있지만, 근본적인 대응 방안이 필요하다고 생각된다.

3.2. 액세스 네트워크 취약성

WiMAX 포럼은 Mobile WiMAX를 위한 종단간 네트워크 시스템 구조[6]에 관한 요구사항을 충족시키기 위하여 네트워크 참조 모델을 정의하였다. 네트워크 참조 모델에서는 SS, ASN(Access Service Network), CSN(Connectivity Service Network)으로 구성되는 Mobile WiMAX를 논리적 표현 모델로 정의하여 설명하고 있다. 여기서 SS는 Mobile WiMAX 네트워크에 참여를 원하는 이동 디바이스 중의 하나를 의미하며, ASN은 사용자들에게 무선 접속 기능을 제공하기 위해 필요한 기능들을 정의한 총괄 단위이다. ASN은 최소 하나의 BS와 하나의 ASN Gateway로 구성된다. 또한 CSN은 Mobile WiMAX 사용자들에게 IP 네트워크와의 연결성을 제공하기 위한 네트워크 기능의 집합으로서 AAA 프락시 서버, 정책 서버, 과금 서버, 로밍 개체 등으로 구성된다. 기본적으로 우리는 이미 Mobile WiMAX가 IEEE 802.16 표준안들을 바탕으로 하여 정의 되어 왔음을 알고 있다. 여기서 WiMAX 포럼의 네트워크 참조 모델이 가지는 의미는 기존 IEEE 802.16 표준안이 단지 SS와 BS간 인터페이스 및 통신 기능의 정의에 초점을 맞추고 있다고 할 때 WiMAX 포럼의 모델은 SS-BS간의 표준을 포함하며 Mobile WiMAX 네트워크 구성을 위한 다양한 네트워크 도메인간 통신 및 기능을 정의하였다고 볼 수 있다. 다음의 그림 2는 IEEE 802.16 표준과 WiMAX 포럼의 네트워크 참조 모델을 도식화하여 보안 취약성을 쉽게 나타내준다. 그림 2에 나타난 것과 같이 현재 IEEE 802.16기반의 PKM이 적용되는 보안 구간은 매우 일부분임을 알 수 있다. 앞서 연구에서 SS-BS간 네트워크 진입 과정이 이미 안전하지 않음을 지적했으며, SS와 BS의 통신이 그 이후 ASN과 CSN으로 이동하는 동안의 통신에 관해서 구체적으로 명시된 보안 요구 사항이 없기 때문에 ASN과 CSN으로 정의되는 네트워크 도메인 구간은 실제적인 보안 기능이 미비하거나 또는 실제 네트워크를 전개하는 사업자의 몫으로 돌릴 수 있다. 하지만, 본고에서는 Mobile WiMAX를 단순히 SS와 BS간 물리적 동질 인터페이스를 가진 디바이스간 통신이 아닌 ASN 및 CSN등의 다양한 네트워크로 구성되는 하나의 통합 네트워크로 간주하여 보안 문제를 되짚어 보고자 한다. 그러므로 Mobile WiMAX 사용자들에게 무선 접속 서비스를 제공하는 ASN구간과의 네트워크 도메인간 통신 그리고 IP 연결성을 제공하는 CSN 구간과의 네트워

크 도메인간 통신에 있어 현재 미비한 보안 기능을 새롭게 정의 또는 이미 알려진 보안 기능일지라도 망 구축시 사용을 권고하는 최소한 수준의 보안이 필요할 것으로 생각된다. 현 수준은 IP 연결성을 제공하는 구간의 경우 대표적인 legacy IP 네트워크 보안 프로토콜인 IPSec의 사용이 권장되고 있으며 또한 AAA서버의 사용시 DIAMETER등의 사용을 통해 좀 더 안전한 응용 수준의 보안 기능을 적용할 것을 권고하고 있다.

