유무선 통합망에서 핸드오버시 끊김없는 서비스 제공을 위한 제어 플랫폼

정회원 맹 두 열*, 박 종 계**, 김 성 조***

A Control Platform Scheme for Seamless Service Provisioning During Handover on FMC Networks

Doo-lyel Maeng*, Jong-kae Park**, Sung-joo Kim*** *Regular Members*

요 약

최근의 네트워크 진화 방향은 All-IP 기반의 유무선 통합을 실현하기 위하여 인프라의 공통요소인 IP 기반의 이동성에 대한 연구가 진행되고 있다. 기존의 진행되어진 대표적인 IP 기반의 이동성 기술은 IETF(Internet Engineering Task Force)의 Mobile IP(Mobile Internet Protocol)이다. 하지만 Mobile IP를 제공하기 위하여 기존의 네트워크 인프라 즉, 라우터들(FA:Foreign Agent)에게 기능을 추가/변경하여야 하는 문제와 MN(Mobile Node)이 이동할 경우 패킷 손실 문제, 지연 시간 발생 부분을 해결하기에는 한계가 발생하였다. 본 논문에서는 기존의 IP 기반의 이동성 방식이 가지고 있던 문제점들을 개선하여 IP 기반의 이동성, 품질, 보안성을 제공하는 플랫폼 구조를 제시하였다. 기존 IP 기반의 이동성 방식과의 패킷 손실 및 지연 시간에 대한 시뮬레이션 분석을 통하여 성능이 개선되었음을 보여주고 있다.

Key Words : FMC Control Platform, Mobility, Security, QoS

ABSTRACT

Recently, IP mobility study of infra's common elements is undergoing processes to achieve FMC based on All-IP. Existing typical mobility technology based on IP is IETF's Mobile IP. However, it faced to limitations due to packet loss, delays when MN is moving on Mobile IP, also existing network infra - routers (FA) - needed to add/change the functions to support Mobile IP. In this paper, existing mobility problems based on IP and the suggested improvements for platforms which support mobility, quality, security are proposed. It discusses the performance on the current existing IP infrastructure derived from simulation analysis on mobility packet loss and delay. From the resulting data, improvements will also be outlined for optimal performance.

Ⅰ. 서 론

유비쿼터스 환경 구축을 위한 FMC(Fixed Mobile Convergence) 망은 패킷 서비스 기반의 풍부한 컨텐츠와 새로운 서비스 확보를 위하여 All-IP망으로 진화하고 있으며, MN(Mobile Node)의 빠른 보급에 따라 현재 네트워크 망에서 끊김없는 이동성 제공을 위한 BBM(Break Before Make), 데이터의 보호를 위한 IPSec[3], Flow 기반 품질보장 기술[9]-[11],[18] 들이 표준화되고 있다. 그러나 이동성 지원을 위한

* 한국인터넷진흥원 정보보호본부 지식정보보안산업팀(dybob@kisa.or.kr)
** 씨에스티 사업개발본부 서비스 개발실(jkpark@cst.co.kr)
*** 중앙대학교 컴퓨터공학과 모바일 및 임베디드 컴퓨터 시스템 연구실(sjkim@cau.ac.kr)
논문번호 : KICS2009-05-198, 접수일자 : 2009년 5월 12일, 최종논문접수일자 : 2009년 9월 7일

BBM 방식은 핸드오버 과정에서 패킷 손실이 발생하였고, IPSec과 품질보장 방법은 IP주소를 기반으로 협약을 진행하였기 때문에 IP주소 변경에 따른 재협약이 요구되어 추가적인 손실이 발생한다.

본 논문에서는 이러한 통합 서비스 환경에서 MN의 이동에 따라 발생하는 서비스 지연 최소화를 위하여 핸드오버 과정에서 MBB(Make Before Break)[16], 보안협약 유지를 위한 고정식별자 생성, 품질보장을 위한 QoS Profiler 기반의 flow 관리 기술을 제시하였다. MBB는 MN의 이동에 따라 새로운 신호를 감지할 경우 핸드오버 절차가 수행되며, 기존 CoA (Care of Address)와 신규 CoA를 동시에 유지하여 끊김없는 통신을 보장한다. 고정 식별자는 IP와 TCP 계층 사이에 IPv6 기반의 HoA(Home of Address)를 생성하여 보안협약을 유지하기 때문에 CoA 변경에도 보안협약은 유지된다. QoS Profiler 기반의 Flow 관리는 FMC 제어 플랫폼 서버에서 MN의 CoA를 관리하기 때문에 MN의 이동에 따라 변경된 CoA 갱신을 위하여 서버에 접속하고, 서버는 QoS Profiler에 MN의 정보를 전달하여 신규 CoA 기반의 Profile을 생성하여 Flow 정보를 유지한다. 이러한 FMC 제어 플랫폼은 고정 식별자 기반의 IPv6 over Tunnel 기법[8]으로 통신 서비스를 제공하기 때문에 모든 네트워크 환경에 적용이 가능하고, 서버 기반으로 주소를 관리하기 때문에 NAT 환경에서도 끊김없는 서비스를 제공한다.

본 논문은 NS-2 시뮬레이터를 기반으로 이동성, 보안성, 품질보장 통합 서비스 환경에서 핸드오버 및 재협약 과정에서 발생하는 패킷 손실 및 지연시간을 측정하고, 이동성에 대한 표준으로 제정된 MIPv6와 FMIPv6과 성능을 비교 분석한다.

본 논문의 구성은 다음과 같다. 2장은 이동성, 보안성, 품질보장 서비스에 대한 관련 기술을 소개하고, 3장은 FMC 제어 플랫폼 구조 및 동작 방법에 대하여 설명한다. 4장에서는 제안 시스템에 대한 성능시험 시나리오 및 결과를 비교·분석하고, 마지막으로 5장에서 결론을 맺는다.

Ⅱ. 관련 연구

유무선통합망에서 TPS/QPS를 사용하는 고객들의 품질만족을 위해서는 L2, L3 핸드오버가 빠르게 지원되는 Seamless Mobility가 이루어져야한다. 이번 장에서는 이동성 관리 기술인 MIPv4, MIPv6, PMIPv4 그리고 FMIPv6에 대해 살펴보고 본 논문에서 제시하는 모델과의 비교 대상을 정한다. 또한 보안성을 제공하기 위한 기술인 IPSec과 품질보장을 위한 IntServ 및 DiffServ에 대해서도 간략히 살펴본다.

