논문 13-38A-04-06

한국통신학회논문지 '13-04 Vol.38A No.04
http://dx.doi.org/10.7840/kics.2013.38A.4.337

F-PMIPv6 네트워크에서 지능적인 계층적 이동성 지원 기법

한 성 희◆, 정 종 필°

Intelligent Hierarchical Mobility Support Scheme in F-PMIPv6 Networks

Sunghee Han◆, Jongpil Jeong°

요 약

본 논문에서는 i-FP(intelligent Fast PMIPv6)로 명명한 새로운 이동성관리 네트워크 기법을 제안한다. i-FP는 지역 이동성관리 문제를 해결하기 위해 고안했다. 하나의 도메인 내에서 MN(Mobile Node)을 다른 네트워크로 이동이 가능하게 하기 위해 i-FP에서는 PMIPv6(Proxy Mobile IPv6)의 세가지 네트워크 엔티티인 LMA(Local Mobility Anchor), MAG(Mobile Access Gateway), MN의 개념을 확장하여 기능을 추가했다. 세가지 네트워크 엔티티로 i-FP에서는 MN의 핸드오버 지연 시간을 감소시키고 IP 헤더 스와핑 메카니즘을 사용하여 트래픽 오버헤드를 회피하여 네트워크 처리량을 증가 시킨다. i-FP의 성능을 평가하기 위해, 새롭게 제안하는 i-FP와 같은 로컬 이동성 관리 프로토콜인 HMIPv6(Hierarchical Mobile IPv6), PMIPv6까지 이상 총 세가지 기법으로 다양한 기준을 사용하여 네트워크 기법의 성능을 측정 / 평가하였다. 성능평가 결과를 종합해서 i-FP가 트래픽 오버헤드가 없어지고 다른 비교 기법 대비 평균 라우팅 홉수 10.2%, 트래픽 시그널링 비용 58.5%, 핸드오버 지연은 16.3% 감소의 성능향상이 일어남을 보여준다.

Key Words : Fast Handover, i-FP, HMIPv6, PMIPv6, FPMIPv6

ABSTRACT

In this paper, we propose a new mobility management scheme, called i-FP(intelligent Fast PMIPv6). Our proposed i-FP scheme is addressed for solving the existing local mobility management problems from legacy frameworks. To move MN(Mobile Node) to other networks in one domain, i-FP employs three network entities which are extended from PMIPv6(Proxy Mobile IPv6), LMA(Local Mobility Anchor), MAG(Mobile Access Gateway) and MN. In i-FP, the three network entities can reduce the handover delay time of MNs. Also, i-FP uses an IP header swapping mechanism to avoid the traffic overhead and improve the throughput of network. To evaluate the performance of i-FP, we analyze our i-FP, HMIPv6(Hierarchical Mobile IPv6) and PMIPv6 which are legacy protocols of local mobility management in terms of various parameters. Finally, our i-FP scheme shows good performance(reduction of routing hops 10.2%, signaling costs 58.5% and handover delay 16.3%) than other network schemes for the total cost.

◆ 주저자 : 성균관대학교 정보통신대학원 석사 과정, iwas1006@gmail.com, 준회원
° 교신저자 : 성균관대학교 정보통신공학부 교수, jpjeong@skku.edu, 정회원
논문번호 : KICS2012-12-570, 접수일자 : 2012년 12월 20일, 최종논문접수일자 : 2013년 3월 21일

Ⅰ. 서 론

최근 새로운 무선 네트워크의 수요 폭증과 그에 따른 새로운 기술의 발달로 다양한 계층적 이동성 프레임워크가 나타나고 있다. 무선 네트워크 프레임워크에서 사용자의 이동성은 크게 도메인 내부의 이동과 도메인 간의 이동 두 가지로 구분된다. 이 두 가지 이동성은 무선 네트워크의 이동성 프로토콜의 글로벌 이동성 프로토콜[11]과 로컬 이동성 프로토콜[8,9] 두 가지에 대응된다. 글로벌 이동성 프로토콜[3]은 하나의 도메인 영역을 벗어나는 넓은 지역에서 사용자의 이동에 따른 도달 가능성을 유지하고 로컬 이동성 프로토콜은 한 도메인 내부에서 제한된 영역의 핸드오버를 지원한다.

IPv6[1,2]를 지원하는 모바일 네트워크에 접속하여 서비스를 받고 있는 사용자가 한 네트워크에서 도메인이 다른 네트워크로 접속했을 때, 사용자가 새롭게 접속하는 네트워크에서는 처음 외부에서 접근한 네트워크를 관리하기 위해 트래픽을 도메인으로 재전송하여 관리하기 위한 글로벌 이동성 프로토콜을 사용한다. 그리고 글로벌 이동성 프로토콜에서 사용자 트래픽을 전달 받은 로컬 이동성 프로토콜은 도메인 내에서 트래픽을 전달하고 사용자에 의해 성공적으로 전송을 받았음을 보장하여 사용자에게 원활한 모바일 네트워크 서비스를 제공한다.

글로벌 이동성과 로컬 이동성의 지원으로 사용자는 유연하면서 높은 성능으로 이동성을 제공받아 통신을 즐길 수 있다. MIP(Mobile IP), HIP(Host Identity Protocol)[3], HMIPv6(Hierarchical Mobile IPv6)[4], F-PMIPv6(Fast Proxy Mobile IPv6)[5,23] 등과 같은 글로벌 이동성 프로토콜은 사용자의 이동성관리를 위한 지원을 하고 본 논문은 이러한 글로벌 이동성과 로컬 이동성에 대한 부분에 초점을 맞추고 있다. 기존의 PMIPv6(Proxy Mobile IPv6)[6]나 HMIPv6 프로토콜은 트래픽이 다른 곳으로 이동하기 위해서는 해당 네트워크의 최상위 게이트웨이까지 트래픽이 이동을 해서 네트워크내의 목적지 주소를 확인하고 대상이 있는 곳의 게이트웨이를 확인해야 한다. 이런 방법은 가까이 있는 노드간의 통신에서도 마찬가지로 적용되기 때문에 비효율적인 작동 방법이다. 이러한 기존의 프로토콜이 가지고 있는 문제점을 개선하기 위해 새로운 모바일 네트워크 프로토콜을 제안하고 이를 빠르고 지능적인 PMIPv6라는 의미의 i-FP(intelligent Fast PMIPv6)로 명명한다.

i-FP는 기존의 로컬 이동성 프로토콜의 성능을 향상시킨다. i-FP의 첫번째 목적은 도메인 내 트래픽에 최적화된 라우팅 서비스를 제공하는 것이다. RO(Route Optimization) 서비스는 i-FP가 통신 중인 피어들 사이의 최단 경로를 찾아 빠르게 도메인 내 트래픽을 전달할 수 있게 해준다. i-FP의 두번째 목적은 네트워크 트래픽 오버헤드를 감소시키는 것인데 특히 무선 링크에 초점이 맞춰져 있다. 제한된 대역폭으로 기존의 무선 애플리케이션은 항상 많은 부하를 받기 때문에, 무선 링크의 효율적인 트래픽 관리는 무선 네트워크의 성능을 향상시킬 수 있다. 마지막으로 i-FP는 느슨한 도메인 토폴로지에 적용하여 구현 비용을 감소하는 것을 목표로 하고 있다. i-FP는 이동성 에이전트와 이동성을 관리하기 위해 엑세스 라우터를 사용한다. 동시에 네트워크 트래픽 오버헤드를 피하기 위해 IP 헤더 스와핑 기술을 사용한다. 새롭게 제안하는 i-FP의 성능을 평가하기 위해, 로컬 이동성 프로토콜과 관련된 다른 프레임워크와 i-FP를 비교하는 성능 평가를 실시한다. 그 결과를 토대로 i-FP가 로컬 도메인에서 가장 효과적인 기법이라는 것을 증명한다.

논문은 다음과 같이 구성되어 있다. 2장에서는 관련 연구를 설명하고, 3장은 제안하는 기법의 아키텍처와 작동절차를 설명한다. 4장에서는 제안 기법의 성능평가를 수행하고, 마지막으로 5장에서는 성능평가 결과에 따른 결론을 내린다.