3.3. 핸드오버 과정의 취약성

Mobile WiMAX는 fixed, nomadic, fully-support mobility 지원과 같이 완전한 이동성 서비스 위하여 다양한 핸드 오버 기법을 제공하는 대표적인 IP기반 차세대 이동통신 기술로서 각광받고 있다. IEEE 802.16e 표준안에 정의되어 있는 핸드오버 기능으로는 HHO(Hard HandOver), FBSS(Fast Base Station Switching), 그리고 Macro Diversity 핸드오버가 있다. 이중에서 HHO는 Mobile WiMAX가 기본으로 삼는 핸드오버 기법이다[15]. Mobile WiMAX에서는 이처럼 다양한 핸드오버 기법이 적용되고 fully-supported mobility 강점으로 내세우고 있기 때문에 빈번하게 핸드오버가 발생하는 경우에도 끊김 없는 서비스를 제공할 수 있어야 한다. 따라서 Mobile WiMAX에는 효율적인 핸드오버 지원을 위하여 부가적인 HO 최적화 기능이 포함되어 있다. HO 최적화 기능은 IEEE8 802.16e 표준안에 정의되어 있는 것처럼 8종류의 최적화 옵션으로 구성되며 핸드오버가 발생했을 때 네트워크 재진입 과정이나 재인증 과정을 최소화하기 위하여 사용된다. 많은 HO 최적화 옵션중

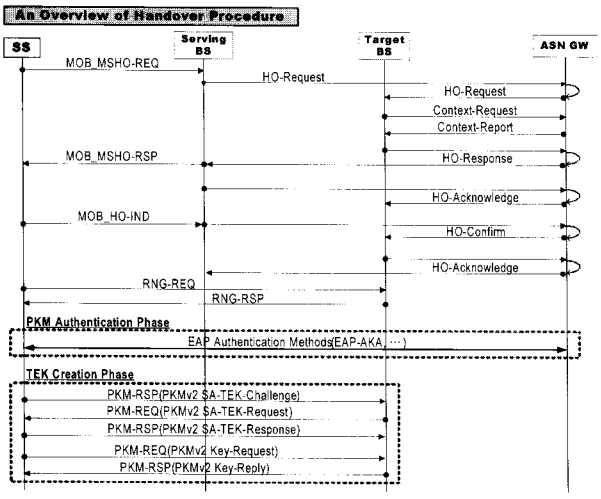


그림 3. 핸드오버 과정
Fig. 3. An Overview of Handover Procedure.

에서, PKM 인증 페이즈(HO 최적화 플래그 #1)과 TEK 생성 단계(HO 최적화 플래그 #2)가 그림 3과 같이 핸드오버시 보안 기능과 연관성을 가지고 있다.

만일 앞서 설명한 것과 같은 두 옵션이 사용된다면, PKM 인증 단계와 TEK 생성 단계는 효율적이고 끊김 없는 서비스를 위하여 핸드오버 과정에서 생략가능하게 된다. 즉, HO 최적화 옵션의 사용으로 핸드오버시에도 끊김 없는 서비스를 제공하며 핸드 오버 지연 시간을 최소화 시키는 빠른 핸드오버 기능을 제공할 수 있다고 긍정적인 면을 감안하더라도, 이러한 최적화 HO 플래그의 사용은 궁극적으로 핸드오버 과정에서의 인증 및 기밀성과 같은 보안 기능의 생략을 초래함으로써 Man-in-the-Middle 공격, 정당한 사용자의 인증 어려움 등 치명적 네트워크 취약성을 야기 시킬 수 있다[12~14]. 결국 보안에 관련된 HO 최적화 플래그의 사용은 핸드오버 성능 향상과 안전한 통신과의 tradeoff관계를 성립시키며, 보다 효율적인 취약성 대응 방안이 Moible WiMAX의 핸드오버 과정 보안을 위해서 필요함을 알 수 있다.

Ⅳ. 제안하는 대응방안

Ⅲ장에서 초기 네트워크 진입, 네트워크 도메인간 통신, 그리고 핸드 오버 과정등과 같이 세 가지 관점에서 Mobile WiMAX 네트워크 보안 취약성들을 살펴보았고 본장에서 그에 대한 대응 방안을 제안한다. 하지만 여기에 제안되는 방안은 절대적인 취약성 제거 방안 혹은 보안성 검증이 끝난 그러한 해결 방안이 아닌 앞서 제기된 문제에 대한 하나의 대응 방안으로서의 시발점을 제시하는 수준으로 인식하는 것이 오히려 다양하게 존재할 수 있는 Mobile WiMAX 네트워크 보안 취약성을 제거하는데 많은 도움을 줄 수 있을 것이다.