2.1 MIPv4 (Mobile IPv4)

MIPv4는 IP 서브넷 사이의 호스트 이동 문제를 처리하기 위해 IETF에서 제안된 기술로 호스트가 IP 네트워크에서 AP(Access Point)를 변경할 수 있도록 고안되었다. MN이 방문 네트워크로 이동하였을 경우 먼저 FA(Foreign Agent)는 Agent Advertisement를 통해 이동노드의 등록을 유도한다. CN(Correspondent Node)은 MN의 영구주소(Permanent Address)로 Datagram을 전달하고 해당 Datagram은 Home Network로 전달된다. HA(Home Agent)는 해당 Datagram의 목적지 주소가 Home Network에 포함되어 있는지를 확인한 후 해당 Datagram을 MN의 CoA를 이용하여 FA에 전달한다. 이 때 해당 Datagram을 새로운 목적지 주소와 근원지 주소를 이용, Encapsulation하여 터널링한다. FA는 해당 Datagram을 MN으로 전달하고 MN은 CN을 목적지 주소로 해서 직접 Datagram을 보낸다.

이러한 간접 라우팅 방식에서는 CN에서 MN으로 전송되는 Datagram이 언제나 HA를 경유하여야 하는 Triangle Routing 문제가 발생하게 된다.

2.2 MIPv6 (Mobile IPv6)

MIPv4에서의 Triangle Routing 문제점을 해결하기 위해 MIPv6[1],[19]에서는 라우팅 최적화 기능이 포함된다. 또한 IPSec이 기본적으로 적용됨으로써 보안성이 뛰어나다고 할 수 있다.

라우팅 최적화 방식은 다음과 같다.

1) MN이 방문 네트워크로 이동.
2) MN은 BU(Binding Update)를 CN 및 HA에게 요청하고 BA(Binding Acknowledgement)를 수신.

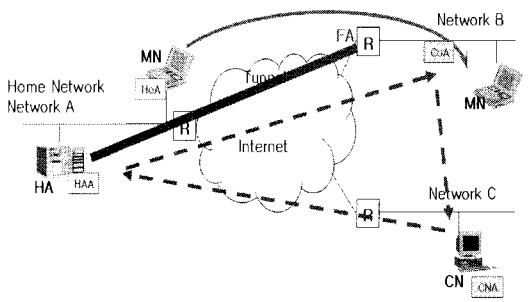


그림 1. Mobile IPv4 구조

3) MN은 HA 대신 CoA를 근원지 주소로 하여 CN을 향한 트래픽을 발생.(패킷은 HoA 목적지 옵션을 포함)
4) CN은 근원지 주소를 HoA로 교체하여 상위 계층으로 전달.
5) CN은 CoA를 목적지 주소로 하여 MN을 향한 트래픽 발생. 패킷은 두 번째 홉으로 HoA를 갖는 특별한 라우팅 헤더를 포함.
6) FA는 라우팅 헤더를 제거하고 두 번째 홉에 담긴 주소(HoA)로 패킷을 포워딩.

2.3 PMIPv6

PMIPv6는 MN의 부담을 경감하고 로컬 이동성을 제공하기 위해서 IETF NETLMM (Network-based Localized Mobility Management) 워킹그룹에서 네트워크 기반으로 이동성을 제공하기 위한 기술이다. PMIPv6 도메인 내 이동성을 위해서 설계되었고, MAG(Mobile Access Gateway)들에 의해서 제어된다. MN 대신 MAG가 LMA(Local Mobility Anchor)로의 바인딩 갱신 등의 이동성 기능을 수행하는 MN이 같은 PMIPv6 도메인 내 MAG들 간을 이동한다면 MN은 하나의 홈 주소만 가지고 마치 자신이 홈 링크에 있는 것처럼 네트워크에 접속한다. 그림 2와 같이 MN이 핸드오버하면 망쪽에서 알아서 LMA-MAG 간 터널을 변경한다.

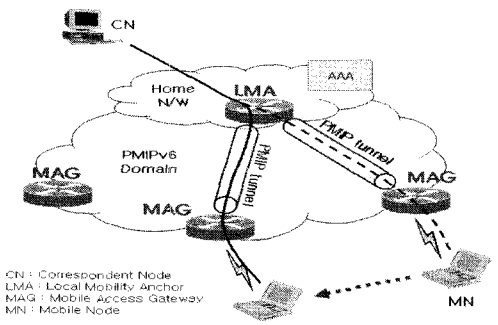


그림 2. PMIPv6 구조

2.4 FMIPv6 (Fast Mobile IPv6)

Fast Mobile IPv6[15]는 Mobile IPv6 핸드오버 시의 지연을 최소화하기 위하여 2계층에서의 핸드오버 예상 정보를 바탕으로 2계층 핸드오버가 완료되기 전에 3계층 핸드오버의 일부를 수행하거나 또는 양방향 터널을 이용하여 3계층 등록을 미룸으로써 실시간 서비스를 지원하는 기술이다.

Mobile IPv6는 MN의 Movement detection, IP Address Configuration, Location Update 등에 따른 지연요소들이 존재하므로 실시간 응용서비스를 제공하기에 문제점이 존재하였다. FMIPv6는 이러한 지연을 줄이기 위한 기술로서 새로운 링크 검출 시 즉각적인 데이터 송신을 가능토록 하여 새로운 링크에 부착되는 즉시 MN으로 패킷이 전달될 수 있도록 하는 것을 목표로 하고 있다.

FMIPv6의 기본 구조는 다음 그림 3과 같고 구체적인 동작과정을 살펴보면, FMIPv6에서 이동단말이 PAR에서 NAR로 이동하는 경우 이동단말 또는 PAR은 2계층 핸드오버가 완료되기 이전에 NAR의 2계층 정보를 미리 얻을 수 있다고 가정된다. 이동단말이 NAR의 2계층 정보를 미리 얻으면 NAR에 대한 IP 계층 정보를 PAR에 요청하며 PAR은 미리 가지고 있는 NAR 정보를 이용하여 NAR에 사용될 새로운 CoA를 미리 구성하여 이동단말에 알려주어 이동단말이 새로운 링크에 부착되는 즉시 바인딩 갱신을 수행할 수 있도록 해준다. 또한 새로운 CoA에 대한 바인딩 갱신이 이루어지기 전까지의 패킷 손실을 막기 위하여 NAR과의 사이에 양방향 터널을 설정한다.