Ⅱ. 관련연구

F-PMIPv6(Fast Proxy Mobile IPv6)[5]는 PMIPv6 환경에서 FMIPv6의 고속 핸드오버 기법을 적용하였으며, MN(Mobile Node)이 이동하기 전에 이동 신호를 감지하여 pMAG(previous Mobile Access Gateway)가 nMAG(new Mobile Access Gateway)에게 MN(Mobile Node)의 정보 전송을 위해 HI(Handover Initiate)와 HAck(Handover Acknowledgement) 메시지를 이용하여 MN의 핸드오버를 준비한다. 이때, pMAG와 nMAG 사이에 터널이 형성되고, MN과 통신이 끊기는 동안에 LMA(Local Mobility Anchor)로부터 오는 데이터를 pMAG에서 nMAG로 버퍼링한다. MN이 nMAG에 접속하여 통신이 연결되면 nMAG가 버퍼링하고 있던 패킷 데이터를 MN으로 전송하여 핸드오버하는 시점에 연결이 단절되어 발생하는 패킷 데이터 손실을 방지하여 통신을 유지할 수 있다. F-PMIPv6는 두 가지 모드로 나

뉘어 수행되며, Predictive 모드와 Reactive 모드가 있다. Predictive 모드는 MN이 nMAG로 이동하기 전에 pMAG와 nMAG사이에 양방향 터널이 생성되는 모드이다. 따라서 MN이 이동하기 전에 pAN에게 이동이 예측되는 nAN의 정보와 MN의 정보(MN-ID)를 포함한 Report메시지를 전송한다. Report 메시지를 받은 pAN은 pMAG에게 MN-ID와 n-AN ID를 포함한 HI 메시지를 전송하여 MN의 이동을 알린다. pMAG는 MN과 LMA의 정보를 담은 HI메시지를 nMAG에게 전송한다. HI메시지를 받은 nMAG는 그에 대한 응답인 HAck(Handover Acknowledgement) 메시지를 pMAG에게 전송한다. pMAG가 HAck메시지를 받은 후, pMAG와 nMAG 사이에 양방향 터널을 형성한다. 양방향 터널이 형성된 시점부터 pMAG는 LMA가 MN에게 전송한 패킷을 nMAG에게 전송하며, nMAG는 pMAG에게 전송받은 패킷을 버퍼에 담아둔다. MN이 L2 핸드오버가 끝난 후 nMAG에 연결이 되면 nMAG는 저장한 패킷을 MN에게 전송하고, LMA에 MN의 바인딩을 위해 PBU(Proxy Binding Update) 메시지를 전송한다. LMA는 PBU 메시지를 받은 후 BCE에 MN의 상태 정보를 등록하고 PBA 메시지를 nMAG에 전송한다. MN은 nMAG가 LMA에게 PBA 메시지를 응답 받는 것으로 바인딩 과정을 완료한다. 이후 MN으로 전송되는 패킷은 nMAG를 통해서 전송하게 된다. Reactive 모드는 MN이 nMAG로 이동한 후에 pMAG와 nMAG 사이에 양방향 터널이 형성되는 모드이다. 따라서 MN이 nMAG로 빠르게 이동하여 Predictive 모드가 실패하고 nMAG에게 연결되었을 때 수행하며, nMAG는 HI메시지를 pMAG에 전송하고, HI 메시지를 받은 pMAG는 HAck 메시지를 nMAG에게 전송한다. Predictive 모드와 동일하게 pMAG와 nMAG 사이에 양방향 터널이 형성되고, nMAG는 MN의 패킷을 버퍼링하여 저장한다. 또한, nMAG는 LMA에게 MN의 바인딩을 위해 PBU 메시지를 보낸다. LMA는 PBA(Proxy Binding Acknowledgement) 메시지를 nMAG에게 전송하여 바인딩 과정을 완료한다. 내용은 그림 1과 같다.

PMIPv6[2]는 네트워크에서 이동성 지원을 위한 모바일 노드의 참여나 활용 없이 IP 기반 시그널링 모바일 노드의 이동성을 지원하는 프로토콜이다. 모든 이동성 시그널링과 라우팅 상태의 설정은 네트워크의 이동성 엔티티에 의해 이루어진다. 이 기법에서 주요 기능적인 엔티티는 LMA와 MAG이다.

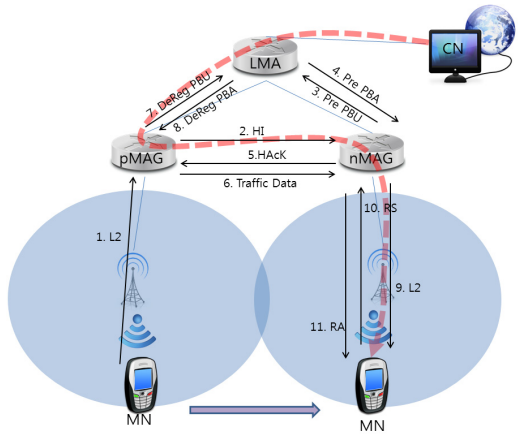

그림 1. F-PMIPv6의 작동 절차
Fig. 1. Handover operation of the F-PMIPv6

LMA는 모바일 노드의 도달 가능성 상태와 모바일 노드 HNP(Home Network Prefix)의 토폴로지 앵커 포인트가 되는 책임을 가지고 있다. MAG는 모바일 노드가 연결되어 있는 엑세스 링크이고 모바일 노드를 대신해 이동성관리를 수행한다. MAG의 역할은 모바일 노드가 엑세스 네트워크 안으로 들어오고 나가는 것을 감지하고, 모바일 노드의 LMA로 바인딩 등록을 초기화하는 것이다. 내용은 그림 2와 같다.

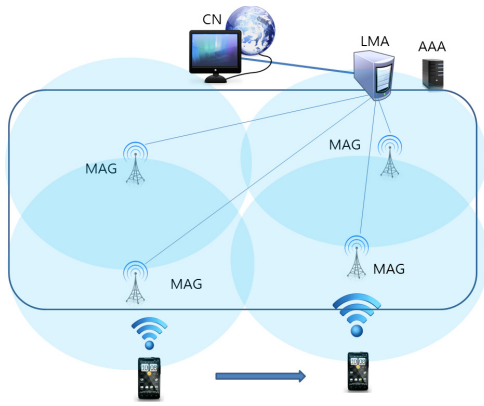

그림 2. PMIPv6의 개념도
Fig. 2. Concept of the PMIPv6

HMIPv6(Hierarchical Mobile IPv6)[4]는 MIPv6에서 MN이 이동하면서 발생하는 핸드오버 지연을 줄이기 위한 방법의 하나로 IETF에서 제안된 프로토콜이다. HMIPv6는 모바일 노드의 이동을 지역적으로 관리함으로써 모바일 노드의 핸드오버로 인한 시그널링을 줄여주는 프로토콜이고 MIPv6가 바인딩 업데이트를 하는 동안 발생하는 지연과 시그널링 오버헤드를 감소시킨다. MIPv6는 MN이 다른 서브넷으로 이동할 때 HA(Home Agent)와

CN(Corresponding Node)으로 바인딩 업데이트가 필요하다. MN이 HA나 CN에서 멀리 있으면 바인딩 업데이트 절차는 불필요한 지연과 시그널링 오버헤드를 유발한다. 엑세스 네트워크는 이 문제를 해결하기 위해 HMIPv6에서 계층적으로 구성되어 있다. HMIPv6는 지역 이동성관리에 증가하고 있는 네트워크에서의 사용자 이동성과 확장성으로 인한 시그널링 비용을 줄일 수 있고 글로벌 이동성관리와 지역 이동성을 분리했다. 글로벌 이동성관리는 여전히 MIPv6에 의해 관리되지만 로컬 도메인 내에서의 지역 이동성관리는 지역 이동성관리 에이전트인 MAP으로부터 관리된다. 그러므로 MAP 지역에서의 이동은 HA와 CN에서는 알 필요가 없기 때문에 그에 관한 정보를 유지하거나 관리하기 위해 필요한 MIPv6에서의 지연과 시그널링 오버헤드를 상당부분 감소시킬 수 있다. 내용은 그림 3과 같다.