4.1. 초기 네트워크 진입 취약성에 대한 대응방안

초기 네트워크 진입 과정에서는 Ranging/SBC 협상/PKM/Registration등 네트워크 연결에 관련된 다양한 파라미터들이 설정된다. 하지만 앞서의 설명과 같이 초기 네트워크 진입 과정에서의 적절한 보안 수단이 아직 IEEE 802.16 또는 Mobile WiMAX 프로파일에 마련되어 있지 않다. 초기 네트워크 진입 과정에서의 보안 취약성을 제거하기 위해서, 가장 근본적으로 필요한 수단은 그 과정에서 교환되는 메시지들을 안전하게 유지하

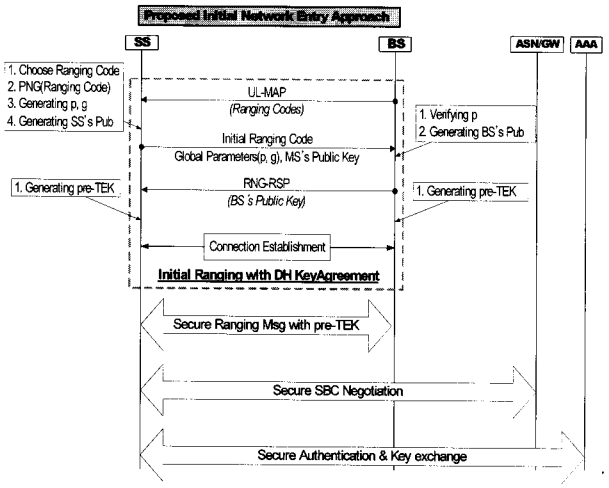


그림 4. 제안하는 네트워크 초기 진입 과정 대응방안
Fig. 4. Proposed Network Initial Entry Approach.

표 1. 네트워크 진입 보안 방안 성능 검증
Table 1. Security and Performance Analysis in Network Entry Security.

		IEEE 802.16e	Applying Original DH	Proposed Approach
Security	Confidentiality	None	O	O
	Man-in-the-Middle Attack	None	None	O
Performance	Processing Overhead	-	Random Number & Key Generation	Random Number & Key Generation & Hash processing
	Communication Overhead	-	None	None

도록 만들어 줄 수 있는 수단을 제공하는 것이다. 본 논문에서는 초기 네트워크 진입 과정 중 ranging 과정에 DH 키 교환 기법을 적용하여 부가적인 보안 스킴을 적용하는 것 없이 기존의 네트워크 진입 과정의 결과로서 보안 기능을 제공할 수 있는 방안을 제안한다.

그림 4에서 초기 ranging 과정을 살펴보면 초기 통신 코드로 사용할 ranging 코드를 수신하여 설정하는 과정이 있는데 이때 BS가 보낸 UL-MAP에 포함된 여러 ranging 코드 중 SS가 하나의 ranging 코드를 선택하게 된다. 이때 이 선택된 코드를 DH 키교환의 랜덤 넘버 'p'를 생성하는데 사용하고, 'p'로부터 원시근인 'q'를 생성하고 DH 키교환의 전역 파라미터로 사용한다. SS는 먼저 이 'p', q'로부터 공개키/개인키 쌍을 유도하고, BS에게 'p','q', 그리고 SS의 공개키를 초기 ranging 코드 응답 메시지로서 전송한다. 이때 BS는 SS로부터 받은 'p'를 검증하고, 마찬가지로 공개키 쌍을 생성한다. 이후 BS는 RNG-RSP를 SS에게 전송하며 이때 자신의 공개키를 SS에게 전달한다. 이렇게 DH 키교환과정을 마치고 SS와 BS는 각각 서로가 공유할 수 있는 키(pre-TEK)를 생성할 수 있다. 그러므로 SS와 BS는 Ranging과정의 DH 키교환을 통해서 생성된 pre-TEK를 통해서 이후 SBC 협상과 PKM 보안 context교환과정에서의 기밀성을 제공할 수 있게 된다. 하지만, 이 방안은 DH 키교환 자체의 취약성이나 빈번한 네트워크 진입등에서 발생할 수 있는 취약성들을 제외한 단지 기존 Mobile WiMAX 시스템의 변경 없이 초기 네트워크 진입 과정에서 보안성을 제공할 수 있는 하나의 방안으로서 의미를 가진다. 표 1에서는 네트워크 진입과정의 보안 방안의 성능을 분석하였다.