하지만, FMIPv6는 PAR에서 NAR로 포워딩되는 동안 Triangle routing 현상이 발생한다. Triangle routing은 네트워크 리소스 낭비를 발생시킨다. 포워딩 패킷은 CN가 MN의 이동 사실을 인식하지 못한 채 PAR에게 패킷을 전송하기 때문에 발생한다. 게다가 동일한 데이터 패킷을 처리하기 위해 NAR과 PAR가 동시에 각각의 리소스를 이용하여야 하기 때문에 라우터의 자원 낭비도 발생 하게 된다.

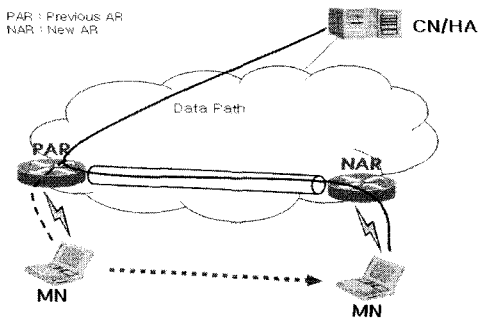


그림 3. FMIPv6 구조

2.5 IPSec

IP 패킷에 대해 기밀성, 무결성, 인증과 같은 보안성을 제공하는 국제표준 프로토콜인 IPSec은 IP 계층의 구조적 결함을 극복하고, IP 수준에서 제공

되는 보안 서비스 표준을 목적으로 개발되었으며, 하나의 프로토콜이 아니라 IP 네트워크를 위한 완전한 보안 솔루션을 제공하는 서비스와 프로토콜 모음이라고 할 수 있다. 여러 기술 중 인증 서비스 제공을 위한 AH(Authentication Header)와 Privacy를 보장하기 위한 ESP(Encapsulating Security Payload)가 대표적인 두 가지 기술이라고 할 수 있다.

IPSec은 TCP/IP 프로토콜과 애플리케이션이 사용할 수 있도록 IP 계층에서 보안 서비스를 제공한다. IPSec에는 Transport Mode와 Tunnel Mode 두 가지가 정의되어 있다. Transport Mode에서 IPSec 프로토콜은 전송 계층에서 IP로 내려온 메시지를 보호한다. 이 메시지는 AH, 혹은 AH와 ESP의 조합에 의해 처리되며 적절한 헤더가 전송 헤더 앞에 붙고 그 앞에 IP헤더가 붙는다. Tunnel Mode에서 IPSec은 IP 헤더가 이미 추가된 완전히 캡슐화된 IP Datagram을 보호하는데 쓰인다. IPSec 헤더는 원본 IP 헤더의 앞에 붙으며 새로운 IP 헤더가 다시 이 IPSec 헤더 앞에 붙는다. 즉 다음 그림 4와 같이 전체 원본 IP Datagram이 또 다른 IP Datagram 안으로 캡슐화된다.

IPSec 보안 통신은 "IP 주소, 보안 파라미터 식별자, 보안 알고리즘"으로 노드를 식별하기 때문에 노드의 이동에 따라 IP 주소가 변경될 경우 기존 보안협약을 유지할 수 없는 단점이 있다[3]-[5].

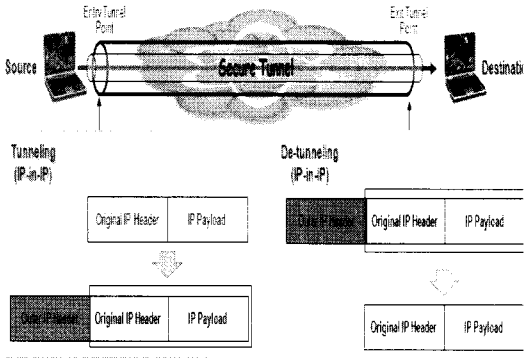


그림 4. IPSec Model (Tunnel Mode)

2.6 IntServ, DiffServ

실시간 멀티미디어 서비스의 품질을 만족시키기 위하여 플로우 기반의 품질 보장 방법인 IntServ[9]와 DiffServ[10] 모델이 제안되었다. IntServ는 사전에 자원을 예약하는 방식에 의하여 QoS를 제공하는 모델로서, RSVP(Resource Reservation Protocol)와 같은 자원예약 프로토콜에 의해 요구되는 자원을 사전에 예약하도록 하여 망으로 유입되는 트래픽에 대하여 수락제어를 하여 QoS를 제공하는 형태이다. 다음 그림 5는 IntServ Reference 모델로서 Control Plane과 Data Plane으로 구분하여 Control Plane이 Traffic flow들을 특성화하고 QoS 요구조건을 명시하여 미리 Reservation을 하고, Data plane은 Reservation되어 있는 경로로 데이터 패킷을 전달하는 것으로서, Control plane에서 적용되는 프로토콜이 RSVP이다. 하지만, IntServ 모델은 모든 플로우에 대한 정보를 유지·관리하기 때문에 광대역 망에 적용하기 어려운 문제점(Scalability Problem)이 존재한다.

DiffServ는 PHB(Per Hop Behavior)에 의한 Class별로 Resource를 Allocation하는 QoS 제공 모델로서, 플로우의 서비스 등급에 맞게 통합하여 품질을 제공하는 기술로 널리 활용되고 있다. 하지만, 여러 종류의 플로우를 집합 단위(Class of Service)로 QoS를 제공함으로써 사용자가 요구하는 응용별 품질보장을 제공할 수 없다. 다음 그림 6은 TC(Traffic Conditioning) 구조로서 Classifier, Meter, Marker, Shaper/Policer 등으로 구성되어 있다. Classifier는 입력 패킷들을 BA(Behavior Aggregate)로 구분해 주며, Marker는 결정된 PHB에 따라 패킷에 DSCP (DiffServ Code Point)값을 마킹한다. Meter는 패킷이 미리 정해진 트래픽 Profile을 준수하는지 여부를 결정하고, 위배된 패킷에 대해서는 Shaper/Policer에서 조정 또는 폐기시키게 된다.