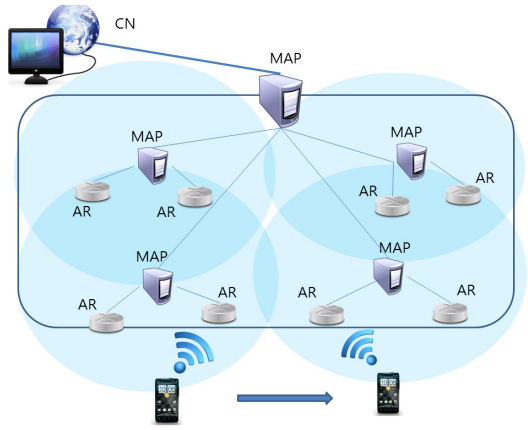

그림 3. HMIPv6의 개념도
Fig. 3. Concept of the HMIPv6

로컬 이동성 프로토콜에는 CIP[8], HAWAII[9], HMIPv6[4], TeleMIP[10], DMA[11], PMIPv6[6,20-22] 등 많은 프로토콜이 있지만 이들은 여러 단점[12-15]을 가지고 있다. 예를 들면 CIP와 HAWAII는 도메인 토폴로지에 엄격한 트리 구조를 강제하고 있다. 계층적 구조는 이동성 에이전트를 기반으로 하고 있으며, 모든 라우터는 이동성 시그널링에 관여해야 한다. 그러므로 CIP와 HAWAII는 도메인내에 있는 모든 라우터의 업그레이드가 필요하기 때문에 이를 위한 구현 비용이 많이 든다. HMIPv6, TeleMIP, DMA, PMIPv6와 같은 다른 프로토콜은 모든 라우터의 이동성 시그널링 참여가 필요하지 않다. 대신에 토폴로지 앵커 포인트로서의 이동성 에이전트와 외부 에이전트로서 엑세스 라우터를 도입한다. 이동성 에이전트와 엑세스 라우터의 협력을 통해, 위 프로토콜들은 트래픽을 로컬 도메인내의 이동하는 사용자에게 전달할 수 있다. 비록 이 프로토콜들이 도메인 토폴로지 내에서 별다른 기능을 요구하지 않는다 해도, 이들은 인트라 도메인 트래픽에 대한 심각한 라우팅 문제를 가지고 있다. 만일 한 사용자가 패킷을 같은 도메인에 위치해 있는 통신 중인 피어에게 보내려고 하면, 패킷은 처음 도메인 게이트웨이 라우터로 전달되고 사용자가 통신하고 있는 피어에게 전달된다. 요즘 온라인 게임 등과 같은 멀티미디어 어플리케이션이 인기가 많은데 삼각 라우팅 경로는 추가적인 전송 지연이 발생하고 대역폭의 자원 낭비를 가져온다. HMIPv6, DMA, TeleMIP은 비슷한 전달 절차와 이동성 시그널링을 공유하고 있다. 이 프로토콜들은 글로벌 이동성과 도메인 전달 수행을 위한 네트워크 특정 주소의 바이딩을 위해 도메인의 특별 주소를 사용한다. HMIPv6, DMA, TeleMIP, PMIPv6는 네트워크 지원 이동성이 아니며 이들은 도메인 라우팅과 바인딩 수행을 위해 하나의 주소만 사용한다. 네트워크 지원 방식은 신호 비용을 줄이기 위해 PMIPv6를 도울 수 있다.

Ⅲ. 빠르고 지능적인 계층적 이동성 지원(i-FP)

여기서는 소단원에 관한 내용을 간단히 살펴본다. 여기서는 소단원에 관한 내용을 간단히 살펴본다.

3.1. 네트워크 아키텍쳐

HMIPv6, PMIPv6 보다 나은 성능을 얻기 위해 i-FP에서는 PMIPv6의 세가지 주요 엔티티인 LMA, MAG, MN을 그대로 사용하고 이에 추가적인 기능을 부여하여 성능 향상을 시켰다. 그림 4는 i-FP의 시스템 구조를 나타낸다.

LMA는 로컬 도메인의 게이트웨이 라우터이다. LMA는 MN을 위한 프록시 HA와 같은 역할을 한다. MN이 로컬 도메인에서 이동 할 때, LMA는 MN 대신에 트래픽을 받고, 트래픽을 MN이 위치한 링크로 전송한다. 이를 가능하게 하기 위해, i-FP에서는 MN을 관리하기 위한 방법으로 HMIPv6에서 사용하는 두 가지 주소 엔티티인 RCoA(Regional Care of Address)와 LCoA(on Link Care of Address)를 사용한다. RCoA는 MN이 처음 로컬 도메인에 진입했을 때 MN으로부터 얻어진 주소이고 로컬 도메인에서 MN의 고유함을 증명할 수 있는 신원증명서 같은 역할을 한다. MN은 RCoA를 HA[16]나 통신 중인 피어[3]들을 업데이트하기 위한

위치 표시로서 사용한다. 로컬 도메인에서 MN이 움직일 때, RCoA는 변하지 않고 고정되어 있기 때문에 MN은 HA나 통신중인 피어에게 로컬 도메인 밖으로 나가지 않는 한 바인딩 업데이트 메시지를 보낼 필요가 없다. 그러나 RCoA는 MN이 위치한 도메인은 확인할 수 있으나 도메인 내부의 이동에 관한 업데이트 영향을 받지 않기 때문에 명확하게 MAG 에 접속해 있는지 여부를 정확하게 알 수 없다. 따라서 MN의 보다 상세한 위치를 찾기 위해, i-FP는 LCoA라는 주소를 MN에 사용한다. LCoA는 MN의 위치와 동일한 주소이고 MN이 접속한 MAG의 위치를 바꿀 때마다 업데이트를 하여 항상 MN의 위치정보를 가지게 된다. 동시에 LMA는 MN을 위해 RCoA와 LCoA를 관리한다. 만약 LMA가 MN으로 가는 방향의 트래픽을 받으면, LMA는 패킷의 목적지를 RCoA에서 LCoA로 바꾼다. LCoA로 도메인 내에서 보다 빠르고 정확하게 MN이 위치한 게이트웨이를 찾을 수 있다. 그리고 LMA는 업데이트된 패킷을 MN이 접속해 있는 MAG로 보낸다. LCoA는 MN의 위치를 정확하게 나타내고 있으므로 MN은 패킷을 성공적으로 받을 수 있다. LMA의 RCoA와 LCoA간의 바인딩을 통해 i-FP는 도메인 내에서 접속한 MN과 CN간의 트래픽을 정확하고 빠르게 전달 할 수 있다. 그러나 LMA는 도메인내의 로컬 이동성을 단독으로 관리할 수 없다.

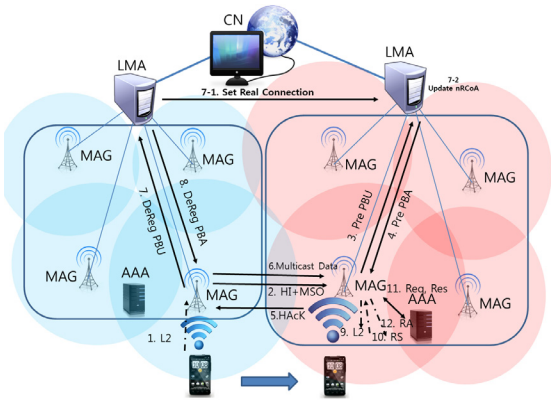

그림 4. i-FP의 개념도
Fig. 4. Concept of the i-FP

i-FP는 MN의 핸드오버 관리를 위해 PMIPv6의 MAG를 이용한다. MAG는 엑세스 라우터인데, 이것은 i-FP 도메인 내의 무선 네트워크를 책임지고 있다. MAG는 로컬 도메인 내에서 AR(Access Router) 엔티티에 해당된다. MAG는 MN에 무선 링크를 제공하는 여러 AP를 상호 연결한다. MN이 MAG의 네트워크에 접속하면, MAG는 MN을 위한 RR(Register Request) 메시지를 LMA에 전송한다. MN이 인증된 사용자라면, MAG는 MN에 접속을 허용하는 엑세스 서비스를 제공한다. 예를 들면, MAG는 새로운 LCoA를 MN에게 지정하고, MN의 트래픽을 그에 대응하는 무선 링크에 전달하는 것을 말한다. 또한, MN이 i-FP 도메인 내에 위치하고 있는 다른 MN에 패킷 전송을 시도 할 때는 MAG는 패킷의 목적지 주소를 업데이트하고, 패킷이 최적의 경로를 통해 MN의 피어에게 라우팅되었다는 것을 보증할 것이다. 패킷 포워딩의 절차는 다음 섹션에서 자세히 다룬다.

i-FP을 위한 세번째 엔티티는 MN이다. MN은 로컬 도메인 내에서 로밍을 하는 무선 장비이다. i-FP 도메인에서 모든 MN은 데이터 링크 레이어와 네트워크 레이어 사이에 IP 스와핑 메커니즘[7]을 가지고 있다. 이 에이전트는 MN 트래픽의 IP 헤더를 처리 할 때 사용된다. MN이 목적지가 LCoA인 패킷을 받으면 IP 스와핑 에이전트는 패킷의 목적지를 RCoA로 변경하고 그 다음 패킷을 네트워크 레이어로 보낸다. 동시에 네트워크 레이어에서 패킷을 보낼때 IP 스와핑 에이전트는 패킷 소스 주소를 MN의 LCoA에 업데이트한다. IP 스와핑 에이전트의 IP 헤더 관리를 통해 MN은 LCoA의 변경을 알지 않고 통신 세션을 유지할 수 있다. 이런 이유로, MN은 도메인내의 다른 네트워크로 이동하더라도 연결을 유지 할 수 있다.