4.2. 액세스 네트워크에서의 취약성 대응방안

Mobile WiMAX 시스템에서의 주요한 보안 구조로서 알려진 PKM은 단지 SS와 BS간 통신에 대한 보안 기능을 정의하고 있다. 즉, Mobile WiMAX 네트워크에서 SS와 BS간 통신 구간 외에 정의된 부분은 IEEE 802.16e 표준문서의 보안 상세의 범주를 넘어선다는 것을 의미한다. 또한 WiMAX 포럼의 네트워킹 워킹 그룹의 기술 문서들에서도 ASN 네트워크 도메인을 신뢰할 수 있는 도메인으로 가정하고 있으며, ASN과 CSN 도메인 사이에 AAA 연결은 IPSec을 사용하여 보호 될 수 있다고 언급하고 있다[6~7]. 그러므로 현재의 IEEE 802.16e 보안 표준 명세나 WiMAX 포럼의 관련 기술 상세에는 Mobile WiMAX 도메인간 안전한 통신에 관한 구체적인 내용이 언급되어 있지 않기 때문에 도메인간 안전한 통신을 위한 하나의 방안으로서 PKI 구조를 기반으로하는 인증서 기반 키교환 및 암호화 통신방안을 제안한다. 우선 이러한 방안은 Mobile WiMAX의 여러 네트워크 디바이스들이 SS와 BS같이 인증서 기반의 인증 기능을 지원한다고 가정하고 ASN 및 CSN으로 구성된 도메인간 PKI를 통한 인증서 검증 체인이 존재한다고 정의한다.

그림 5와 같이 Mobile WiMAX 네트워크의 모든 네트워크 디바이스들은 자신의 고유 인증서와 인증서 검증을 위한 체인을 가지고 있다. 만일 BS가 ASN 도메인 내부의 ASN/GW와 안전한 통신이 필요하다고 하면, 먼저 BS는 ASN/GW와 통신에 사용할 세션키를 생성하고 이 세션키 정보를 ASN/GW의 공개키로 암호화하여 ASN/GW에게 전달한다. 이때 전달되는 값으로는 실제 BS와 ASN/GW간 암호화 통신에 사용하기 위해 생성된 세션키 외에 암호화된 실제 메시지, 타임스탬프, 인증기관의 인증서가 포함된다. ASN/GW는 이러한 메시지를 BS로부터 전달 받은 후 타임스탬프로 유효성을

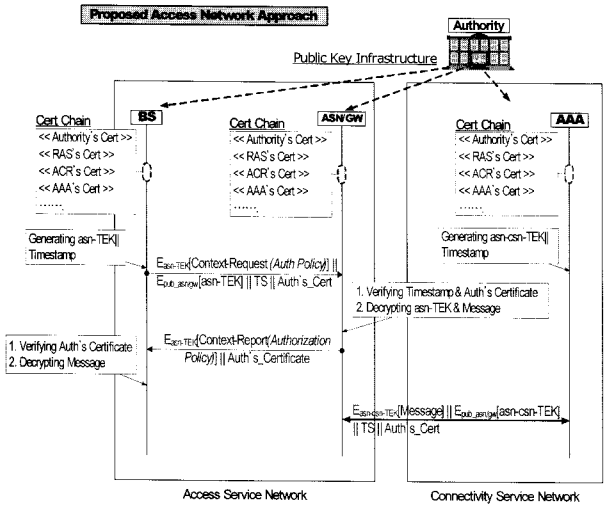


그림 5. 제안하는 액세스 네트워크 대응방안
Fig. 5. Proposed Access Network Approach.