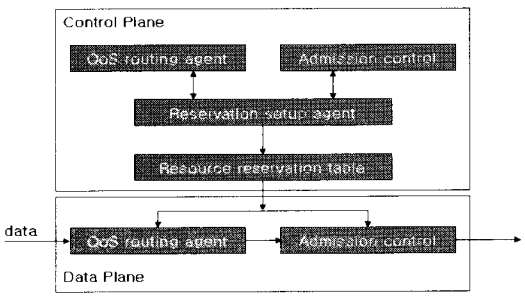


그림 5. IntServ Reference Model

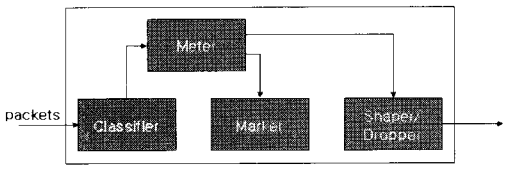


그림 6. DiffServ Traffic Conditioning 구조

따라서 유무선 통합 환경에서 서비스는 개별 사용자의 서비스 단위인 플로우별로 대역폭을 할당하여 사용자 서비스의 품질을 정확하게 보장하면서 효율성을 달성할 수 있어야한다. Congestion 발생시에도 개별 플로우의 특성에 따라 직접적으로 제어하여 기존에 수용된 프리미엄 서비스의 품질을 보장하면서 중요성이 떨어지는 플로우만을 별도로 제어하여 효과적으로 품질제어를 제공할 수 있다.

Ⅲ. FMC 제어 플랫폼 시스템 구조

이번 장에서는 FMC 망에서 MN의 이동성, 보안성, 품질보장 서비스 제공을 위한 시스템 구조와 사용자 및 서비스 인증을 위한 인증 절차와 서비스 지원방안 등 제어 플랫폼 시스템 구조를 설명한다.

3.1 시스템 구조

MN의 이동에 따라 발생하는 핸드오버와 재협상 문제 해결을 위하여 본 논문에서는 FMC 제어 플랫폼 시스템 구조를 그림 7과 같이 FMC 제어 플랫폼, QoS Profiler, MN, CN(Correspondent Node), AR(Access Router), ACR(Access Control Router)로 구성하였다.

FMC 제어 플랫폼은 사용자와 서비스 인증을 수행하고, PKI, QoS Profiler 등 타 서버들과 연동하여 정보를 공유하기 때문에 NAT(Network Address Translator)와 같은 장비[13]가 설치된 환경에도 통신 서비스 제공이 가능하다. 사용자 인증은 초기 ID와 PWD(Password) 기반으로 MN의 HoA와 CoA 등록정보를 저장하고, SLA(Service Level Agreement) 등급을 "일반, 보안, 품질, 보안과 품질"로 구분하여 서비스를 제공한다. 일반 등급은 끊김없는 이동성 지원을 위하여 핸드오버시에 MBB를 지원하고, 보안 등급은 PKI 서버와 연동하여 공개키를 저장 및 분산한다[12]. 품질 등급은 QoS Profiler 서버와 연동하여 MN가 이동시 무선 자원이 변경될 지라도 MN의 HoA와 CoA를 전달받아 사용자에 따라 Profile을 구분하여 AR(또는 ACR)에 전송한다. 따라서 보안 및 품질 등급은 PKI와 QoS Profiler 서버 연동에 따라 단말들의 공개키 분배 및 Profile을 생성하여 전송한다. SLA 등급에 따라 MN과 CN은 각각 클라이언트 모듈 설치에 따라 핸드오버시에 MBB를 제공하고, IPv6 기반의 고정식별자 생성에 따라 보안과 품질 등급 서비스를 제공한다. 본 논문에서는 FMC 제어 플랫폼의 역할을 포함한 시스템을 FMC 제어 플랫폼 서버로 명명하여 사용한다.

3.2 인증 구조

MN의 사용자 및 서비스 인증에 따라 FMC 제어 플랫폼에 HoA, CoA가 등록되고, 서비스 등급에 따라 협약을 맺은 후 통신 서비스를 제공한다.

그림 8과 같이 DHCP에 접속하여 통신을 위한 IP 주소를 생성(1,2)한 MN은 FMC 제어 플랫폼 서버에 ID/PWD를 전송하여 사용자 인증을 요청(3)한다. 사용자 등록이 되어있지 않을 경우 서버는 사용자 등록을 위하여 Service Portal에 전달(4)한다. MN은 Service Portal에 접속하여 MN 서비스 등록과 클라이언트 모듈을 제공(6)받아 설치(7)하고, FMC 제어 플랫폼 서버에 접속하여 MN 사용자 인증을 요청(8)한다. FMC 제어 플랫폼 서버는 초기 인증 과정에서 HoA와 CoA를 테이블에 저장(8,9)하고, MN 이동에 따라 변경되는 CoA를 갱신(10)한다. 만약 보안성과 품질보장 서비스 제공을 원할 경우 CN의 HoA, CoA, 공개키를 MN에 전송하여 PKI

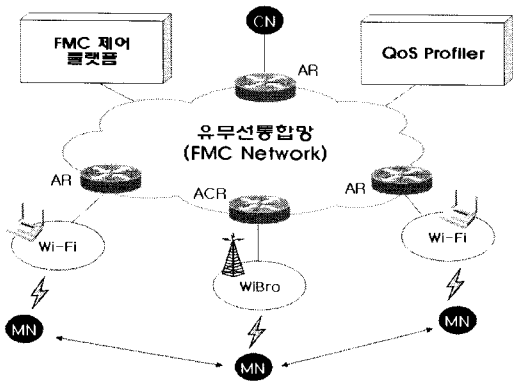


그림 7. FMC 제어 플랫폼 시스템 구조

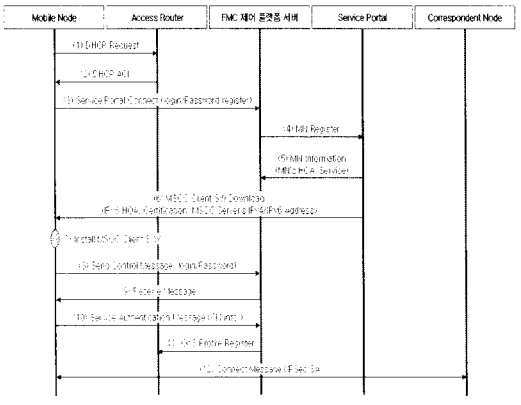


그림 8. FMC 제어 플랫폼 인증 절차

기반의 IPSec 보안협약을 지원(11)하고, QoS Profiler에 MN과 CN의 CoA를 기반으로 Profile을 생성하여 Profile 기반의 Flow 상태 정보를 생성(11)한다. MN과 CN은 HoA를 기반으로 IPSec 보안협약을 수행하고, AR은 Flow 상태정보를 기반으로 라우팅 테이블에 등록·분산하여 보안 및 품질보장 서비스를 제공(12)한다[7].

3.3 동작 절차

MN과 CN에는 클라이언트 모듈이 설치되고, MN은 데이터 보안과 품질보장 서비스를 신청하였다고 가정했을 때, MN과 CN의 통신을 위한 FMC 제어 플랫폼 동작 절차는 그림 9와 같다.