로컬 도메인에서 HMIPv6와 PMIPv6는 IP 터널링 기술을 사용하고 i-FP는 IP 스와핑 메커니즘을 사용한다. 트래픽을 전달할 때, HMIPv6는 MAP와 MN사이에 터널을 생성한다. 그러나 PMIPv6는 LMA와 MAG사이에 터널을 생성한다. 그렇기 때문에 HMIPv6의 모든 데이타 패킷은 무선과 유선 링크에서 하나의 추가적인 IP 터널 헤더를 발생시키지만 PMIPv6는 유선 링크에서만 트래픽 오버헤드를 발생시킨다. 또한, 터널 전송 기술로 HMIPv6와 PMIPv6는 인트라 도메인 트래픽을 위한 서브 최적화 경로를 제공한다. i-FP는 IP 스와핑 기술을 사용하기 때문에 터널링 비용과 지연 시간이 발생하지 않고 서브 최적화 경로 문제를 해결하고 추가적인 IP 헤더가 필요 없다. HMIPv6는 MAP, MN이라고 하는 두 가지 엔티티가 관련되어 있고 PMIPv6는 세가지 네트워크 엔티티인 LMA, MAG, MN이 이동성관리에 사용되며 i-FP는 PMIPv6와 같은 LMA, MAG, MN을 이동성관리에 사용한다. 다음으로,

MN의 IP 주소는 세가지 이동성관리 프로토콜에서 사용된다. HMIPv6와 i-FP에서 MN은 RCoA와 LCoA라는 두 가지 IP 주소를 가지고 있다. RCoA는 MN의 식별을 위해 사용되고 로컬 도메인 내에서 MN이 이동하는 동안에는 변경되지 않는다. LCoA는 MN을 접근할 수 있는 위치를 나타내고 MN이 새로운 네트워크로 이동할 때 마다 변경된다. 그러나, PMIPv6에서는 LMA와 MAG가 이동성 시그널링을 MN대신에 관리하기 때문에 MN의 IP 주소는 PMIPv6 도메인 내에서는 변경되지 않는다. i-FP가 PIMPv6보다 IP 주소를 더 사용하지만, IPv6가 충분한 IP 주소 리소스를 가지고 있기 때문에 큰 문제가 되지 않는다. HMIPv6는 유선, 무선 링크에 프로토콜 시그널링 비용이 들어가지만 PMIPv6와 i-FP에서는 무선 링크에 대한 시그널링 비용은 없고 프로토콜 데이터는 유선 네트워크에서만 전송된다. 그러므로 PMIPv6와 i-FP는 핸드오버 시에 무선 대역폭 오버헤드를 발생하지 않는다.

3.2. 작동절차

i-FP 네트워크에서 등록절차를 수행하기 전에, MN은 네트워크에 처음 접속하게 되면 RCoA를 얻게 되는데 MN은 처음 SC(Stateless Configuration)나 DHCP[17]를 사용하여 네트워크상에서 고유한 MN의 RCoA를 얻는다. 그리고 MN은 RCoA를 글로벌 이동성 에이전트에 등록한다. RCoA는 MN이 한 도메인에 위치하고 있는 동안 바뀌지 않기 때문에 도메인 내의 어떤 이동에도 글로벌 이동성 프로토콜은 유지된다. RCoA를 얻고 나면, MN은 그림 4에 나온 것과 같은 등록절차를 시작한다. MN이 핸드오버를 하면, 새롭게 접속된 MAG는 MN에 RA(Router Advertisement) 메시지를 전송한다. RA 메시지는 MN이 새로운 네트워크 게이트웨이(MAG)에서 LCoA를 얻는 것을 도와준다. 그리고 MAG는 로컬 도메인에 속해있는 MN에게 얻은 LCoA와 RCoA를 바인딩하고 LCoA와 RCoA를 LBU(Local Binding Update) 메시지에 담아 LMA에 보낸다. LMA가 LBU 메시지를 허용하면, RCoA와 LCoA사이에 바인딩 엔트리를 설정한다. 이 정보는 도메인 간 통신에 사용된다. 동시에 LMA는 LBA(Local Binding Acknowledgement) 메시지를 MAG에 보낸다. MAG가 LBA를 받는 즉시, 등록 절차는 완료되고 MN은 새로운 위치에서 패킷 전송을 시작할 수 있다. i-FP 도메인에서 트래픽은 두 가지로 구분된다. 하나는 도메인 간 트래픽이고, 하나는 도메인 내의 트래픽이다. CN(Corresponding Node)과 MN이 다른 로컬 도메인 내에 위치하고 있으면, 전송되는 트래픽은 도메인 간 트래픽이고, 그렇지 않은 경우는 도메인 내 트래픽을 의미한다. 두 종류의 트래픽을 위해 i-FP는 두 가지 다른 포워딩 절차를 사용한다.

도메인내의 트래픽 전달은 MAG에서 주소 관리에 관여한다. MN1이 MN2로 패킷을 전송할 때, MN1의 IP 스와핑 에이전트(ISM)는 처음 소스 주소를 LCoA로 업데이트하고 MAG1로 패킷을 보낸다. 전송 경로상의 첫번째 홉인 MAG1은 패킷의 목적지를 MN2의 LCoA로 업데이트하고 도메인 내 패킷 전송이기 때문에 LMA를 거치지 않고 MAG2로 패킷을 LCoA를 참조하여 바로 보낸다. 패킷을 수신한 MAG2는 패킷의 목적지가 자신에게 접속해 있는 MN이라는 것을 LCoA를 통해 인식하고 MAG2는 패킷 소스의 주소를 원주소인 RCoA로 변경한다. 마지막으로 패킷이 MN2로 보내지면, MN2의 IP 스와핑 에이전트는 패킷의 목적지를 RCoA로 바꾼다. MN2는 패킷을 전송 받게 된다. MN2가 전달 받은 패킷을 처리하고 난 후 다시 MN1로 응답 메시지를 전송하면, 무선 링크의 IP 스와핑 메커니즘은 MN2의 주소를 LCoA로 변경하고 MAG2로 패킷을 전송한다. MAG2에서는 도메인내의 패킷 이동이기 때문에 도착지 주소를 LCoA로 변경 한 후 MAG1로 패킷을 전송한다. 패킷을 전달 받은 MAG1는 도착지가 자신이 관리하는 MN을 가리키고 있기 때문에 도착지 출발 주소를 원주소인 RCoA로 변경하고 MN1로 패킷을 전달한다. MN1이 패킷을 받기 전 무선 링크의 IP 스와핑 메커니즘에서는 MN1의 주소인 도착지 주소를 원주소인 RCoA로 변경하고 패킷을 전달한다. 이러한 절차로 인해 MN1, MN2와 같은 모바일 노드에서는 원주소만 알고 있으면 도메인 내부의 패킷 주소 관리 메커니즘으로 다른 기능적 요구사항 없이 패킷을 주고 받을 수 있다. 이러한 내용은 그림 5와 같다.

도메인 내부에서의 MN의 핸드오버는 MN이 최초 자신이 접속해 있는 pMAG에게 핸드오버를 곧 하겠다는 의미의 L2 신호를 보낸다. 이를 인식한 pMAG는 MN이 핸드오버를 할 것으로 예상되는 nMAG에게 핸드오버를 준비하라는 의미의 HI 메시지를 MN의 LCoA와 함께 보낸다. HI 메시지를 전달받은 nMAG는 새롭게 부여할 nLCoA를 생성하여 LMA에게 사전 등록을 요구하는 Pre-BU 메시지에 LCoA와 nLCoA를 담아 전송한다. LMA에서는 Pre-BU 메시지를 받게 되면, 사용자 인증을 AAA 서버에 하고, 통과된 사용자는 RCoA와 nLCoA 정

보를 맵핑시켜 사전 등록을 임시로 시킨다. 그 후 LMA는 nMAG에게 등록이 완료되었음을 의미하는 Pre-BA 메시지를 보내고 이를 받은 nMAG는 pMAG에게 핸드오버가 준비되었음을 알리는 HAck 메시지를 전송한다. HAck를 받은 pMAG는 자신에게 전송되는 트래픽을 nMAG에게 전송하고 nMAG는 이를 버퍼링한다. pMAG는 바로 MN의 등록을 해지하기 위해 DeReg BU 메시지를 LCoA를 담아 LMA에 보내고 LMA는 이를 확인하고 LCoA를 nLCoA로 업데이트하여 nMAG에 사전 등록한 MN을 정식으로 등록하게 된다. 이에 대한 응답으로 DeReg BU 메시지를 pMAG에 전달하고 nMAG는 MN에게 L2 메시지에 대한 응답 메시지를 전송한다. MN은 nMAG에 접속을 요청하는 RS 메시지를 전송하고 nMAG에서는 사전에 MN을 등록시켜 두었기 때문에 바로 새로운 LCoA주소인 nLCoA를 RA에 담아 전송하고, 바로 버퍼링 해두었던 트래픽을 전송한다. 이와 같은 절차로 도메인 내의 핸드오버는 마무리되고 MN은 nMAG와 통신을 하게 된다. 이와 같은 절차는 그림 6과 같다.