표 2. 액세스 네트워크 보안 방안 성능 검증
Table 2. Security and Performance Analysis in Access Network Security.

		IEEE 802.16e	Applying IPSec	Proposed Approach
Security	Confidentiality	None	O	O
Performance	Processing Overhead	-	High	Low
			SA negotiation/ IKE/ Key Generation	Certification Operation/ Key Generation
	Communication Overhead	-	High	Low
			2phase 6~9 times packet exchange	1phase 2times packet exchange
	Requiring Additional Features	-	O	None

검증하고 인증기관의 인증서로 신뢰기관으로부터 인증된 개체임을 검증한다. 그 후 자신의 공개키로 암호화된 세션키를 복호화하여 실제 전달하려던 암호화된 메시지를 복호화하여 사용한다. 그러므로 위 그림 5의 설명과 같이 각 도메인의 네트워크 디바이스들은 PKI 기반 인증서 인증 체계를 가지고 있다고 하면 앞서의 예시와 같이 BS와 ASN/GW간에는 asn-TEK와 같이 두 디바이스간 임시 암호화 키를 생성 할 수 있으며, ASN/GW 및 AAA간 통신의 경우에는 asn-csn-TEK를 생성하여 두 도메인간 보안 통신에 활용 할 수 있다. 표 2에서는 액세스 네트워크 과정의 보안 방안의 성능을 분석하였다.

4.3. 핸드오버 취약성에 대한 대응방안

Mobile WiMAX의 이동성 지원 기능에서 핸드오버 과정은 핸드오버 과정의 메시지 교환을 최소화하며 끊김 없는 서비스를 제공하기 위한 핸드오버 최적화 옵션을 사용하는 일종의 Fast Handover 기능을 채택하고

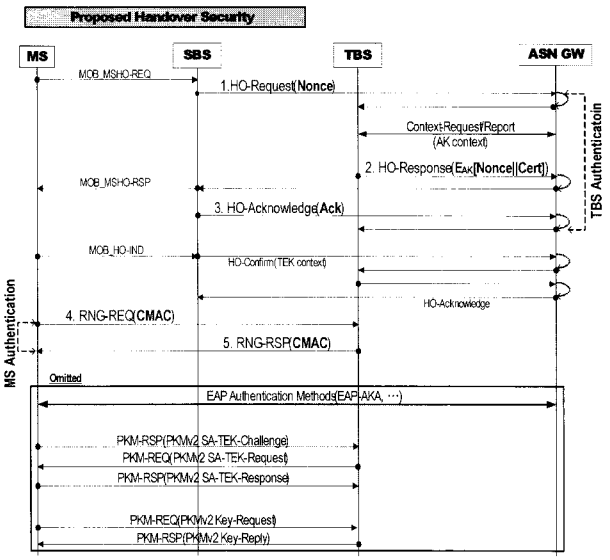


그림 6. 제안하는 핸드오버 보안 방안
Fig. 6. Proposed Handover Security Approach.

있다. 그러나 그런 핸드오버 과정은 이미 앞서 설명한 것과 같이 효율적이고 빠른 핸드오버 지원에 따른 보안 취약성을 내포하고 있다. 그러므로 본 장에서 보안성을 가지며 기존의 빠른 핸드오버과정을 지원할 수 있는 새롭게 수정된 방안을 제안한다. 제안하는 방안은 그림 6과 같이 핸드오버 메시지의 교환 중 몇몇 추가된 메시지 필드를 가진다. 핸드오버를 위해서 교환되는 메시지의 종류와 횟수는 동일하지만 핸드오버 최적화 옵션의 사용과 동시에 보안성을 제공하기 위하여 몇몇 필드가 추가된 것이다. 이 제안하는 방안은 일종의 challenge-response 스킴을 적용한 것으로서 핸드오버 과정에서 상호인증 기능을 수행하여 후에 핸드오버 최적화 옵션이 사용될지라도 보안 취약성을 제거할 수 있게 된다. 상호 인증 과정 중 그림 6의 메시지 1부터 메시지 3과 같이 먼저 Target BS(TBS)인증이 이루어지는데 이것은 HO-Request 과정 중에 수행된다. 핸드오버 과정이 시작될 때 Serving BS는 Nonce가 포함된 HO-Request 메시지를 TBS에게 전달한다. TBS는 이 Nonce와 자신의 인증서를 암호화하여 다시 SBS에게 HO-Response 메시지로서 응답하게 된다. 만일 SBS가 HO-Response 메시지 안에 포함된 Nonce와 인증서를 성공적으로 검증하게 되면 SBS는 Ack를 가진 HO-confirm 메시지를 TBS에게 보내게 되는 것으로 상호인증 과정 중 TBS인증을 마무리하게 된다. SS인증의 경우, CMAC/HMAC 튜플이 그림 6의 메시지 4와 5처럼 적용된다. HO과정 후, SS는 Ranging과정을 시도