MN은 CN과 통신하기 위하여 FMC 제어 플랫폼 서버에 접속하여 CN의 정보를 요청(1)한다. FMC 제어 플랫폼 서버는 MN의 서비스 등급을 조사하고, 데이터 보호 서비스 제공을 위하여 PKI 서버에 연동하여 CN의 공개키와 HoA, CoA를 MN에게 전달(1)한다. 그 다음 CN에게 MN의 정보를 전달(2)하고, 품질보장 서비스를 위하여 QoS Profiler로 MN과 CN의 HoA와 CoA를 전달하여 Profile 기반의 Flow를 생성함으로써 품질보장 서비스를 제공(3)한다. MN은 CN의 공개키를 활용하여 HoA 기반의 보안협약을 수행하고, 안전한 통신 서비스를 제공(4)한다.

MN가 이동함에 따라 CoA가 변경된다 할지라도, 보안협약의 식별자인 HoA는 변경되지 않았기 때문에 기존 협약은 그대로 유지된다. 품질보장은 CoA가 변경되었기 때문에 FMC 제어 플랫폼 서버에 접속하여 CoA 갱신을 요청한다. FMC 제어 플랫폼 서버는 HoA를 키 값으로 CoA를 갱신하고, QoS Profiler에 HoA와 CoA를 전달하여 MN의 Profile 정보를 갱신하기 때문에 지연 시간이 발생하지 않는다.

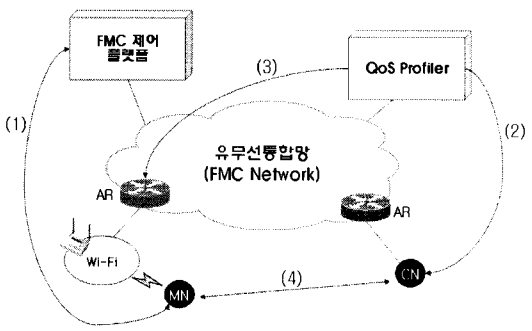


그림 9. FMC 제어 플랫폼 동작 절차

3.4 이동성 지원 방안

본 논문에서 제안한 이동성 구조는 끊김없는 통신이 가능하도록 클라이언트/서버 기반의 MBB를 이용한다. FMC 제어 플랫폼 서버는 MN의 HoA와 CoA 테이블을 저장하고 있으며, MN의 이동에 따라 신규 CoA를 생성하고 갱신된 CoA를 CN에 전달한다. 끊김없는 이동성 지원을 위해 클라이언트 모듈은 MN에 설치된다. 클라이언트 모듈을 설치한 MN은 WiBro[20] 신호를 수신하기 위한 가상의 네트워크 연결 프로토콜을 설치하고, WiFi와 WiBro 신호를 동시에 수신한다. MN은 이기종망에서 WiFi와 WiBro의 주소를 동시에 유지하였고, 초기 CoA가 생성된 상태에서 타망으로 MN이 이동에 따라 신규 신호가 탐지되어 L2 Trigger가 발생됨에 따라 MBB가 실행된다.

그림 10과 같은 절차에 따라 MBB가 실행되면 수신되는 신호의 감도가 가장 강한 WiFi와 WiBro 신호를 선택(1)하고, 활성모드(Active Mode)인 WiFi와 대기모드(Standby Mode)인 WiBro를 생성(2)한다. 현재 통신 중인 WiFi 인터페이스를 사용하는 CoA가 특정 기준치 이하로 신호세기가 떨어질 경우, 대기모드의 WiBro CoA는 활성모드로 변경되고, 신규 신호를 탐색하여 WiFi CoA를 갱신한다. 갱신된 WiFi CoA는 신규 활성모드로써 FMC 제어 플랫폼 서버에 터널 생성을 요청(3,4)하고, 생성된 터널을 통해 BU 메시지와 CN의 주소를 전송(5,6)한다. FMC 제어 플랫폼 서버는 BU 메시지에 등록된 신규 CoA를 갱신(7,8)하고, CN에 BU 메시지를 전달(9)함으로써 핸드오버 과정을 종료한다.

3.5 보안 협약

본 논문은 클라이언트 모듈이 설치된 단말(MN, CN)들에 대해 안전한 통신을 제공하기 위하여 고정

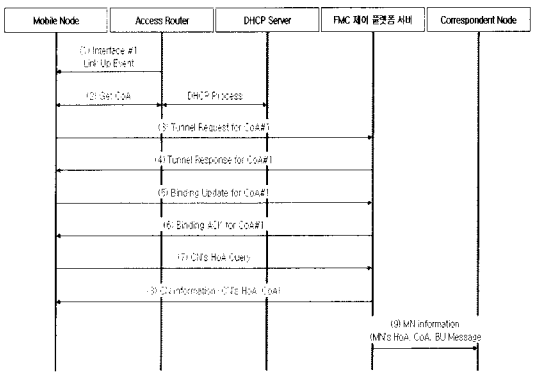


그림 10. MBB 동작 절차

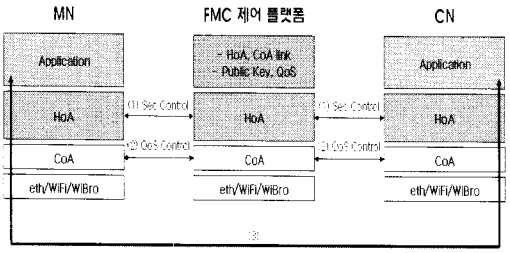


그림 11. 고정 식별자 생성

식별자 기반의 IPSec 보안협약을 제안한다. 클라이언트 모듈이 설치된 단말(MN, CN)은 IPv6 기반의 고정식별자를 생성하고, 등록된 서비스가 보안성 제공 등급일 경우 고정식별자를 기반으로 IPSec 보안협약을 맺기 때문에 CoA가 변경되어도 기존 보안협약은 그대로 유지된다.

그림 11과 같이 MN에 클라이언트 모듈이 설치될 경우 HoA 계층이 생성되고, 사용자 및 서비스 인증을 위하여 FMC 제어 플랫폼 서버에 접속을 요청한다. MN은 사용자 인증절차에 의해 HoA와 CoA를 등록하고, 서비스 등급에 따라 보안 및 품질보장 서비스를 지원한다. 만약 MN과 CN이 보안 서비스를 요청할 경우, MN은 FMC 제어 플랫폼 서버에 접속하여 CN의 공개키, CoA, HoA에 대한 정보를 요청하고, 전송받은 정보에 따라 HoA(1)를 기반으로 IPSec 보안협약을 맺는다. 따라서 MN의 이동에 따라 CoA가 변경되어도 보안 협약을 맺은 HoA가 유지되기 때문에 MN 이동에 따른 보안 재협상 지연 문제를 해결하였다.

