보안성이 강화된 타원곡선 암호 기반의 Mobile WIMAX 초기 진입 구간

정회원 최 도 현*, 박 중 오**°, 전 문 석***

ECC Based Mobile WIMAX Initial Network Entry with Improved Security

Do-hyun Choi*, Jung-Oh Park**°, Moon-Seog Jun*** *Regular Members*

요 약

(4G)세대 이동통신 기술인 Mobile WIMAX 환경에서 네트워크 초기진입 구간은 평문 Parameter 노출 되는 취약성이 존재한다. 각 노드의 메시지의 유출 및 제 3자의 공격을 예방하기 위해서는 메시지의 암호화가 요구된다. 본 논문은 타원곡선 암호가 적용된 Mobile WIMAX 네트워크 초기 진입 구간을 제안한다. OPNET 시뮬레이터를 이용해 기존 모델와의 성능 비교를 하였으며, 시뮬레이션 결과 기존 초기 진입 구간에 비해 다소 지연율이 증가하였으나 암호화가 적용된 기존의 연구에 비교하여 평균 지연율 및 처리율이 효율적인 것으로 나타났다.

Key Words : Mobile WIMAX, Wibro, 802.16, 4G, OPNET

ABSTRACT

Initial entry section has vulnerability which exposes plain text parameter in Mobile WIMAX environment which is the 4th generation technology. Each node message need to be encrypted to prevent the third party attack or message leakage.

In this paper, we propose Mobile WIMAX initial entry section encryption using Elliptic Curve Cryptosystem. We have compared proposed model with existing model using OPNET simulator tool. he delay rate has increased little bit in initial entry section than before after the comparison, but it has shown more effective in average delay and throughput than encryption applied other existing model.

Ⅰ. 서 론

인터넷이 발전함에 따라 무선 환경에서도 사용자들은 점점 더 높은 데이터 전송율을 제공할 수 있는 시스템을 요구하고 있다. 무선 엑세스 망에서 이러한 사용자들의 요구를 충족시키기 위해 IEEE 802 LMSC(LMSC, LAN/MAN Standards Committee (Project 802)에서는 IEEE 802.16 워킹그룹을 신설하고 IEEE 802.16 계열을 표준화 하였다.[6] 이 기술은 국외에서는 Mobile WIMAX 국내에서는 WiBro로 알려져 있다. 기존 3세대 무선통신 기술은 현재 무선통신 시장에서 사용자에게 데이터 서비스를 제공하기 위한 한계를 드러냄에 따라 각 국내외 이동통신 기업에서는 이를 해결하기 위한 기술로 LTE(Longterm Evolution), WIMAX(WiBro)등 4세대 기술을 중점으로 상용화를 준비하고 있다. 현재 Mobile 시장은 국내 이동통신 가입자 수 2007년 말 4,350만 명으로 전체 인구대비 90.6%을 기록하

* 숭실대학교 컴퓨터학과(cdhgod@nate.com, mjun@ssu.ac.kr),
** 성결대학교 정보산업기술연구소(jopark02@sungkyul.edu), (° : 교신저자)
논문번호 : KICS2011-07-293, 접수일자 : 2011년 7월 14일, 최종논문접수일자 : 2011년 10월 30일

여 이미 시장 포화에 근접하였으며 2009년 전 세계 Mobile 시장의 보급률은 66.7%, 2013년 87.9%에 이를 전망이다.[1] 2010년 스마트폰 사용자가 크게 증가하면서 앞으로 4(G)세대 기술이 상용화에 따른 단말기 및 Contents 요금제 등의 성장에 따라 가입자 전체가 데이터 서비스를 이용하게 될 것이며 이는 모바일 트래픽이 크게 증가할 것으로 예상된다.

IEEE 802.16m 표준에는 무선통신 보안을 위한 사용자 인증, 키 관리, 암호화 등 보안기능을 관리하는 Private Sublayer라는 보안부계층이 존재한다.[5]

현재 Mobile WIMAX의 보안성 강화에 대한 연구는 대부분 이 보안부계층을 부분을 중심으로 이루어졌다. 보안부계층의 기능은 네트워크 초기 진입 과정 이후 진행된다. 본 논문에서는 이 초기 진입 과정의 메시지 교환 구간을 Ranging 구간이라 정의한다. Ranging 구간에서 생성되는 메시지들은 암호화 기능을 제공하지 않기 때문에 평문으로 노출되는 Mobile WIMAX의 취약성 중 하나이다.[2] 본 논문은 Mobile WIMAX의 초기진입구간의 평문노출 문제를 해결하기 위해 네트워크 초기 진입 구간에 타원곡선 암호를 적용하였으며 실제 Mobile WIMAX 네트워크에 서비스 품질(Quality of Service)의 효율성을 분석하기 위해 OPNET 시뮬레이터를 이용하여 비교분석을 진행하였다.

본 논문은 2장 관련연구에서는 기존 암호화가 적용된 연구의 문제점을 분석하고, 3장에서는 본 논문의 제안, 4장에서는 성능분석, 5장 결론으로 마친다.

Ⅱ. 관련연구

Mobile WIMAX의 네트워크 초기진입 구간은 가입자 단말기가 기지국에 등록되는 과정을 의미한다.