표 3. 핸드오버 보안 방안 성능 검증
Table 3. Security and Performance Analysis in Handover Security.

		IEEE 802.16e Handover	**Proposed Handover Approach**
Security	Mutual Authentication	None	O
Performance	Processing Overhead	None	Low
			1 time Encryption/Decryption
	Communication Overhead	None	None

하고 TBS는 RNG-REG 메시지에 포함되어 있는 CMAC/HMAC 튜플을 검증함으로써 SS를 인증할 수 있게 된다. 이때 CMAC/HMAC은 TBS 인증과정 중 교환된 AK context에 포함된 AK를 이용하여 생성되었다. 그러므로 제안하는 방안은 실제 HO 최적화 옵션들이 실행되어 핸드오버 과정중 재인증이나 키생성등의 과정이 생략될지라도 이전 핸드오버 준비과정에서의 상호인증을 통해 보다 효율적이고 안전한 이동성 지원을 가능케 할 수 있다. 표 3에서는 핸드오버 과정의 보안 방안의 성능을 분석하였다.

V. 강건한 모바일 와이맥스 보안 구조

본 논문에서는 Mobile WiMAX 네트워크에서 보안 위협을 최소화하기 위한 새로운 방안들을 제안하였다. 제안한 방식을 바탕으로 기존 방식들과 비교하여 분석한 장점과 적용 가능한 부분을 표4와 같이 도출하였다.

제안된 몇 가지 방안들로 구성된 신뢰성 있는 Mobile WiMAX 보안 구조를 그림 7에 나타난 것처럼 ROSMEX(RObust and Secure MobilE WiMAX) 구조로서 제안한다. ROSMEX 구조에서는 먼저 초기 네트워크 진입 과정의 보안성 제공을 위해서 DH 키교환을 적용한다. 이 방안은 SS와 BS사이의 primary 관리 통신과정의 암호화된 통신을 위하여 임시 Security Association(pre-TEK, pre-defined cryptographic suite)을 할당한다. 그러므로 본 제안 방안은 초기 네트워크 진입 과정중 SBC 협상 과정전에 DH 키교환을 통해 형성된 임시 TEK를 사용하여 무선 통신 구간의 신뢰성 있는 통신을 제공할 수 있다. 또한 ROSMEX 구조는 Mobile WiMAX 네트워크 도메인간 통신에 PKI를 기반으로하는 신뢰성 있는 통신을 제공한다. 물론 단순한 PKI기반 키교환 구조를 Mobile WiMAX의 모

표 4. 제안 방식의 비교 검증
Table 4. Verification of Proposed Approaches.

	네트워크 초기구간	Access 네트워크구간	핸드오버 구간
기존안	보안기능 미제공	IPSec등 권고	Handover옵션에서 보안기능 미제공
제안 방식	Ranging과정에 DH키분배 적용	인증서 기반 세션키 분배방식 적용	Fast Handover중에도 상호인증 적용
강점	네트워크 초기과정의 보안파라미터에 대한 암호화 가능	네트워크 양단간 IPSec설정 없이 인증서를 통한 상호인증	핸드오버를 위한 메시지 교환 중 상호인증가능
적용 타당성	Ranging 과정의 파라미터를 사용	IPSec 미지원 장비에서 적용가능	추가적인 인증 메시지 교환 불필요