품질보장 서비스는 CoA(2)를 기반으로 협약을 진행하기 때문에 MN의 이동에 따라 주소가 변경된다. 이에 대한 동작 절차는 3.6절에서 다룬다.

3.6 QoS Profiler 기반의 Flow 관리

본 논문은 FMC 제어 플랫폼에서 MN과 CN의 품질 보장 지원을 위하여 QoS Profiler 기반의 Flow 관리 방법을 제안한다. MN의 이동에 따라 변경되는 CoA 주소를 기반으로 AR에서 Flow 정보를 생성하기 때문에 클라이언트 기반의 품질보장 서비스는 MN 재인증에 따른 지연이 발생한다. 따라서 FMC 제어 플랫폼이 QoS Profiler로 MN의 갱신된 주소 정보를 전달함으로써 재인증 과정에 따른 지연문제를 해결한다.

그림 12에서 보듯이 품질보장 서비스를 신청한 MN은 FMC 제어 플랫폼 서버에서 사용자 및 서비스 인증 절차를 수행(1)하고, 통신을 원하는 CN의

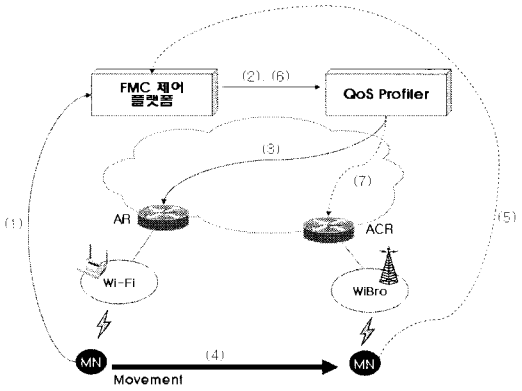


그림 12. QoS Profiler 기반 Flow 관리 구조

주소를 요청한다. FMC 제어 플랫폼 서버는 MN과 CN의 HoA와 CoA를 QoS Profiler에게 전달하여 서비스 등급에 대한 Profile을 구성(2)하고, AR에 Profile 초기 CoA와 신규 CoA를 전달(3)함으로써 초기 CoA 기반의 Flow 상태 정보를 생성한다. AR은 생성된 Flow 상태 정보와 CoA를 AR의 라우팅 테이블에 저장하고, 인근 라우터에 이들을 전달하여 라우터의 라우팅 테이블에 Flow 상태 정보를 기록한다. 라우팅 테이블에 Flow 정보가 등록되어 있을 경우, 라우터는 Flow 정보에 따라 서비스의 품질을 관리한다.

QoS Profiler 기반 Flow 관리 방법에서 MN의 이동에 따라 CoA가 변경(4)될 경우 FMC 제어 플랫폼 서버에서 CoA의 갱신을 위하여 BU 메시지를 전송(5)한다. 이처럼 MN의 정보를 QoS Profiler에 전달(6)하고 CoA 정보를 갱신하기 때문에 CoA 갱신 과정(7)에서 재인증 과정에 따른 지연문제를 해결하였다.

Ⅳ. 성능시험

4장에서는 FMC 제어 플랫폼의 성능 검증을 위하여 이동성, 보안성, 품질보장 서비스 통합 환경에서 성능검증을 위한 시나리오를 제시하고, 성능시험 결과를 분석한다.

4.1 시나리오

FMC 제어 플랫폼의 성능 시험을 위하여 Linux Kernel 2.4.18에 NS-2를 설치하고, FMC 제어 플랫폼 서버와 클라이언트 모듈을 구현하여 MN의 이동성, 보안성, 품질보장 서비스 통합 환경에서 서비스 지연을 측정하기 위한 시뮬레이션을 수행하였다.

FMC 제어 플랫폼 서버는 MN들의 CoA와 HoA를 데이터베이스 관리 모듈과 MN의 정보를 Service Portal이나 QoS Profiler에게 포워딩하는 모듈을 구현하여 핸드오버 과정에서 전송되는 BU 메시지의 CoA 정보 갱신 및 분배하는 역할을 수행한다. 클라이언트 모듈은 WiBro/WiFi 듀얼모드 네트워크 드라이브와 MBB 제공을 위한 알고리즘, 그리고, 보안 및 QoS 제공을 위한 HoA 계층 생성 모듈을 구현하였다.

성능시험을 위한 테스트베드는 그림 13과 같이 MC 제어 플랫폼 서버, AR, AP, MN 그리고 CN으로 구성된다. FMC 제어 플랫폼 서버에 MN과 CN의 HoA와 CoA를 사전에 저장하였고, MN의 이동에 따라 갱신된 CoA와 변경된 주소를 CN에게 전달한다. AR은 Flow 기반의 품질보장 서비스를 제공하고, AP는 802.11b 무선 신호를 지원한다. MN과 CN은 클라이언트 모듈을 기반으로 핸드오버 알고리즘인 MBB를 수행하고, 보안 협약 유지를 위하여 HoA 고정식별자를 생성하였다.

이러한 테스트베드 환경에서 성능시험을 위해 MN과 CN 사이에 IPSec 보안협약을 맺었고, 경유하는 라우터에 Flow 상태정보를 사전에 저장하였다. 그림 13에서 볼 수 있는 바와 같이 MN은 Net 1(Wi-Fi Network)에서 Net 2(WiBro Network)로 이동한 후 신규 신호를 탐지하였고, 핸드오버 알고리즘인 MBB를 동작시켜 패킷 손실과 지연 시간을 측정하였다. 또한 신규 CoA 생성에 따라 보안성과 품질보장 협약 정보가 변경되기 때문에 재협상에 따른 패킷 손실과 지연 시간을 측정하였다.

핸드오버와 재협상 과정이 네트워크 트래픽에 미치는 영향을 측정하기 위해서 본 실험에서는 msec 단위로 VoIP Traffic을 CN이 수신하는 UDP 트래픽을 측정하였다.