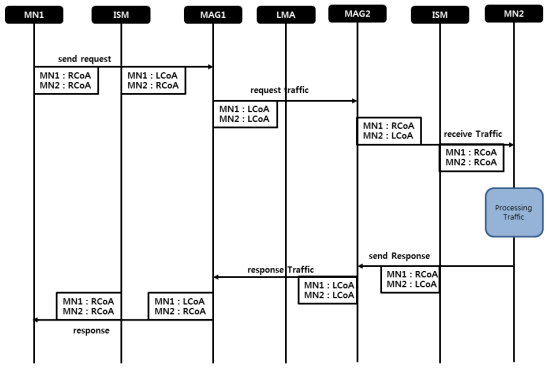

그림 5. i-FP의 도메인 내 흐름
Fig. 5. Flow of i-FP in Intra Domain

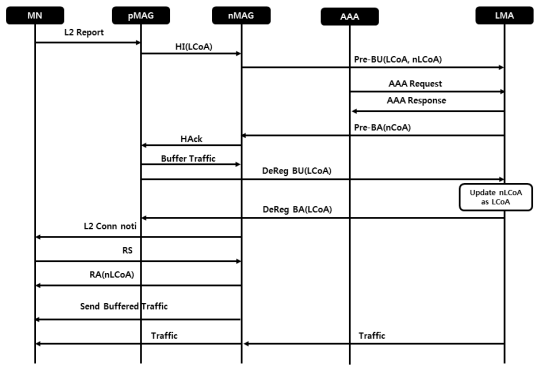

그림 6. i-FP의 도메인내 핸드오버 절차
Fig. 6. Handover of i-FP in Intra Domain

도메인내 트래픽 이동과는 다른 도메인간 트래픽 이동은 처음 MN이 데이터를 요청하기 위해 무선 네트워크를 통해 CN으로 패킷을 보내면, 무선 링크에서는 패킷이 가기 전에 IP 스와핑 매커니즘을 동작시켜 패킷의 소스 주소를 외부 도메인에서도 인식할 수 있는 RCoA로 바꾼다. 바뀐 주소를 가지고 패킷은 MAG로 도착하고, MAG는 로컬 도메인 게이트웨이인 LMA로 패킷을 그대로 전송한다. LMA는 패킷의 목적지가 외부 도메인인 CN이기 때문에, 패킷의 소스 주소를 다시 RCoA로 변환하고 CN에 전달하게 된다. CN은 패킷을 처리한 후 그에 대한 응답 메시지를 RCoA로 보내고 이 패킷은 LMA에서 받아 내부 도메인으로 전달하기 위해 위상적으로 일치하는 주소인 LCoA로 변경하고 해당 MN이 있는 MAG로 패킷을 전송하게 된다. 패킷을 전달받은 MAG는 MN에게 패킷을 전달하고 그 전에 IP 스와핑 메커니즘이 동작해서 LCoA로 되어 있는 주소를 원주소인 RCoA로 전환한 후 MN에 전송한다. LMA 도메인 내부의 IP 전환 메커니즘을 통해 i-FP에서 MN은 IP의 변화를 관여하거나 알고 있을 필요 없이 외부 도메인과 패킷을 주고 받을 수 있게 된다. 이는 그림 7의 i-FP의 도메인 간 트래픽 이동 경로에 나와 있다.

도메인간의 핸드오버는 최초 자신이 접속해 있는 pMAG로 접속이 곧 단절될 것을 의미하는 L2 메시지를 보낸다. 이를 받은 pMAG는 접속이 예상되는 도메인의 nMAG로 HI 메시지와 함께 MN의 RCoA를 전송한다. 이를 식별한 nMAG는 자신이 속한 nLMA에게 MN을 사전 등록시키기 위해 Pre-BU 메시지를 RCoA와 새로 할당할 주소인 nLCoA를 함께 전송한다. nLMA에서는 Pre-BU 메시지를 받고 AAA서버에 사용자인증을 하고 인증이 통과되면 nRCoA를 생성하여 nLCoA와 함께 저장하고 사전 등록을 시킨다. LMA는 이에 대한 응답으로 nMAG에 Pre-BA 메시지를 nRCoA와 함께 전송한다. 이를 받은 nMAG는 pMAG에게 핸드오버 준비가 완료되었음을 의미하는 Hack 메시지를 전송한다. 이를 받은 pMAG는 nMAG로 자신에게 전달되는 트래픽을 전송하고 nMAG는 전송받은 트래픽을 버퍼링한다. 이후 pMAG는 MN을 접속 해지하기 위해 자신이 속한 pLMA에게 DeReg-BU 메시지를 LCoA값을 담아 전송하고, pLMA는 nLMA에게 사전 접속한 MN을 정식 등록하라는 메시지를 RCoA와 함께 보내고 nLMA는 맵핑된 RCoA와 nRCoA를 이용해 nRCoA를 식별하여

nRCoA를 정식등록하고, pLMA에게 응답 메시지를 보낸다. 응답 메시지를 받은 pLMA는 pMAG에게 DeReg BA 메시지를 보내어 등록 해지를 알린다. nMAG에서는 최초 MN이 전송한 L2 메시지에 대한 응답메시지를 전송하고 MN는 nMAG에 접속을 요청하는 RS 메시지를 전송한다. 이를 받은 nMAG는 MN에게 새롭게 할당된 nRCoA와 nLCoA주소를 RA메시지에 담아 전송한다. 그 후 버퍼링 해두었던 트래픽 데이터를 MN에게 전송한다. 이와 같은 과정으로 도메인간 핸드오버는 마무리되고 MN은 nMAG와 빠른 접속과 통신이 가능하다. 이는 그림 8에 나와있다.

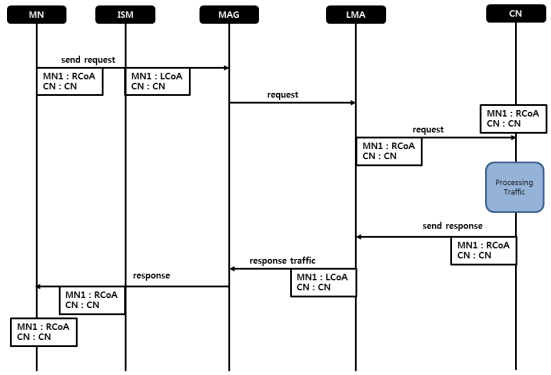

그림 7. i-FP의 도메인 간 흐름
Fig. 7. Flow of i-FP in Inter Domain

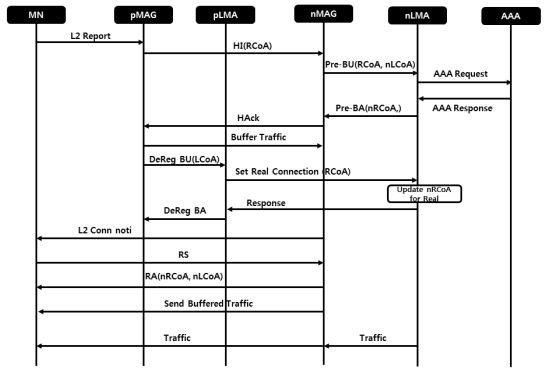

그림 8. i-FP의 도메인 간 핸드오버 절차
Fig. 8. Handover of i-FP in Inter Domain

Ⅳ. 성능평가

이번 장에서는, 기존에 제안된 두 가지 방식인 HMIPv6, PMIPv6와 새롭게 제안하는 i-FP 기법을 수학적 모델링을 하여 성능평가를 실시한다. 동일 조건하에서 각 기법이 얼마나 많이 네트워크에서 생성된 비용을 감소시킬 수 있는지 분석했다. 각 비용은 메시지의 크기와 대역폭 관점으로 홉 거리에 의해 정의된다. 이 정의에 따라, 라우터 프로세싱 비용은 고려하지 않았으며, 분석적인 모델을 위해 표 1에는 성능 분석에 사용되는 모바일 프로토콜을 위한 매개변수가 정의 되어 있다.

표 1. 성능분석에 사용된 매개변수 값
Table 1. Parameter values for performance analysis

Parameter	value	Parameter	value
H_{CN-DGR}	2 hops	$H_{AR1-AR2}$	1 hop
H_{DGR-AR}	1 hop	i-FP_BU	96 bytes
H_{AR-MN}	1 hop	i-FP_BA	96 bytes
$H_{MN1-AR1}$	1 hop	i-FP_RouterSol	44 bytes
$H_{AR1-DGR1}$	1 hop	i-FP_RouterAdv	68 bytes
$H_{DGR1-AR2}$	1 hop	i-FP_BEU	142 bytes
$H_{AR2-MN2}$	1 hop	HMIPv6_RBU	80 bytes
HMIPv6_RBA	60 bytes	PMIPv6_PBA	88 bytes
HMIPv6_RouterSol	44 bytes	PMIPv6_RouterSol	44 bytes
HMIPv6_RouterAdv	68 bytes	PMIPv6_RouterAdv	68 bytes
PMIPv6_PBU	88 bytes	$T_{MAG-LMA}$	100 ms
D_{L2}	100 ms	$W_{MAG-LMA}$	300 ms
A	10 ms	T_{MN-LMA}	200 ms
T_{MN-MAP}	100 ms	$L_{IPHeader}$	100 bytes
W_{MN-MAP}	300 ms	H_{MAP-MN}	2 hops
$H_{LMA-MAG}$	1 hop	U	10000 bytes
R	1000 bps	p	0.5