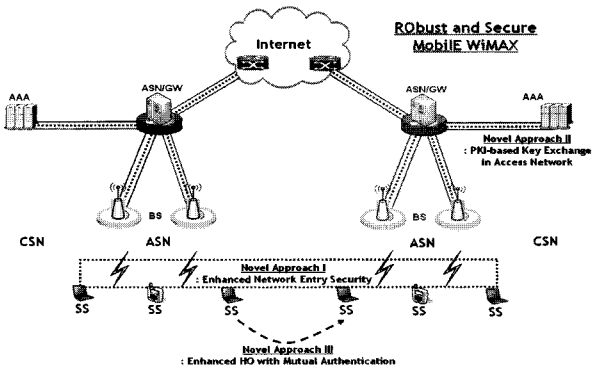


그림 7. 강건하고 보안성 있는 모바일 와이맥스 네트워크 구조
Fig. 7. Robust and Secure Mobile WiMAX Network Architecture.

든 통신 개체들에게 적용하기 위해서 아직 고려해야 할 몇몇 사항들이 남아있긴 하지만, 도메인간 통신에 있어 신뢰성 있는 수단이 필요하고 하나의 대안으로서 PKM의 디바이스 인증서 기반 신뢰 구조를 확장시키는 것으로 적용 가능성이 있다. 이 방법은 기존의 IPSec을 사용하는 것과 같은 제한적 통신 개체들 간의 보안성 제공 방안보다는 보다 효율적으로 기밀성 제공이 가능하다. 마지막으로 ROSMEX는 Mobile WiMAX의 가장 큰 특징 중의 하나인 이동성 지원 기능에 있어 효율적으로 기밀성을 제공할 수 있다. 앞서의 설명과 같이 Mobile WiMAX의 HO 최적화 옵션들의 사용은 기본적으로 빠른 HO제공을 목적으로 하기 때문에 핸드오버

과정중 인증이나 키생성 등을 최소화하려고 한다. 그러므로 제안하는 구조에서는 이러한 HO 최적화 옵션의 사용과 함께 이전 HO 초기화 과정에서 새로운 필드의 추가로서 부가적인 메시지 교환없이 효율적인 상호 인증 기능을 제공하였다.

즉, ROSMEX 구조는 근본적으로 기존 Mobile WiMAX 네트워크의 보안성 향상을 목표로 하는 구조이며, 제안한 방안들의 실현을 통해 새롭게 요구되는 보안 요구사항들의 충족은 물론이거니와 성능적 요구사항들을 충족시킬 수 있다.

VI. 결 론

Mobile WiMAX는 광대역 무선 접속을 위한 사용자의 요구를 충족시켜주는 가장 적합한 차세대 통신 시스템 후보 중의 하나이다. Mobile WiMAX는 world-wide roaming, 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 Mobile WiMAX는 3G와 4G를 연계하는 좋은 대안일 뿐 궁극적인 솔루션으로 아직 자리 잡지 못하고 있는 실정이다. 특히 보안 관점에서 몇몇 취약성을 내포하고 있다.

본 논문에서는 초기 네트워크 진입 과정에서의 보안 context 노출 취약성, Mobile WiMAX 네트워크 도메인 간 기밀성 부족, 그리고 핸드오버 과정 중 SS와 BS간 상호 인증 부재 등의 취약성을 살펴보았다. 이러한 Mobile WiMAX 보안 취약성을 해결하기 위하여, DH 키교환을 적용, PKM기반 디바이스 인증서를 적용하는 와이맥스 네트워크의 PKI, 핸드오버 메시지 교환과정 중의 상호 인증 방안 등의 세 가지 대응방안을 제시하였으며, 제시된 대응방안들을 기반으로 한 ROSMEX 보안 구조를 제안하였다.

제안된 Mobile WiMAX 보안 구조는 Mobile WiMAX 네트워크/시스템을 보다 안전하고 강건하게 만드는데 도움을 주리라 사료되며, 향후에는 제안된 대응 방안들에 대한 시뮬레이션 및 실제 망 적합성 시험 등이 필요하다.