Mobile WIMAX의 기본 구성요소에는 가입자(SubScriber), 기지국(BaseStation), 서버(AGN GW)가 존재한다. 각 노드는 연결 정보를 유지하기 위해서 다양한 프로세스 과정을 진행한다. 이 과정에서 초기진입 구간에 대한 암호화 적용 이후 성능분석을 위해서는 일반적인 시뮬레이션 분석결과와는 다른 Mobile WIMAX 망의 실제 환경을 고려한 종단간 서비스 품질 분석이 필요하다.

2.1 Novel Approaches to Enhance Mobile WIMAX Security[3]

본 관련 연구는 Mobile WIMAX의 알려진 MAC와 identity 취약성을 이용한 Auth-Invalid 취약성, Rogue BS 취약성, RNG-RSP 공격, RNG-CMD 공격, Auth-Reject 등 다양한 DoS 공격들의 취약성을 가능하게 하는 네트워크 진입 과정에 MAC 관리 메시지들에 대한 Security Context들의 노출문제를 해결하기 위해 RSA 공개키 암호를 적용했다.[7],[8]

Mobile WIMAX의 보안 계층의 PKMv2 보안 기능은 통신을 요청한 가입자 단말의 초기 네트워크 진입 과정을 끝마친 후 적용된다는 문제점이 존재한다. 그림 1과 같은 초기 Ranging 구간의 DH 키 교환을 통해서 생성된 pre-TEK를 통해서 SBS 협상과 Security Context 교환과정의 기밀성을 제공하였다.

초기 통신 코드로 사용되는 Ranging 코드를 수신하여 설정하는 과정에서 SS는 BS가 보낸 UL-MAP의 포함된 Ranging 코드중 하나의 Ranging 코드를 선택한다. 이 때 선택된 코드를 DH 키 교환의 랜덤넘버 'p'를 생성하는데 사용하고, 'p'로부터 원시근인 'q'를 생성하여 DH 키 교환의 전역 파라미터로 사용한다. 이후에는 RSA 암호화 과정을 따라 각각의 'p', 'q'를 이용하여 공개키/개인키를 생성하고 이후 공개키 교환, 개인키를 이용한 검증, 공유키(pre-TEK) 생성을 진행한다.

Ranging 과정의 파라미터를 사용하여 암호화를 적용하고 Mobile WIMAX의 시스템 변경 없이 신뢰성 있는 통신을 제공하였지만 실제적인 망에서 QoS 요구사항을 위한 종단간 성능분석은 이뤄지지 않았다. 일반적으로 Mobile WIMAX의 네트워크 망에서 다수의 가입자가 하나의 서비스 네트워크에 오랫동안 머물러 있을 경우, 단말의 인증을 위한 인

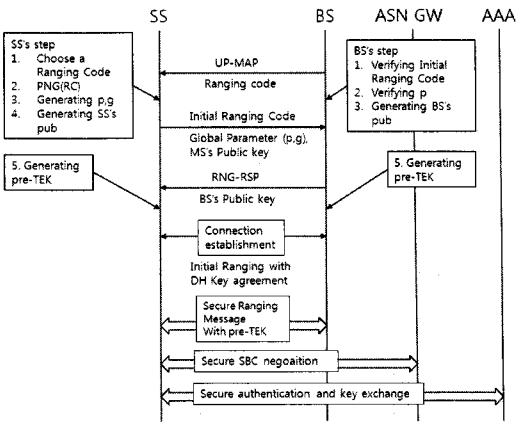

그림 1. RSA 암호가 적용된 초기진입 구간

증 벡터 분배를 각 단말에 대해 여러 번 수행해야 한다. Ranging 구간의 암호화 적용은 다수 서버들(AAA)의 Diameter 프로토콜 동작을 요구하는 네트워크 노드 사이의 Bandwidth Consumption 문제를 증가시키는 원인이 된다. 현재 RSA 암호 기반에서 안전하다고 알려진 1024bit 키는 Ranging 구간의 메시지(Ranging Code : 144bit)보다 비교적으로 그 키 사이즈가 매우 크다. 이것은 암호화로 인한 초기 진입 구간의 재협상에 따른 연산상의 오버헤드, 인증 벡터의 저장 공간의 증가 시킬 수 있는 문제가 될 수 있다.

최근 국내 공인인증기관은 공인인증서의 보안성을 강화하기 위해 RSA 키 길이를 기존 1024bit 체계에서 2048bit 체계로 전환하여 사용하고 있다. RSA는 안전성이 키 길이 의존하는 단점을 가지고 있기 때문에 앞으로 4세대 이동통신망에서의 응용 및 확장에는 적합하지 않다. 각 노드 사이의 Bandwidth Consumption 문제는 최근 스마트 폰의 무제한 요금제로 인한 무선 트래픽 부하 문제를 더욱 악화시키는 원인 중 하나이다.

2.2 Performance of WIMAX Security Algorithm[4]

본 관련 연구는 Mobile WIMAX 모델의 초기 진입 구간인 Initial Ranging, Registration, Bandwidth Requests 등 MAC Layer의 물리계층에 Scrambling 과 jamming의 공격 위험성에 대한 취약성[9],[10]을 해결하기 위해 SS(MS)와 BS 노드 사이의 보안 협상과정을 Data SA, Authorization SA로 구분하였다.

기존 X.509 인증서를 이용한 WTLS 인증 방식을 이용하였고, AK(Authentication Key), TEK(Traffic Encryption Key)생성과 키 교환 과정에 RSA 1024bit 키가 아닌 ECC 기반의 163bit 키를 이용하여 연산상의 오버헤드, 메모리 공간 오버헤드를 효율적으로 처리하고자 하였다.

그림 2는 제안 모델의 보안 메카니즘을 나타낸다.