4.1. 라우팅 홉 수

첫 성능 분석은 전송 지연의 정도를 알 수 있는 척도인 트래픽 라우팅 홉 수다. i-FP의 한가지 중요한 목적은 도메인 내부의 트래픽에 최적의 라우팅 경로를 제공하는 것이다. 이번 섹션은 인트라 도메인 트래픽의 라우팅 홉 수를 세가지 프로토콜로 나타낸다. 동시에 인트라 도메인 트래픽의 전송 지연을 비교하고, 세가지 프로토콜의 인트라 도메인 트래픽의 라우팅 홉 수를 나타낸다. 인트라 도메인 트래픽의 라우팅 홉 수는 세가지 프로토콜이 동일하다. CN에서 패킷이 보내질 때, 도메인의 DGR은

패킷 목록을 받는다. 그때, DGR은 패킷을 새로운 MN이 접속해 있는 AR로 전송한다. AR은 패킷을 무선링크를 통해 MN에게 전송한다. 그렇기 때문에 도메인 외부에서 온 트래픽의 라우팅 홉 수는 식 (1)과 같이 나타낼 수 있다. H_{X-Y} 는 노드 X와 노드 Y의 라우팅 홉 수를 의미한다. HMIPv6와 PMIPv6에서는 패킷은 DGR에 의해 전송 받는 것이 요구된다. 그리고, DGR은 패킷을 캡슐화하고 이를 MN의 현재 위치로 전송한다. 그렇기 때문에 HMIPv6와 PMIPv6에서의 인트라 도메인 트래픽은 삼각 라우팅 문제를 발생한다. 그러나 i-FP에서는 인트라 도메인의 라우팅 홉 수는 기존 방법과는 다르다. i-FP에서 MN이 패킷을 다른 MN으로 보내려고 하면, 패킷은 AR1에 도착하고 AR1은 트래픽을 MN2가 위치해 있는 AR2로 전송한다. 그리고 마지막으로 AR2는 패킷을 MN2로 전송한다. 패킷은 가장 짧은 경로로 전송되므로 i-FP의 라우팅 홉 수는 HMIPv6와 PMIPv6 보다 작다. 식 (1)은 HMIPv6, PMIPv6, i-FP의 도메인 외부에서 전달되는 트래픽의 라우팅 홉 수를 나타내고, 식 (2), 식 (3), 식 (4)는 도메인 내의 트래픽에 대한 라우팅 홉 수를 나타낸다. PMIPv6의 MAG는 동일한 MAG 네트워크에 MN1, MN2가 위치해 있을 때 모바일 노드의 브릿지로 설정될 수 있다. 로컬 라우팅 최적화 메커니즘은 전송 지연을 감소시킬 수 있다. 그러나 만약 인트라 도메인 통신이 다른 MAG 네트워크에 위치해 있으면 패킷은 LMA로 전송되어야 하므로 LMA는 CN의 네트워크로 패킷을 전송할 것이다. 전송 트래픽의 절반정도가 같은 MAG에서 발생하고 나머지 절반의 트래픽은 다른 MAG에서 발생한다고 가정한다. 이런 의미에서 PMIPv6의 평균 라우팅 홉 수는 HMIPv6보다 작다.

$$H_{Inter}^{HMIPv6} = H_{Inter}^{PMIPv6} = H_{Inter}^{i-FP} = H_{CN-DGR} + H_{DGR-AR} + H_{AR-MN} \quad (1)$$

$$H_{Intra}^{HMIPv6} = H_{MN1-AR1} + H_{AR1-DGR1} + H_{DGR1-AR2} + H_{AR2-MN2} \quad (2)$$

$$H_{Intra}^{PMIPv6} = H_{MN1-AR1} + H_{AR2-MN2} + \frac{H_{AR1-DGR1} + H_{DGR1-AR2}}{2} \quad (3)$$

$$H_{Intra}^{i-FP} = H_{MN1-AR1} + H_{AR2-MN2} + \frac{H_{AR1-AR2}}{2} \quad (4)$$

4.2. 프로토콜 시그널링 비용

프로토콜 시그널링 비용은 MN이 위치를 업데이트 할 때 사용되는 패킷의 양이다. 시그널링 비용에는 RS(Router Solicitation) 메시지, BU(Binding Update) 메시지, BA(Binding Acknowledgement) 메시지가 포함된다. 또한 프로토콜 시그널링 비용은 각각 네트워크의 변경하는 MN에 의해 발생한다. 이 장에서는 프로토콜 시그널링 비용을 C_S 로 표현하고 이는 핸드오버 절차로부터 추가적인 비용이 발생한다. 특별히 C_S 에는 네가지 매개변수가 사용된다. p는 단위 시간 t동안 발생하는 하나의 핸드오버가 일어날 확률이다. 핸드오버 확률 p로 인해, MN에 머무를 확률은 $\Pi_{MN} = 1 - p$ 로 표현한다. s는 핸드오버 절차에 사용되는 프로토콜 패킷의 총 사이즈이다. m은 도메인 내의 모바일 노드의 수이고 t는 단위 시간이다. N은 단위 시간에 발생하는 핸드오버의 수이며, 프로토콜 시그널링 비용은 식 (5)에 의해 계산될 수 있으며, HMIPv6, PMIPv6, i-FP의 시그널링 비용은 각각 식 (6), 식 (7), 식 (8)으로 표현된다.

$$C_S = \sum_{n=1}^{\infty} n * p^n * (1-p) * m * \frac{s}{t} \quad (5)$$

$$C_S^{HMIPv6} = \sum_{n=1}^{\infty} n * p^n * (1-p) * m * \frac{RBU + RBA + RS + RA}{t} \quad (6)$$

$$C_S^{PMIPv6} = \sum_{n=1}^{\infty} n * p^n * (1-p) * m * \frac{PBU + PBA + RS + RA}{t} \quad (7)$$

$$C_S^{i-FP} = \sum_{n=1}^{\infty} n * p^n * (1-p) * m * \frac{RS + RA}{t} \quad (8)$$

4.3. 핸드오버 지연

MN이 하나의 네트워크에서 다른 네트워크로 핸드오버 할 때, MN이 트래픽을 전송 받지 못하는 시간이 있다. 이 시간을 핸드오버 지연이라고 한다. 일반적으로 핸드오버 지연 D_{HO} 에는 세가지 이유가 있다. 첫째로, MN이 다른 네트워크로 이동할 때, MN의 이전의 무선 연결은 단절된다. 그러므로 MN은 사용할 수 있는 무선 링크를 찾고 다른 무선 링크에 접속할 필요가 있다. D_{L2} 는 L2 링크 스위치 절차의 결과인 지연을 표현하는데 사용된다. 새로운 네트워크의 링크로 접속한 후에, MN은 새로운 위치에 의한 새로운 IP 주소를 얻을 것이다. D_{IP} 는 새로운 네트워크에서 MN이 IP 연결을 얻기 위한 시간을 나타내는데 사용된다. 이는 핸드오버 지연에 큰 영향을 차지한다. 그러나 D_{IP} 를 줄이는 몇 가지 메카니즘이 있다. 예를 들어, 최적화된 주소 설정[18,19]은 MN이 DAD(Duplicate Address Detection) 없이 IP 주소를 얻는 것을 허용한다. 이는 D_{IP} 를

감소시킬 수 있고 이 메커니즘은 MN이 새로운 네트워크에 링크 주소를 설정하기 위해 사용된다. 마지막으로 MN은 새로운 네트워크에서 IP 주소를 얻은 다음 LU 메시지를 보낸다. D_{LU} 는 위치 업데이트 절차를 완료하기 위해 사용되는 시간을 의미한다. 실제로, D_{LU} 는 MN과 그 에이전트 사이의 거리에 의해 주 영향을 미친다. 로컬 이동성 프로토콜은 해당 도메인의 프록시 HA(Home Agent)를 사용하여 D_{LU} 를 관리한다. 핸드오버 지연은 식 (9)로 나타낸다. 같은 네트워크 내에서 세가지 프로토콜의 성능을 평가했다. 이는 세가지 프로토콜의 D_{L2} 는 같다는 것을 의미한다. 그러나 세가지 프로토콜에서 D_{IP} 는 다르다. 첫째로, PMIPv6는 새로운 네트워크에서 MN의 주소를 변경하지 않기 때문에 PMIPv6의 D_{IP} 는 0과 같다. 그 다음, i-FP와 HMIPv6의 D_{IP} 는 MN이 새로운 주소를 설정할 필요가 있기 때문에 0보다는 크다. MN이 새로운 네트워크로 이동할 때, MN은 MN의 주소를 자동으로 설정하기 위한 RA 메시지를 기다릴 필요가 있다. RA 메시지는 AP에 의해 매 간격 마다 보내진다. 그러므로 D_{IP}^{HMIPv6} 와 D_{IP}^{i-FP} 는 랜덤 값을 가지고 만약 MN의 이동 시간이 일정하다고 가정하면 D_{IP}^{HMIPv6} 와 D_{IP}^{i-FP} 의 평균 값은 $\frac{A}{2}$ 와 같다. 세가지 프로토콜의 핸드오버 지연 D_{LU} 는 각기 다르다. HMIPv6는 MN과 MAP사이의 위치 메시지를 변경한다. 동시에 HMIPv6는 핸드오버 절차가 끝난 다음에 터널을 생성할 필요가 있다. MN와 MAP 사이의 터널 생성 시간인 W_{MN-MAP} 는 MN과 MAP의 라운드 트립 시간과 같다. 그러므로 HMIPv6의 D_{LU} 는 $2*T_{MN-MAP}+W_{MN-MAP}$ 와 같다. T_{MN-MAP} 는 MN과 MAP의 전송 시간을 의미하고, W_{MN-MAP} 는 MN과 MAP사이의 터널 생성 시간을 의미한다. 비슷하게, D_{LU} 는 PMIPv6를 위해 MAG와 LMA사이의 업데이트 메시지 변경에 사용된다. 그리고 PMIPv6의 D_{LU} 는 $2*T_{MAG-LMA}+W_{MAG-LMA}$ 로 정의된다.