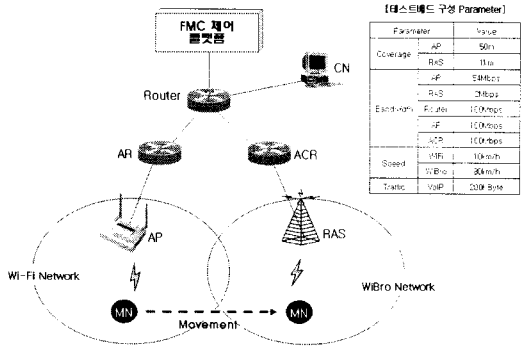


그림 13. 테스트베드 망 구조

4.2 시험 결과 및 분석

4.1절에서 설명한 것과 같이 성능시험을 위해 MN과 CN간은 보안성과 품질보장 협약을 맺고, CN은 MN에게 메시지를 1Kbyte 단위로 전송한다. 성능시험을 위한 시뮬레이션 환경에서 MN의 핸드오버와 재협상 과정에서 발생하는 패킷 손실과 지연 시간을 측정하였다. MN과 CN은 보안성 제공을 위한 IPSec과 품질보장을 위한 Profiler 협약을 맺은 상태에서 MN의 이동에 따라 동작하는 핸드오버 절차의 지연과 기존 보안 및 품질보장 협약 유지를 위한 재협약 절차에서 발생하는 패킷 손실을 측정하기 위하여 UDP 기반의 패킷을 전송하였고, CN이 응답하는 메시지의 순차 번호와 패킷 도착 시간을 이용하여 패킷 손실이 발생하는 구간을 측정하였다.

UDP의 경우, 그림 14와 같이 BBM 핸드오버 방식의 MIPv6와 FMIPv6[2]는 MN 이동에 따른 재협상 과정에서 MIPv6는 Sequence Number 80~121, FMIPv6는 80~108번째까지 패킷 손실이 발생하였다. 그러나 본 논문에서 제안한 FMC 제어 플랫폼은 MBB 핸드오버 사용과 고정 식별자 기반의 보안협약, QoS Profiler의 품질 서비스에 따른 통합 서비스 제공에서도 패킷 손실이 발생하지 않아, VoIP 서비스 지원을 위한 1% 미만의 PER 조건을 만족시켰다.

또한 MIPv6의 지연 시간은 그림 15와 같이 L2 기반 지연으로 홈 에이전트에 CoA를 등록하는 과정에서 722msec, HA와 터널링 협약 과정에서 1713msec 이 지연이 발생하였다. L3 기반 지연 시간으로 CN에 CoA를 등록함에 따라 136msec, 명확한 라우팅 경로 설정을 위하여 203msec, 보안 재협약을 위해 Phase 1에서 910msec, Phase 2에서 358msec, 그리고 마지막으로 품질 재협약을 위해 35msec의 지연

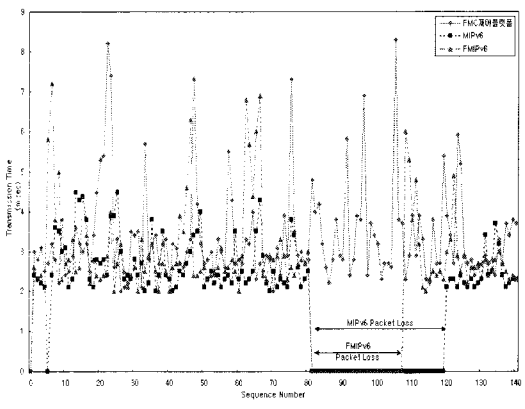


그림 14. UDP 핸드오버 패킷 손실 구간

표 1. Delay-time Parameter들의 정의

Delay-time Parameter	Definition
M_{crh}	CoA Registration Time(HA)
M_{tu}	Tunneling Association Time
M_{crc}	CoA Registration Time(CN)
M_{ro}	Routing Optimization Time
M_{L2}	L2 handover delay time
M_{L3}	L3 handover delay time
M_{fna}	Fast Neighbor advertisement time
M_{MBB}	MBB Operation Time
M_{phase1}	Security Re-association Time(1)
M_{phase2}	Security Re-association Time(2)
M_{SLA}	QoS Re-association Time
TDT	Total Delay Time

이 발생하였다. 따라서 MIPv6의 총 지연시간은 4077msec이다.

그림 15와 같이 FMIPv6의 지연 시간은 L2 기반 지연으로 L2 핸드오버를 위해 191msec, L3 기반 지연으로 Fback에서 637msec, 그리고 FNA(Fast Neighbor Advertisement) 요청을 위해 689msec의 지연이 발생하였다. 또한 보안 재협약을 위해 Phase 1에서 810msec, Phase 2에서 460msec, 그리고 품질 재협약을 위해 38msec의 지연이 발생하였다. 따라서 FMIPv6의 총 지연시간은 2825msec이다.

FMC 제어 플랫폼의 경우 그림 15와 같이 활성(Active) CoA를 기반으로 연결을 유지한 상태에서 대기모드의 CoA를 생성하기 때문에 핸드오버 지연 시간을 최소화하였고, 고정 식별자 기반으로 보안 협약 유지에 따라 CoA 변경에도 초기 협약 정보를 그대로 유지하였다. 또한 품질보장 협약 유지를 위하여 FMC 제어 플랫폼이 Profile을 관리하기 때문

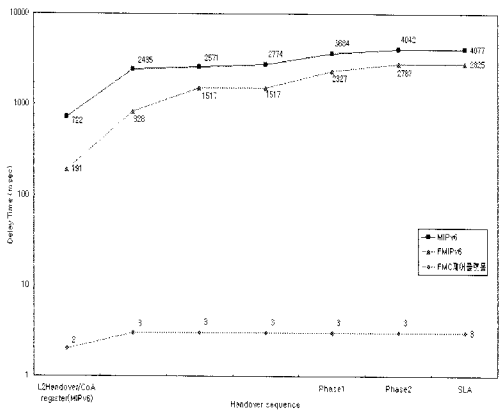


그림 15. MIPv6, FMIPv6, FMC제어플랫폼 지연시간 측정 결과

에 품질보장 재협상에 따른 MN의 지연시간이 발생하지 않았다. 따라서 제안된 방안은 FMC 환경에서 이동성, 보안성, 품질을 보장하면서도 음성서비스의 품질 기준인 10msec 이하의 지연이 발생하여 실시간 멀티미디어 데이터 전송에서도 끊김없는 서비스 제공이 가능함을 알 수 있다.