성능분석 결과 RSA의 경우 100ms에서 125ms, ECC의 경우 80ms에서 110ms로 ECC가 RSA보다 지연 성능이 효율적으로 개선되었지만 본 관련연구의 성능분석에 사용된 파라미터는 단일 파라미터로 Mobile WIMAX 네트워크 노드 상의 가입자의 단말기부터 인증서버까지의 종단간 성능분석으로 적합하지 않다. 또한 암호화 범위가 초기진입 구간의 평문 대상이 아닌 등록과정 이후에 해당되며 표준 프로세스 과정을 변경해야 하는 단점이 존재한다.

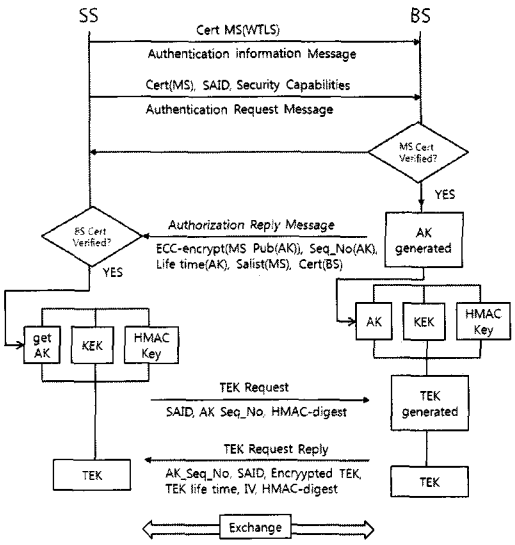

그림 2. X.509 인증서 and ECC 기반의 초기진입 구간

2.3 Mobile WIMAX Parameters Analysis

Mobile WIMAX 환경에서 Ranging 구간의 서비스 플로우와 각 파라미터들은 단말과 기지국 양쪽 모두에서 어디서나 일관성 있는 방법으로 암호화를 진행해야 한다. 모든 트래픽은 연결에 의해 전달되며, IP와 같은 비 연결형 프로토콜을 구현하는 서비스 플로우의 경우에도 이와 같은 연결에 의해 전달된다.[5] Initial Ranging은 초기 진입 과정의 가장 기본적인 과정으로 초기 네트워크 진입 시 실행된다.

각 MAC 인터페이스를 통과하는 패킷들에서 맵핑되어 식별되는 CID(Conenction ID)와 같은 고유한 파라미터는 각 노드상의 메시지에 포함되어 초기 접속을 위해 스캔 시도 후 Ranging 및 등록단계의 MAC 관리 메시지를 의미한다. 단말기와 기지국의 생성되는 초기 진입 구간의 파라미터들은 암호화 및 키 관리(Privacy Key Management)과정에서 사용된다.[5]

Mobile WIMAX의 MAC Management 메시지들은 MAC PDU의 Payload에 실려 전송되며 모두 Message Type 필드로 시작된다. DCD, UCD, UL-MAP, DL-MAP은 프레임의 구조와 대역 할당, 그리고 물리 계층 파라미터를 직접 규정하는 대표적인 관리 메시지로 Ranging 구간 초기에 생성되는 파라미터들이다. RNG-REQ 메시지는 초기화할 때 그리고 초기화 이후에 주기적으로 통신망 지연을 결정하고, 파워 또는 하향링크 burst profile의 변경을 요구하기 위해 단말에 의해 전송되는 메시지이다.

기지국은 RNG-REQ의 응답으로 RNG-RSP를 전송하는데 이 메시지는 수신한 다른 데이터 또는 MAC 메시지들 상에서 측정된 값에 따라 수정값(correction)을 전송하기 위해 비동기적으로도 전송될 수 있다.

RNG-REQ, RNG-RSP 메시지의 Parameter 분석 결과 각각의 고유한 정보를 생성하고 키 교환 과정에서 사용되는 Parameter들이 포함되는 것을 확인할 수 있다. 두 메시지는 단말기의 MAC_ADDRESS, 기지국(BS)의 ID, 현재 상태를 나타내는 Connection ID 뿐만 아니라 기지국이동이나 HANDOVER시 사용되는 HO ID, Controller ID, Ranging Code 속성 등 노출 시 공격 대상 정보로 될 수 있는 정보이다.

이 정보들은 Ranging Code(144비트)에 포함하여 총 두 구간에 걸쳐 메시지가 교환된다.

단말기는 RNG-RSP를 수신할 수 있도록 언제든지 준비해야 하기 때문에 Ranging 과정의 암호화는 Mobile WIMAX 망의 성능에 영향을 주게 된다. Ranging이 완료 이후 단말은 링크가 설정되고, 기지국에 의하여 관리가 가능하도록 등록과정을 진행한다.

Ⅲ. 제안 시스템

Ranging 구간에 암호화 적용 시 다수의 단말기에 대한 Bandwidth Consumption 문제를 해결하려면 암호화 적용 시 효율적인 암호화 알고리즘 및 키 교환 알고리즘의 적용, 암호화 파라미터 등 다양한 고려사항이 요구된다. Ranging 구간에 타원곡선 암호화 알고리즘의 적용을 위한 가정사항은 표 1과 같다.