참 고 문 헌

[1] IEEE Standard for Local and Metropolitan Area Networks Part 16: Air Interface for Fixed Broadband Wireless Access Systems, IEEE Std 802.16-2004. IEEE, 2004.

[2] IEEE Standard for Local and Metropolitan Area Networks Part 16: Air Interface for Fixed Broadband Wireless Access Systems, Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands and Corrigendum, IEEE Std 802.16e-2005. IEEE, 2005.

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

[4] WiMAX Forum (2005): Fixed, nomadic, portable ad mobile applications for 802.16-2004 and 802.16e WiMAX networks.

[5] W. Diffie, M. E. Hellman, New directions in cryptography, IEEE Transactions on Information Theory 22 (1976), 644 - 654.

[6] WiMAX Forum (2006): WiMAX End-to-End Network Systems Architecture - Stage 2

[7] WiMAX Forum (2006): WiMAX End-to-End Network Systems Architecture - Stage 3

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

[9] C. Wullems, K. Tham, J. Smith, M. Looi, A Trivial Denial of Service Attack on IEEE 802.11 Direct Sequence Spread Spectrum Wireless LANs, Proceedings of the 2004 Wireless Communications Symposium. IEEE, 2004.

[10] R. Boshonek,Advanced Denial of Service Techniques in IEEE 802.11b Wireless Local Area Networks, Naval Postgraduate School Master's Thesis, June 2002.

[11] W. Meyers, Exploitation of an IEEE 802.11 Standard Wireless Local Area Network through the Medium Access Control (MAC) Layer, Naval Postgraduate School, Master's Thesis, June 2001.

[12] D. D. Boom, Denial of Service Vulnerabilities in IEEE 802.16 Wireless Networks, Master's thesis, Naval Postgraduate School, CA, 2004

[13] D. Johnston, J. Walker, Overview of the 802.16 Security. IEEE computer society, May/June 2004

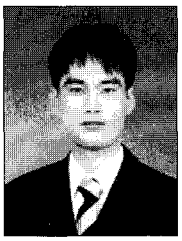
[14] M. Barbeau, WiMax/802.16 threat analysis, Source International Workshop on Modeling Analysis and Simulation of Wireless and Mobile Systems archive, Proceedings of the 1st ACM international workshop on Quality of service & security in wireless and mobile networks, Montreal, Quebec, Canada, pp 8~15, 2005.

[15] C.H. Park, Y.H. Oh, "와이브로기반의 서비스영역 확대와 핸드오프 보장에 관한 연구", 대한전자공학회, 전자공학회논문지, 제43권 TC편 제5호, 2006. 5, pp. 113~120
[16] W. Choi, T. S. Shon, H. H. Choi, Y. Lee, "IEEE 802.16 기반의 무선 액세스 망에서 Unlicensed 대역 액세스 릴레이에 대한 설계", 대한전자공학회, 전자공학회논문지, 제44권, TC편 제10호, 2007. 10, pp. 169~177

저 자 소 개

손 태 식(정회원)
2005년 아주대학교 정보 및 컴퓨터공학부 졸업
2002년 아주대학교 컴퓨터공학 석사
2005년 고려대학교 정보보호학 박사
2004년~2005년 Research Scholar, Univ. of Minnesota
2005년~현재 삼성전자 DMC 연구소 책임연구원
<주관심분야 : Wireless/Mobile Network Security, Wireless Sensor Network, Anomaly Detection>

최 효 현(정회원)-교신저자
1994년 서강대학교 전자계산학 학사
1996년 서강대학교 컴퓨터공학 석사
2005년 서강대학교 컴퓨터공학 박사
2005년~2009년 삼성전자 통신연구소 책임 연구원
2009년~현재 인하공업전문대학 컴퓨터정보과 조교수
<주관심분야 : Ubiquitous Sensor Network, Wireless Mesh Network, Mobile Ad hoc Network, Routing Protocol, Group Mobility>



구 본 현(정회원)
2005년 동서대학교 정보통신공학과 학사
2007년 고려대학교 정보보호대학원 석사
2007년~현재 삼성전자 DMC 연구소 선임연구원
<주관심분야 : Mobile Security, Wireless Sensor Network, Visualization>