$T_{MAG-LMA}$ 는 MAG와 LMA의 전송 시간을 의미한다. 그리고 $W_{MAG-LMA}$ 는 MAG와 LMA 사이의 터널 생성 시간을 나타낸다. i-FP에서는 MN과 LMA간 터널을 사용하지 않기 때문에, D_{LU}^{i-FP} 는 $2*T_{MN-LMA}$ 와 같다. 그러므로 핸드오버 지연 공식은 HMIPv6, PMIPv6, i-FP 각각 식 (10), 식 (11), 식 (12)로 표현할 수 있다. A는 이웃하는 응답 메시지의 간격이며, T_{X-Y} 는 노드 X와 Y의 전송 시간이고 W_{X-Y} 는 노드 X와 Y의 터널 생성 시간을 의미한다.

$$D_{HO} = D_{L2} + D_{IP} + D_{LU} \quad (9)$$

$$D_{HO}^{HMIPv6} = D_{L2} + \frac{A}{2} + 2*T_{MN-MAP} + W_{MN-MAP} \quad (10)$$

$$D_{HO}^{PMIPv6} = D_{L2} + 0 + 2*T_{MAG-LMA} + W_{MAG-LMA} \quad (11)$$

$$D_{HO}^{i-FP} = D_{L2} + \frac{A}{2} + 2*T_{MN-LMA} \quad (12)$$

4.4. 트래픽 오버헤드

마지막으로 세가지 프로토콜의 트래픽 오버헤드를 측정해서 결과를 비교한다. HMIPv6와 PMIPv6는 트래픽을 보낼때 IP 터널링 기술을 사용한다. 터널 헤더는 네트워크에서 사용자 데이터의 오버헤드를 발생한다. 세가지 이동성관리 프로토콜의 트래픽 오버헤드는 $C_{overhead}$ 로 표시하고 $C_{overhead} = L_{IPHeader} * H$ 로 정의한다.

$L_{IPHeader}$ 는 IP 터널의 길이이고 H는 패킷이 로컬 도메인에서 가로지르는 홉 수를 뜻한다. 만약 데이터 비율이 R bps이고 사용자 데이터의 패킷 크기를 U라고 하면, HMIPv6, PMIPv6, i-FP의 오버헤드 비용은 식 (13), 식 (14), 식 (15)로 표현할 수 있다.

$$C_{overhead}^{HMIPv6} = L_{IPHeader} * H_{MAP-MN} * \frac{R}{U} \quad (13)$$

$$C_{overhead}^{PMIPv6} = L_{IPHeader} * H_{LMA-MAG} * \frac{R}{U} \quad (14)$$

$$C_{overhead}^{i-FP} = 0 \quad (15)$$

4.5. 수치분석 결과

다양한 조건으로 HMIPv6와 PMIPv6, i-FP 기법의 성능상의 차이를 확인하기 위해 성능 평가를 실시하였고, 그에 따른 수치 결과를 얻었다. 라우팅 홉수, 트래픽 시그널링 비용, 핸드오버 지연, 트래픽 오버헤드 등 네가지 항목으로 평가를 하였으며 언급한 순서대로 각 평가기법의 수치분석 결과를 분

석한다. 그림 9는 세가지 프로토콜의 평균 라우팅 홉 수를 나타낸다. i-FP는 최소의 라우팅 홉 수를 가지고 PMIPv6의 평균 라우팅 홉 수는 HMIPv6보다 작다. δ는 도메인 내 트래픽 F_{intra}을 도메인 간 트래픽 F_{inter}과 도메인내 트래픽 F_{intra}의 합으로 나눈 비율을 나타내고 $\delta = F_{intra} / (F_{inter} + F_{intra})$의 의미이다. 그림에서 보면, i-FP의 평균 라우팅 홉 수는 다른 두 가지 프로토콜 보다 낮은 것을 알 수 있다.

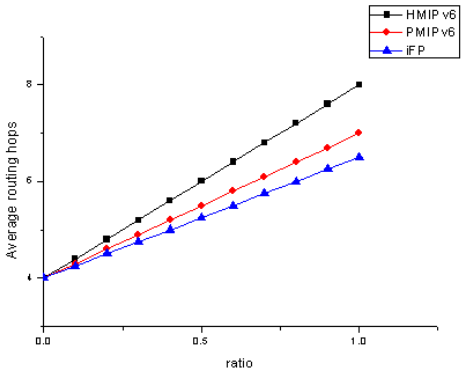

그림 9. 평균 라우팅 홉 수
Fig. 9. Average routing hops

그림 10은 핸드오버시 발생하는 유선과 무선 링크의 프로토콜 시그널링 비용의 합을 나타낸 결과이다. 핸드오버가 발생하는 MN의 증가에 따라 HMIPv6, PMIPv6, i-FP 세가지 기법 모두 시그널링 비용이 증가하지만 i-FP가 PMIPv6와 HMIPv6보다 더 낮은 비용과 속도로 증가하는 것을 확인할 수 있다. 또한 PMIPv6가 HMIPv6 보다 많은 시그널링 비용을 발생시켜 가장 높은 수치를 나타내고 있다.

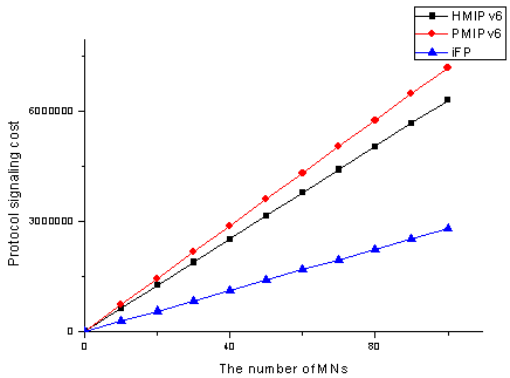

그림 10. 트래픽 시그널링 비용
Fig. 10. Traffic signaling cost

핸드오버 지연의 성능은 MN의 수에 따라 발생하는 총 비용을 측정하였다. MN이 하나의 네트워크에서 다른 네트워크로 이동할 때, MN이 트래픽을 받지 못하는 시간이 있다. 긴 핸드오버 지연은 핸드오버 절차에서 보다 많은 패킷 손실을 유발한다. 그러므로 MN에 의해 수신된 패킷의 손실 기간은 패킷을 수신할 때까지 전체 비용은 세 프로토콜의 핸드오버 지연을 측정하는데 사용된다. 그림 11에 보면 핸드오버하는 MN의 수에 따라 i-FP의 지연 비용이 가장 적고 PMIPv6, HMIPv6의 지연 시간이 상대적으로 크게 나온 것을 알 수 있다.

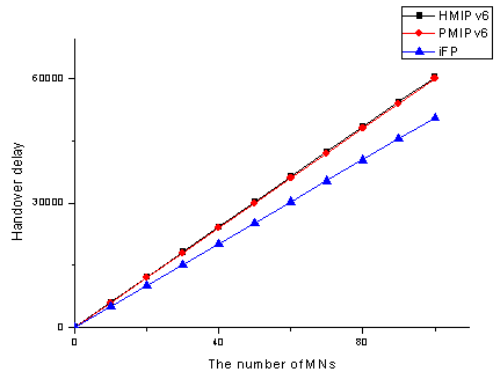

그림 11. 핸드오버 지연
Fig. 11. Handover delay

각각의 기법에 대해 트래픽 오버헤드의 총 비용을 측정하기 위해 핸드오버를 수행하는 MN의 수를 변수로 사용하여 평가를 실시하였다. 트래픽 오버헤드 평가의 결과로 i-FP는 IP 터널링을 하지 않고 IP 스와핑 메커니즘을 사용하기 때문에 핸드오버를 수행하는 MN의 수에 관계없이 유지되는 것을 볼 수 있으며, HMIPv6와 PMIPv6는 IP 터널링을 수행하기 때문에 핸드오버를 하는 MN이 증가함에 따라 오버헤드가 증가하는 것을 확인 할 수 있다. HMIPv6가 PMIPv6에 비해 MN의 수가 늘어남에 따라 비용이 급증하는 것을 볼 수 있다. 내용은 그림 12와 같다.