표 1. 암호화 알고리즘 적용을 위한 가정

No.	Description
1	802.16M Mobile WIMAX의 표준 프로세스 과정을 준수한다.
2	RSA(1024bit)에 강도에 비례하는 타원곡선 160비트 키를 사용한다.
3	연산이 효율적이고 간단한 유한체 F상(GF(p))의 타원곡선을 사용한다.
4	연산 및 확장성을 위해 원소 표현방법을 선택 가능하게 한다.
6	단말기와 기지국은 이미 사전에 동의한 타원곡선 정의하고 있다.
7	인증 서버(AAA)는 신뢰할 수 있는 서버이다.

3.1 타원곡선 암호 정의

본 논문에서는 타원곡선 기반의 ElGamal 암호 방식과 Diffie-Hellman 키 교환 알고리즘을 사용한다. 유한체 GF(2p)를 기반의 타원곡선은 이동통신 기기 기반의 환경에서 VLSI chip 같은 특수목적 연산장치(Chip)에 구현에 적합하다. 또한 원소 표현 방법의 선택 가능하게 하여 확장성을 고려한다.

체 F상의 타원곡선의 구현 용이성을 위해 암호화 과정에서 사용되는 난수는 정수값을 이용하고, SS와 BS는 이미 사전에 동의한 타원곡선을 정의한다.

표 2는 본 논문에서 사용되는 암호화 알고리즘에서 사용되는 파라미터를 나타낸다.

표 2. 암호화 알고리즘 파라미터

No.	Parameters	Description
1	BSPr_Key	Basestation's Private Key
2	BSPu_Key	Basestation's Public Key
3	SsPr_Key	Subscriber's Private Key
4	SsPu_Key	Subscriber's Public Key
5	M	Message
6	r	Random Integer Number
7	Ss_S_1, Ss_S_2	Subscriber's Digital Signature
8	BS_S_1, BS_S_2	Basestaion's Digital Signature
9	Ts	Time Stamp
10	Ss_C	First Ranging Node's CiperText
11	BS_C	Second Ranging Node's CiperText

3.1.1 키 생성 및 서명 생성

각 개인키와 공개키의 생성은 ElGamal 기반의 타원 곡선 알고리즘, 타원곡선 기반의 디지털 서명 구조(ECDSA)를 이용하고, 해쉬 함수는 SHA-1 160비트를 사용한다. 서명값은 동기화과정 이전에 제 3자가 메시지를 가로채어 저장한 후 재전송 공격을 방지를 위한 타임스탬프를 포함한다. 표 3은 각 키 생성과 디지털 서명을 생성하는 방법을 나타낸다.

모듈로 p 덧셈연산으로 얻는 타원곡선을 $E_p(a, b)$로 정의한다. 공개키로 선언되는 파라미터는 사전에 동의한 타원곡선p, $E_1(a_1, b_1)$, $E_2(a_2, b_2)$이다. r값은 Ranging Code 생성 시 사용되는 Code Set을 이용한 임의의 수이다. SS와 BS는 한 쌍의 암호문과 서명(가입자 예 : (r x $E_1(a_1, b_1)$, MS_C), (MS_S_1, MS_S_2))을 생성한다. 첫 번째 암호문은 첫 번째 서명과 같이 r값과 타원곡선 상에 선택된 좌표의 곱에 의해 생성되는 값으로 생략되며 첫 번째 서명을 암

표 3. 개인키 및 공개키 생성과 디지털 서명 생성

No.	Parameters	Description
1	BsPr_Key	163bit Interger Number
2	BsPu_Key	$E_1(a_1, b_1)$ $E_2(a_2, b_2) = E_1(a_1, b_1) \times BsPr\_Key$
3	SsPr_Key	163bit Integer Number
4	SsPu_Key	$E_1(a_1, b_1)$ $E_2(a_2, b_2) = E_1(a_1, b_1) \times SsPr\_Key$
5	Ss_S_1, Ss_S_2	$Ss\_S_1 = r \times E_1(a_1, b_1)$ $Ss\_S_2 = (h(M\|\|Ts) + SsPr\_Key \times Ss\_S_1)r^{-1} \bmod q$
6	Bs_S_1, Bs_S_2	$Bs\_S_1 = r \times E_1(a_1, b_1)$ $Bs\_S_2 = (h(M\|\|Ts) + BsPr\_Key \times Bs\_S_1)r^{-1} \bmod q$
7	r	Ranging Code set h(M + L + 0 / mod 256)

호화와 복호화에 파라미터로 사용하여 연산의 효율성을 증가시켰다.

3.1.2 암호화 및 복호화

가입자와 기지국은 표 4와 같이 암호화와 복호화를 진행한다. 평문 M, 임의의수 r, 타원곡선 상의 점 E_2을 이용하여 암호화를 진행하고, 복호화의 경우 자신의 개인키와 각 전송받은 디지털 서명을 이용하여 복호화를 진행한다.

가입자와 기지국은 그림 3과 같이 전송된 암호문에서 복호화된 메시지 M과 디지털 서명을 이용하여 검증을 진행한다.