각 방식별(MIPv6, FMIPv6, FMC제어플랫폼) MN이 이동함에 따라 발생되는 총 지연 시간 계산식은 다음과 같다.

$$TDT_{mipv6} = M_{crh} + M_{tu} + M_{crc} + M_{ro} + M_{phase1} + M_{phase2} + M_{SLA} \quad \text{(수식 1)}$$

$$TDT_{fmipv6} = M_{L2} + M_{L3} + M_{fna} + M_{phase1} + M_{phase2} + M_{SLA} \quad \text{(수식 2)}$$

$$TDT_{fmc} = M_{L2} + M_{MBB} + M_{phase1} + M_{phase2} + M_{SLA} \quad \text{(수식 3)}$$

V. 결론 및 향후 연구

기존의 IP이동성 기술을 통하여 IP이동성을 제공하기 위해서는 인프라 즉, 라우터들에서 신규 기능(FA) 필요함에 따라 인프라의 기능 변경이 요구되었으나, 본 논문에서는 클라이언트-서버기반의 FMC 제어 플랫폼 도입을 통하여 IP 관리 및 이동성을 제공하므로 기존 인프라의 변경없이 적용 가능한 방안을 제시하였다.

또한, MN이 이기종망 이동시 MN의 핸드오버 과정에서 패킷 손실과 보안 문제, 서비스품질 재협상에 따른 지연 문제를 해결하기 위한 방안으로 FMC 제어 플랫폼을 제안하였다. FMC 제어 플랫폼은 동일망 또는 이기종망 환경에서 끊김없는 핸드오버 지원을 위하여 MBB 방식 기반으로 패킷 손실 및 지연 시간을 최소화하였다. MN의 주소 변경에도 IP와 TCP 계층에 IPv6 기반의 고정 식별자를 기반으로 IPSec 보안협약을 유지하여 모든 네트워크 환경에서도 적용이 가능하게 설계하였다. 또한, 실시간 멀티미디어의 품질을 보장하기 위하여 QoS Profiler 기반의 Flow 상태 정보 지원을 통해 MN이 이기종 망으로 이동상황에서도 품질보장 서비스의 재협약에 따른 지연 요소를 제거하였다.

FMC 제어 플랫폼 성능시험 결과 패킷 손실이 거의 없었고, 지연 시간이 10msec 이하로 실시간 VoIP 서비스 지원에 합당함을 알 수 있었다.

향후에는 MBB 동작 절차에서 활성모드와 대기모드 생성 및 갱신을 위한 최적의 알고리즘과 클라

이언트 모듈의 설치 없이 보안성을 유지하는 방안에 대한 연구가 필요하다.

참 고 문 헌

[1] D. Johnson, C. Perkins, J. Arkko, "Mobility Support in IPv6," RFC 3775, June 2004.

[2] R. Koodli, Ed., "Fast handovers for mobile IPv6," RFC 4068, Jul 2005.

[3] S. Kent, K. Seo, "Security Architecture for the Internet Protocol," RFC 4301, December 2005.

[4] C. Kaufman, "Internet Key Exchange(IKEv2) Protocol," RFC 4306, December 2005.

[5] J. Arkko, V. Devarapalli, F. Dupont, "Using IPSec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents," RFC 3776, June 2004.

[6] S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury and B. Patil, "Proxy Mobile IPv6," Internet Draft on IETF, May 2008.

[7] T. Kivinen, H. Tschofenig, "Design of the IKEv2 Mobility and Multihoming(MOBIKE) Protocol," RFC 4621, August 2006.

[8] B. Carpenter, C. Jung, "Transmission of IPv6 over IPv4 Domains without Explicit Tunnels," RFC 2529, March 1999

[9] R. Braden, D. Clark, S. Shenker, "Integrated Services in the Internet Architecture an Overview," RFC 1633, June 1994.

[10] T. Li, V. Rekhter, "A Provider Architecture for Differentiated Services and Traffic Engineering," RFC 2430, October 1998.

[11] S. Blaske, D. Black, M. Carlson, E. Davies, Z. Wang, and W. Weiss, "An Architecture for Differentiated Services," RFC 2475, December 1998.

[12] B. Korver, "The Internet IP Security PKI Profile of IKEv1/ISAKMP, IKEv2, and PKIX," RFC 4945, August 2007.

[13] K. Egevang, P. Francis, "The IP Network Address Translator," RFC 1631, May 1994.

[14] R. Jaksa, C. williams, B. Sarikaya, "Mobile IPv6 Make Before Break," Internet Draft, July 2007.

[15] L. Dimopoulou, G. Leoleis, I. S. Venieris, "Fast handover support in a WLAN environment: challenges and perspectives," IEEE Network, Vol.19, No. 3, pp. 15-20, 2005.

[16] Ramachandran, K. Rangarajan, S. Lin. J.C., "Make-Before-Break MAC Layer Handoff in 802.11 Wireless Networks," Communications, 2006. ICC '06. IEEE International Conference, June 2006.

[17] 홍성백, 이경호, 김남, "이종 무선망에서 L3 핸드오버 이동성 관리 성능 향상," *한국통신학회논문지*, June 2007.

[18] 씨에스티, "QSS 시스템 분석 시뮬레이터 개발 및 테스트베드 구축," *ETRI 연구보고서*, January 2008.

[19] 유명주, 이종민, 최성곤, "NGN에서의 이동성 관리 방안 성능 분석 및 비교," *한국콘텐츠학회논문지* '07 Vol. 7 No. 4, April 2007.

[20] TTA, "와이브로에서의 IPv6 기술," TTAS.KO-10.0210, December 2006.

맹 두 열 (Doo-lyel Maeng) 정회원

1988년 2월 중앙대학교 무역학과 졸업

2004년 8월 중앙대학교 컴퓨터소프트웨어학과 석사

2008년 8월 중앙대학교 컴퓨터공학과 박사과정

2009년 한국인터넷진흥원 선임연구원

<관심분야> 이동컴퓨팅, 바이오인식, 정보보호, 유무선통신

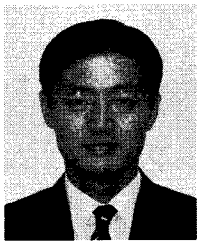
박 종 계 (Jong-kae Park) 정회원

2000년 8월 숭실대학교 컴퓨터공학과 졸업

2002년 8월 숭실대학교 컴퓨터공학과 석사

<관심분야> IPv6, QoS, Mobile IP, IMS

김 성 조 (Sung-joo Kim) 정회원



1975년 2월 서울대학교 응용수학과 졸업

1977년 2월 한국과학기술원 전산학과 석사

1987년 2월 Univ, of Texas at Austin 컴퓨터공학과 박사

<관심분야> 이동컴퓨팅, 임베디드 SW, Cyber Physical Systems