다양한 네트워크 환경의 총 비용을 보여주기 위해, 세션 도착 비율을 핸드오프 비율로 나눈 SMR(Session to Mobility Ratio)을 계산하였다. SMR이 크면, 세션 활동성이 핸드오프 비율보다 비교적 높다는 것을 의미한다. 그림 13, 14에서 iFP는 SMR의 증가에 따라 변동이 상대적으로 없고 다른 기법에 비해 가장 낮은 총 비용을 발생시키는 것을 확인할 수 있다.

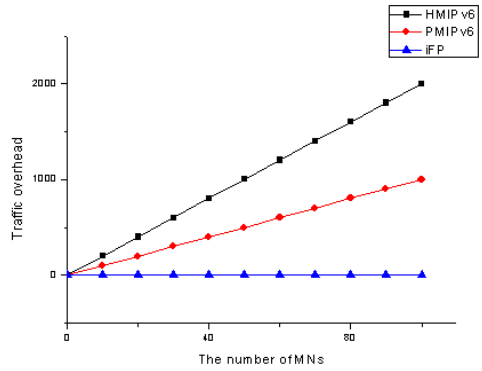

그림 12. 트래픽 오버헤드
Fig. 12. Traffic overhead

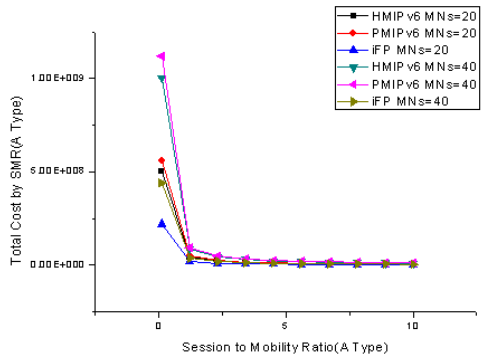

그림 13. SMR에 따른 총 비용 (A 타입)
Fig. 13. Total Cost by SMR (A Type)

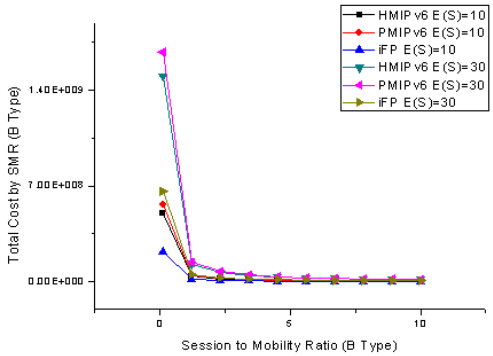

그림 14. SMR에 따른 총 비용 (B 타입)
Fig. 14. Total Cost by SMR (B Type)

V. 결 론

본 논문에서는 PMIPv6 네트워크기반의 i-FP라는 기존 기법의 단점을 개선한 기법을 제안했다. HMIPv6, PMIPv6, i-FP의 총 비용을 분석과 평가하여, i-FP가 인트라 도메인에서 다른 방법들과 비교하여 패킷 데이터 전송, 핸드오버, 시그널링 비용, 트래픽 오버헤드가 가장 낮은 우수한 비용 효율성을 가지는 기법이라는 것을 증명하였으며, 데이터 손실이 적고, 지연시간이 거의 없으며 도메인간의 핸드오버도 지원하는 모바일 네트워크 프로토콜 프레임워크라는 것을 확인했다. 기존의 기법들의 문제점을 개선하여 상대적으로 저비용으로 보다 높은 만족도를 가질 수 있으며, 이는 i-FP가 로컬 이동성 모바일 네트워크 환경에 가장 적합한 솔루션으로 판단할 수 있는 근거가 된다. 또한 추가적인 연구를 통해 고려되지 않았던 기존의 다른 기법들과의 성능 분석을 수행을 할 계획이다.

References

[1] S. Deering, R. Hinden, "*Internet Protocol, Version 6,*" NTWG RFC 2460, Dec. 1998.

[2] T. Narten, E. Nordmark, W. Simpson, and H. Soliman, "*Neighbor Discovery for IP version 6,*" NTWG RFC 4861, Sep. 2007.

[3] R. Moskowitz, P. Nikander, P. Jokela, and T. Henderson, "*Host identity protocol,*" IETF RFC 5201, Apr. 2008.

[4] H. Soliman, C. Castelluccia, K. ElMalki, and L. Bellier, "*Hierarchical mobile IPv6 (HMIPv6) mobility management,*" IETF RFC 5380, Oct. 2008.

[5] H. Yokota, K. Chowdhury and R. Koodli, "*Fast Handovers for Proxy Mobile IPv6,*" IETF RFC 5949, Sep. 2010.

[6] S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury, and B. Patil, "*Proxy mobile IPv6,*" IETF RFC 5213, Aug. 2008.

[7] T. Lim, C. Yeo, F. Lee, and Q. Le, "TMSP: terminal mobility support protocol," *IEEE Trans. Mobile Comput.*, vol. 8, no. 6, pp. 849-863, June 2009.

[8] A. Valko, "Cellular IP: a new approach to internet host mobility," *ACM SIGCOMM Comput. Commun. Review*, vol. 29, no. 1, pp. 50-65, Jan. 1999.

[9] R. Ramjee, K. Varadhan, L. Salgarelli, S. Thuel, S. Wang, and T. La Porta, "HAWAII: a domain-based approach for supporting mobility in wide-area wireless networks," *IEEE/ACM Trans. Netw.*, vol. 10, no. 3, pp.

396-410, June 2002.

[10] S. Das, A. Misra, and P. Agrawal, "TeleMIP: telecommunications enhanced mobile IP architecture for fast intradomain mobility," *IEEE Personal Commun. Mag.*, vol. 7, no. 4, pp. 50-58, Apr. 2000.

[11] D. Saha, A. Mukherjee, I. Misra, and M. Chakraborty, "Mobility support in IP: a survey of related protocols," *IEEE Network*, vol. 18, no. 6, pp. 34-40, June 2004.

[12] Y. Gvvon, J. Kempf, and A. Yegin, "Scalability and robustness analysis of mobile IPv6, fast mobile IPv6, hierarchical mobile IPv6, and hybrid IPv6 mobility protocols using a large-scale simulation," in *Proc. IEEE Int. Conf. Commun. (ICC'04)*, pp. 4087-4091, Paris, France, June 2004.

[13] X. Perez-Costa, M. Torrent-Moreno, and H. Hartenstein, "A performance comparison of mobile IPv6, hierarchical mobile IPv6, fast handovers for mobile IPv6 and their combination," *ACM SIGCOMM Comput. Commun. Review*, vol. 7, no. 4, pp. 5-19, Oct. 2003.

[14] G. Kim, "Low latency cross layer handover scheme in proxy mobile IPv6 domain," in *Proc. Next Generation Teletraffic Wired/Wireless Advanced Networking (NEW2AN 2008)*, pp. 110-121, St. Petersburg, Russia, Sep. 2008.

[15] J. Lei and X. Fu, "Evaluating the benefits of introducing PMIPv6 for localized mobility management," in *Proc. IEEE Int. Wireless Commun. Mobile Comput. Conf. (IWCMC'08)*, pp. 74-80, Crete Island, Greece, Aug. 2008.

[16] D. Johnson, C. Perkins, and J. Arkko, "*Mobility support in IPv6*," IETF RFC 3775, June 2004.

[17] R. Droms, J. Bound, B. Volz, T. Lemon, C. Perkins, and M. Carney, "*Dynamic host configuration protocol for ipv6 (DHCPv6)*," IETF RFC 3315, July 2003.

[18] T. Narten, E. Nordmark, W. Simpson, and H. Soliman, "*Neighbor discovery for IP version 6 (IPv6)*," IETF RFC 4861, Sep. 2007.

[19] S. Thomson, T. Narten, and T. Jinmei, "*IPv6 stateless address auto configuration*," IETF RFC 4862, Sep. 2007.

[20] J. Kempf, "*Problem statement for network-based localized mobility management (NETLMM)*," IETF RFC 4830, Apr. 2007.

[21] J. Kempf, "*Goals for network-based localized mobility management (NETLMM)*," IEFT RFC 4831, Apr. 2007.

[22] C. Vogt and J. Kempf, "*Security threats to network-based localized mobility management (NETLMM)*," IETF RFC 4832, Apr. 2007.

[23] D.-K. Oh and S.-W. Min, "A fast handover scheme of multicast traffics in PMIPv6," *KICS Inform. Mag.*, vol. 36, no. 3, pp. 208-213, Mar. 2011.

한 성 희 (Sunghee Han)

2010년 2월 중앙대학교 정보시스템학과 졸업

2012년 3월~현재 성균관대학교 정보통신대학원 석사과정

<관심분야> 모바일컴퓨팅, 네트워크 보안, IT 융합

정 종 필 (Jongpil Jeong)

2008년 2월 성균관대학교 정보통신대학(공학박사)

2009년 성균관대학교 컨버전스연구소 연구교수

2010년~현재 성균관대학교 산학협력단산학협력중점교수

<관심분야> 모바일 컴퓨팅, 센서 이동성, 차량 모바일 네트워크, 스마트기기 보안, 네트워크 보안, IT 융합, 인터랙션사이언스 등