표 4. 암호화와 복호화 과정

No.	Parameters	Encryption	Decryption
1	Ss_C	$Ss\_C = M + r \times E_2(a_2, b_2)$	$M = Ss\_C - (SsPr\_Key \times Ss\_S_1)$
2	Bs_C	$Bs\_C = M + r \times E_2(a_2, b_2)$	$M = Bs\_C - (BsPr\_Key \times Bs\_S_1)$

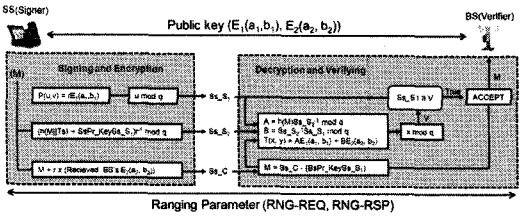

그림 3. 키 분배 및 검증 과정

3.2 제안 시스템의 프로세스 과정

본 논문에서 제안하는 타원곡선 기반의 Ranging 구간은 초기 진입 시 진행되는 Initial Ranging(초기 파라미터 생성), Periodic Ranging(기지국 내에서 핸드오버), HANDOVER Ranging(기지국 간 핸드오버) 총 3가지 과정으로 분류된다. ECC가 적용된 범위는 Ranging 구간에서 평문 노출 시 취약성의 원인이 되는 RNG-REQ와 RNG-RSP 메시지이다.

3.2.1 Initial Ranging

Initial Ranging은 Ranging 과정은 그림 4와 같이 진행된다. 초기에 가입자가 요청한 대역폭 요청에 사용될 수 있는 Ranging Code 집합과 기지국의 공개키를 전송한다. 각 두 구간은 전송 중 받은 서명과 암호문을 이용하여 메시지를 검증한다.

첫 번째 구간에서 선택된 Ranging Code(M)를 이용하여 생성된 디지털 서명과 암호문을 임의의 Ranging 서브채널을 이용하여 기지국에 전송한다. 해당 가입자는 기지국으로부터 받은 정보에 자신의 Ranging Code와 일치하는 정보가 없을 경우 다시 Re-request 요청을 보낸다. 일치할 경우 기지국은 재조정된 Ranging Code(M)을 이용하여 생성된 디지털 서명과 암호문을 가입자에게 전송한다. 두 번째 구간은 Ranging Code 수신에 대한 응답으로 디지털 서명과 암호문을 전송하고 기지국은 응답으로 다시 디지털 서명과 암호문을 전송하여 성공적으로 Ranging을 마치고 이후 Negotiation 과정으로 진입하게 된다.

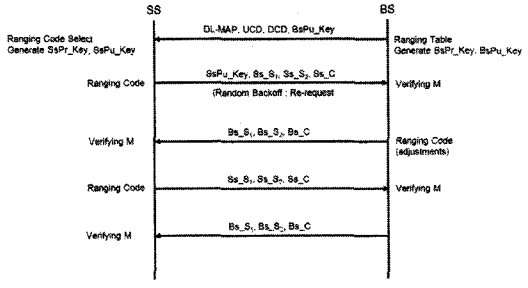

그림 4. ECC가 적용 된 Initial Ranging

3.2.2 Periodic Ranging

Periodic Ranging은 보내는 메시지의 속성과 옵션으로 추가되는 정보 이외에는 과정이 같다. 기지국 내에서 가입자 단말기가 HANDOVER 발생 이후 인접한 기지국 정보를 그대로 유지하면서 획득

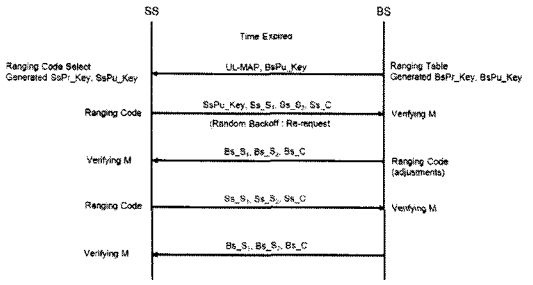

그림 5. ECC가 적용 된 Periodic Ranging

한 상, 하향 링크를 재수정 및 갱신을 위한 Ranging 과정으로 그림 5와 같이 이전에 생성된 개인키와 공개키를 이용하여 Ranging을 수행한다.

3.2.3 HANDOVER Ranging

현재 연결을 유지하고 있는 기지국의 Sector에서 벗어나 다른 기지국의 Sector에 인접할 경우 발생하는 HANDOVER Ranging은 기지국의 변경으로 인해 새로운 키 생성과 교환이 필요하다.

단말기는 핸드오버 이전에 단말기와 기지국이 가지고 있는 Active List에 등록되어 있는 근접 기지국간에 사용자의 공개키를 공유한다. 그림 6과 같이

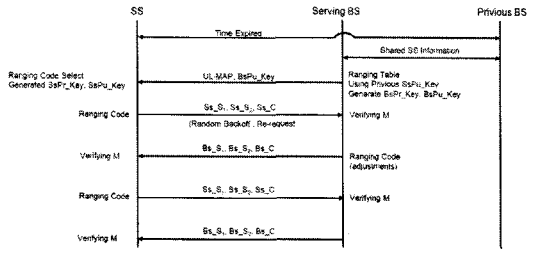

그림 6. ECC가 적용된 HANDOVER Ranging

핸드오버 요청 시 인접 기지국은 Backbone상에서 공유되어 있는 가입자의 공개키를 이용하여 암호화된 메시지를 교환한다.

Ⅳ. 성능평가

WIMAX 모델의 성능분석을 위한 구성 요소로는 사용자 기기(SS), 유선망 종단에서 무선 액세스 기능을 제공하는 기지국(BS), 기지국 제어 및 코어 망의 연결을 담당하는 장비인 서버, ASN GW 모델의 필요한 모든 기능은 기지국의 서버가 가지고 있기 때문에 구성요소에서 제외한다. 그림 7은 본 논문의 시뮬레이션 네트워크 구성도를 나타낸다.

MCS(Modulation Coding Schema)는 레벨 QPSK 1/2 기준으로 10분 동안 시뮬레이션 테스트를 진행하였다. 본 논문의 시뮬레이션은 단일 노드와 다중 노드를 포함하여 모든 항목에 대해 10Mb의 트래픽을 발생시켰다.

4.1 Application Result

그림 8-13은 수치는 Delay(sec)와 Traffic Received (bits/sec)로 지연율과 트래픽 전송에 대한 그래프를 나타내며 각 항목은 평균값과 최대수치를 나타낸다.

표 5는 위의 시뮬레이션 결과로 어플리케이션 별 Delay(sec)와 Traffic Recevied(bits/sec) 수치를 나타내고 각 항목은 평균값과 최대수치를 나타낸다.

암호화 적용 이후 각 어플리케이션 항목의 평균 지연속도는 약 0.01(sec) 증가, 평균 트래픽 전송률이 약간 감소하였다. Heavy Browsing 프로필의 경우 웹 브라우징에 의한 요청과 응답으로 인해 트래픽이 불규칙적인 것으로 나타났으며 High Revoulution Video의 경우 지연과 전송량이 차이가 없는 것을

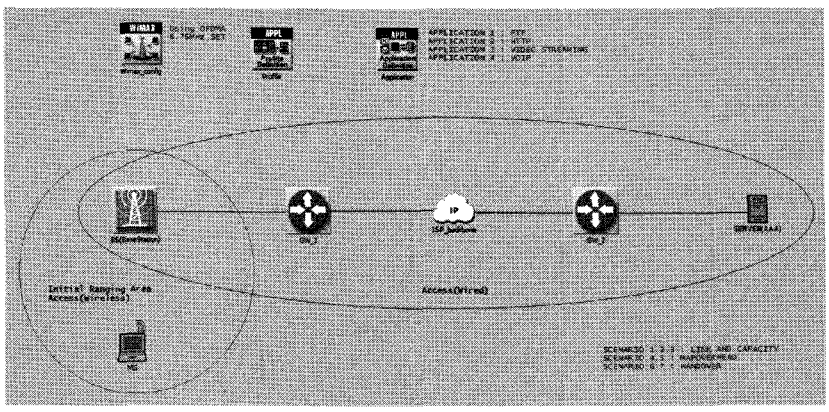

그림 7. 시뮬레이션 네트워크 구성도

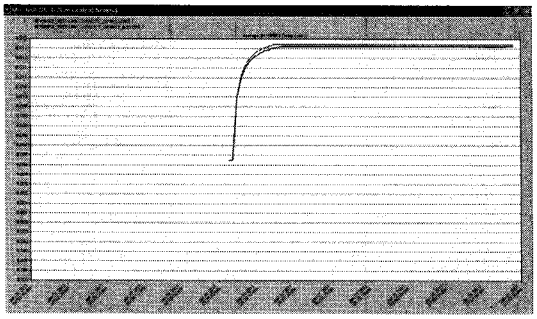

그림 8. Ftp Download - Delay/sec

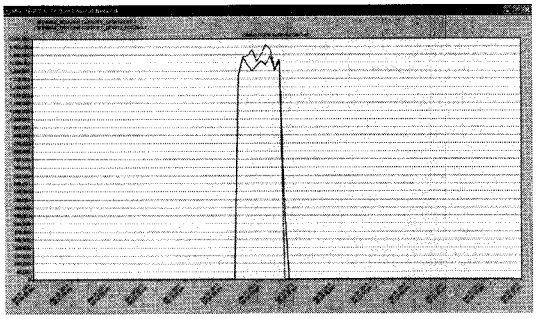

그림 9. Ftp Download - Traffic Received(bits/sec)

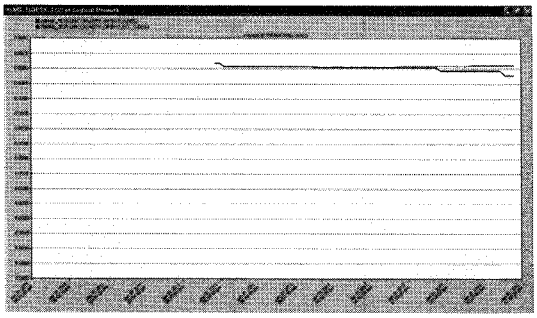

그림 10. Heavy Browsing(Profile Set) - Delay/sec

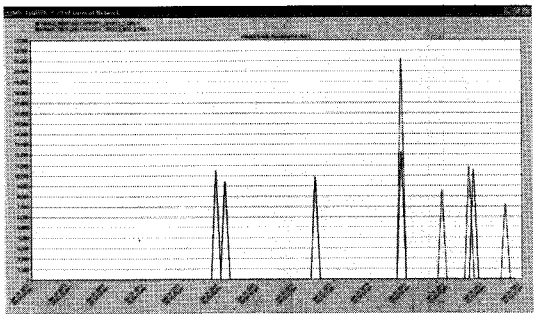

그림 11. Heavy Browsing(Profile Set) - Traffic Received (bits/sec)

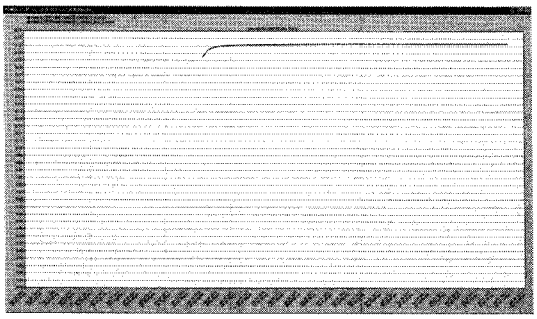

그림 12. High Revolution Video(Profile Set) - Delay/sec

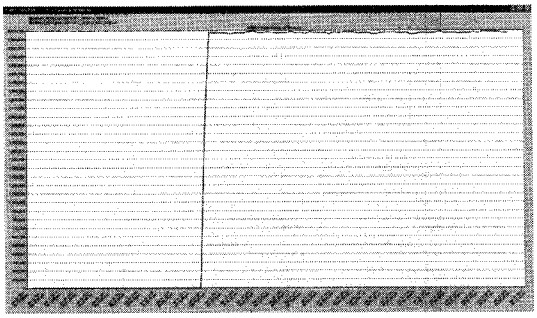

그림 13. High Revolution Video(Profile Set) - Traffic Received (bits/sec)

표 5. 어플리케이션 별 지연과 전송률

Application Result	Delay(sec)		Traffic Received (bits/sec)	
FTP Download(None ECC)	0.012103	0.012805	138,051	1,389,855
FTP Download(Apply ECC)	0.012220	0.012994	138,049	1,460,580
Heavy Browsing(None ECC)	0.006779	0.007176	774.68	21,193
Heavy Browsing(Apply ECC)	0.007104	0.007200	525.15	12,240
High Revolution Video(None ECC)	0.012103	0.012805	138,051	1,389,855
High Revolution Video(Apply ECC)	0.012220	0.012994	138,049	1,460,580

확인했다.

4.2 MAP Overhead

매 프레임마다 전달되는 MAP 정보의 오버헤드를 측정하기 위해 SS를 각각 20대와 100대의 단말기를 설정하고, 짧은 시간 주기적 데이터를 확인할 수 있는 VoIP 프로필을 적용하였다. 그림 14는 각 단말기의 MAP 사용률을 나타낸다.

표 6과 같이 VoIP 프로필을 적용한 MAP 프레임의 Overhead는 ECC를 적용한 경우 기존 모바일 기기 20대를 기준으로 약 2% 증가한 것으로 나타났다. 각 항목은 평균값과 최대수치를 나타낸다.

100대의 기준으로 MAP 프레임의 오버헤드는 ECC를 적용한 경우 오버헤드가 증가수치가 평균 0.1% 미만으로 이것은 적용된 ECC가 Mobile WIMAX 시스템에 큰 영향을 끼치지 않음을 알 수 있다.

표 6. VoIP를 적용한 MAP Overhead의 사용률

MAP Overhead	Frame MAP (20 Devices)	Frame MAP (100 Devices)
VoIP(None ECC)	18.117 %	53.162 %
VoIP(Apply ECC)	20.158 %	53.215 %

4.3 HANDOVER

그림 15, 그림 16은 두 BS 사이에서 SS가 2km 이동하여 HANDOVER 발생 시 단말기의 지연과 전송률 분석결과를 나타낸다. Profile은 FTP download (10Mb)의 트래픽을 동일하게 적용하였다.

표 7은 HANDOVER에서 발생한 패킷의 시뮬레이션 분석결과를 나타낸다. 평균 지연이 약 0.001(sec) 증가한 것으로 나타났다. 각 항목은 평균값과 최대수치를 나타낸다.

표 8은 다중사용자로 인한 트래픽 부하에 따른

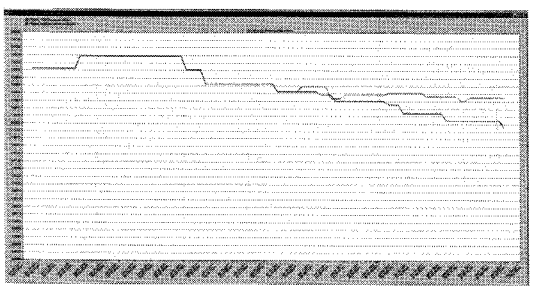

그림 15. HANDOVER - Delay/sec

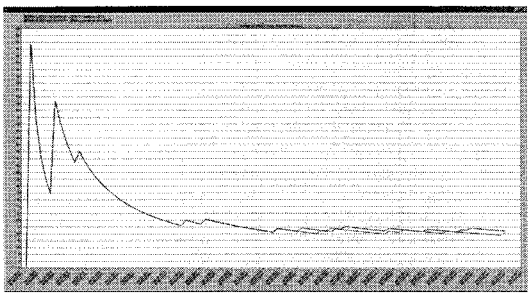

그림 16. HANDOVER - Traffic Received(bits/sec)

표 7. HANDOVER (FTP Ddownload)

HANDOVER	Delay(sec) (100 Devices)		Traffic Received (bits/sec) (100 Devices)	
FTP Download (None ECC)	0.0460020	0.0801000	6.214	110.27
FTP Download (Apply ECC)	0.0721000	0.1030220	6.233	108.15

표 8. 100대의 모바일 기기의 HANDOVER

HANDOVER	Delay(sec) (100 Devices)		Traffic Received (bits/sec) (100 Devices)	
FTP Download (None ECC)	0.0460020	0.0801000	6.214	110.27
FTP Download (Apply ECC)	0.0721000	0.1030220	6.233	108.15

성능을 분석을 위해 Ranging 시도 횟수와 모바일 기기를 추가하여 성능을 분석한 결과이다.

4세대 WIMAX 시스템에서 사용자에게 제공 할 서비스 품질의 요구사항 중 하나는 고속 이동 중에도 빠른 전송 속도를 제공하는 것이다. 802.16m 표준에서 제안하는 현재 핸드오버관련 요구사항의 기준으로는 핸드오버 시 150msec 이내의 접속 단절, IP 망에서의 고속 핸드오버를 1초 이내로 제한한다.

ECC를 적용한 초기진입구간은 모바일 기기 100대 기준으로 약 26msec로 수천대 이상의 모바일 기기가 한 기지국 망에 몰렸을 경우 WIMAX 시스템에 적지 않은 영향을 끼칠 것으로 예상된다.

단일 모바일 기기의 경우 시스템에 영향을 끼치지 않는 것으로 분석되지만 다중 핸드오버에 의한 Ranging의 오버헤드는 증가할 것으로 분석된다. 기존 관련연구의 RSA기반 Ranging 기법은 지연속도가 약 25msec 발생하였다. 이것은 단일 모바일 기기 대상으로 다중 사용자 환경에서는 적합하지 않

은 것으로 분석된다.

결론적으로 WIMAX 시스템에 성능에 영향을 주는 Ranging 구간의 암호화는 본 논문에서 제안한 ECC기반 같은 무선망에 효율적인 암호화가 적용되어야 하며 ECC는 지연속도 평균 1msec 차이로 RSA기반의 초기진입 구간보다 효율성이 높은 것으로 나타났다.

V. 결 론

다중 사용자 환경에서 WIMAX 시스템의 초기 진입 구간의 파라미터 노출은 최근 DOS 공격에 대한 위험에 노출될 수 있는 위험을 가지고 있다. 따라서 본 논문은 파라미터 노출을 방지하기 위해 Ranging 구간에 ECC를 적용하여 보안성을 증가 시키고, 적용된 ECC가 기존의 WIMAX 시스템에 큰 영향을 끼치지 않는 것을 시뮬레이션을 통해 확인하였다.

향후 4세대 네트워크 기술의 보안적인 기능을 적용하기 위해서는 트래픽 분산 제어, 기지국 위치 최적화, 프로세스 최적화 등 서비스 품질을 보장하기 위한 다양한 연구가 선행되어야 한다.

참 고 문 헌

[1] ITU, "Mobile telephony", (http://www-.itu.int/ITU-D/ict/statistics/), 2010.

[2] Perumalraja Rengaraju, Chung-Horng Lung, "Analysis on Mobile WIMAX Security", IEEE TIC-STH 2009, pp. 27-29, Sep., 2009.

[3] Taeshik Shon, Bonhyun Koo, Jong Hyuk Park, and Hangbae Chang, "Novel Approaches to Enhance Mobile WIMAX Security", EURASIP Journal onWireless Communications and Networking, 11pages, 2010.

[4] Masood Habib, Tahir Mehmood, Fasee Ullah, Muhammad Ibrahim, "Performance of WiMAX Security Algorithm", International Conference on Computer Technology and Development, 2009.

[5] IEEE 802.16 Task Group m (TGm), "IEEE 802.16m System Description Document (SDD)", (http://www.ieee802-.org/16/tgm/index.html), IEEE 802.16m-09/0034r4, 2010.

[6] IEEE 802.16 Task Group m (TGm), "IEEE 802.16m Work Plan", (http://www.ieee802.org/16/tgm/)

[7] J. Bellardo and S. Savage, "802.11 denial-of-service attacks: real vulnerabilities and practical solutions," in Proceedings of the 12th USENIX Security Symposium, Vol.12, Washington, DC, USA, Aug., 2003.

[8] C. Wullems, K. Tham, J. Smith, and M. Looi, "A trivial denial of service attack on IEEE 802.11 direct sequence spread spectrum wireless LANs," in Proceedings of the Wireless Telecommunications Symposium (WTS '04), pp.129-136, 2004.

[9] Prof. Dr. Ing. Evren Eren, Prof. Dr. Ing. Kai-Oliver Detken "WiMax-Security- Assessment of the Security Mechanisms in IEEE 802.16d/e".

[10] Mahmoud Nasreldin, Heba Aslan, Magdy El-Hennawy, Adel El-Hennawy, "WiMax Security" International Conference on Advanced Information Networking and Applications 2008, IEEE.

최 도 현 (Do-hyun Choi) 정회원

2008년 3월 동서울대학 소프트웨어공학과

2010년 6월 숭실대학교 컴퓨터학과 석사

2010년 6월~현재 숭실대학교 컴퓨터학과 박사과정

<관심분야> WIMAX, LTE, 암호 알고리즘, 웹 어플리케이션 보안, 서버 보안

박 중 오 (Jung-Oh Park) 정회원

2000년 7월 성결대학교 컴퓨터공학과
2003년 2월 명지대학교 전자계산교육 석사
2011년 8월 숭실대학교 컴퓨터학과 박사
2004년 3월 성결대학교 객원교수
2006년 3월~현재 성결대학교 정보산업기술연구소 전임연구원
<관심분야> 인터넷보안, RFID, 네트워크 보안, PKI, 암호알고리즘

전 문 석 (Moon-Seog Jun) 정회원

1981년 2월 숭실대학교 전자계산학과
1986년 2월 University of Maryland Computer Science 석사
1989년 2월 University of Maryland Computer Science 박사
1989년 3월~7월 Morgan State University 조교수
1989년 9월~1991년 2월 New Mexico State University Physical Science Lab. 책임연구원
1991년 3월~현재 숭실대학교 컴퓨터학과 정교수
<관심분야> 정보보호, 전자여권, 전자상거래