동적 VPN 사이트 구성을 이용한 Provider Provisioned 기반 모바일 VPN

(Provider Provisioned based Mobile VPN using Dynamic VPN Site Configuration)

변 해 선 † 이 미 정 ††
(Haesun Byun) (Meejeong Lee)

요 약 모바일 기기의 다양화와 무선 기술의 발전으로 모바일 사용자가 증가함에 따라, 이들을 위한 효율적이고 안전한 VPN(Virtual Private Network) 접속 및 관리가 중요한 이슈가 되고 있다. 이에, 본 논문에서는 모바일 VPN 사용자가 서로 다른 사이트에 있는 하나 이상의 사용자와 효율적으로 통신할 수 있도록 하는 PE(Provider Edge) 기반 PP(Provider Provisioned) 모바일 VPN 메커니즘을 제안한다. 제안하는 방안은 모바일 VPN 사용자의 IPSec 터널 오버헤드를 최소화 했을 뿐만 아니라, 모바일 VPN 사용자의 위치에 관계없이 추가적인 IPSec 터널 오버헤드를 발생하지 않고 모바일 VPN 사용자 및 정적 VPN 사용자 간 최적화된 경로로 트래픽을 전달할 수 있도록 한다. 제안한 구조 및 프로토콜은 RFC2547에 제시된 "BGP/MPLS VPN" 기술을 기반으로 한다. 제안하는 방안에서는 모바일 VPN 사용자가 외부 네트워크로 이동했을 때, BGP/MPLS VPN 서비스를 모바일 VPN 사용자까지 확대하기 위해 서비스 제공자 측에 PNS(PPVPN Network Server)를 새로이 정의하였다. 제안하는 방안은 사용자 기반 모바일 VPN 및 CE 기반 모바일 VPN과 비교하여 IPSec 터널 관련한 오버헤드가 더 적으며, 시뮬레이션 결과, CE 기반 모바일 VPN 방안에 비하여 종단간 패킷 지연에 있어서 더 우수한 성능을 보임을 알 수 있었다.

키워드 : 모바일 IP, 가상사설망, IPSec 터널, 모바일 VPN, 이동성, PE 기반 VPN

Abstract Increase in the wireless mobile network users brings the issue of mobility management into the Virtual Private Network (VPN) services. We propose a provider edge (PE)-based provider provisioned mobile VPN mechanism, which enables efficient communication between a mobile VPN user and one or more correspondents located in different VPN sites. The proposed mechanism not only reduces the IPSec tunnel overhead at the mobile user node to the minimum, but also enables the traffic to be delivered through optimized paths among the (mobile) VPN users without incurring significant extra IPSec tunnel overhead regardless of the user's locations. The proposed architecture and protocols are based on the BGP/MPLS VPN technology that is defined in RFC2547. A service provider platform entity named PPVPN Network Server (PNS) is defined in order to extend the BGP/MPLS VPN service to the mobile users. Compared to the user- and CE-based mobile VPN mechanisms, the proposed mechanism requires less overhead with respect to the IPSec tunnel management. The simulation results also show that it outperforms the existing mobile VPN mechanisms with respect to the handoff latency and/or the end-to-end packet delay.

Key words : Mobile VPN, IPSec Tunnel, Mobile IP, PPVPN, Mobility, PE based VPN

1. 서 론

인터넷과 같은 공중망을 사용하여 가상의 사설망을 구축하는 VPN(Virtual Private Network) 서비스는 기업의 사설망 구축을 위한 비용절감 효과 면에서 매우 큰 주목을 받고 있지만, 관리의 복잡성 및 보안을 위한 추가적 오버헤드가 VPN을 구성하는데 걸림돌로 작용해 왔다. 이에, 서비스 제공자들이 기업의 네트워크 관리자

· 본 논문은 정보통신연구진흥원의 대학 IT연구센터(ITRC) 육성사업 (ITAC1090060300350001000100100)의 지원에 의해 수행되었음
† 학생회원 : 이화여자대학교 컴퓨터학과
ladybhs@ewhain.net
†† 정 회 원 : 이화여자대학교 컴퓨터학과 교수
lmj@ewha.ac.kr
논문접수 : 2006년 10월 4일
심사완료 : 2006년 11월 26일

를 대신하여 VPN 설립부터 관리까지 모든 책임을 갖는 PPVPN(Provider Provisioned VPN)이 주목 받고 있다. PPVPN은 현재 IETF(Internet Engineering Task Force) L2VPN(Layer 2 VPN)과 L3VPN(Layer 3 VPN) WG(Working Group)에서 활발한 표준화 활동이 진행 중이다. 그 중, L3VPN WG에서 진행 중인 3 계층에서의 VPN 기술로는 BGP/MPLS VPN, Virtual Router 방안, CE 기반 IPSec 방안이 있다[1]. BGP/MPLS VPN과 Virtual Router 방안은 VPN 사이트를 서비스하는 CE(Customer Edge)와 서비스 제공자 네트워크의 PE(Provider Edge)를 접속 회선(Attachment Circuit)으로 연결하고, PE가 VPN 설립에 관련된 작업을 BGP/MPLS나 Virtual Router 매커니즘을 이용하여 수행하도록 하는 방안이다. 특히, BGP/MPLS VPN은 MPLS 네트워크를 기반으로 3계층 VPN 서비스를 제공함으로써 VPN 수요를 확대시키는 대표적 기술이 되고 있으며, 현재 다수의 서비스 제공자들이 MPLS 기반의 VPN 서비스를 제공하거나 고려하고 있는 추세이다.

CE 기반 IPSec 방안은 GW 기능을 가지고 있는 CE와 CE간 IPSec 터널을 설립함으로써 VPN 데이타의 안전한 통신을 보장하고, CE가 VPN 설립에 관련된 작업을 수행하도록 하는 방안이다. 그러나 CE 기반 VPN은 많은 수의 사이트를 갖는 VPN의 경우 터널의 수가 크게 증가하며, 새로운 사이트를 추가하거나 제거하는 경우 각 사이트의 정보를 수정하여야 하므로 확장성 문제가 있다. BGP/MPLS VPN이나 Virtual Router를 이용한 VPN 서비스나 CE 기반 IPSec VPN 서비스는 공통적으로 주로 사이트-대-사이트 VPN을 구성하기 위해 사용된다.

한편, 호텔, 공항 등의 공공장소에 무선 LAN의 설치가 증가하고, 모바일 기기의 다양화와 무선 기술의 발전으로 모바일 사용자의 이동성 지원에 대한 요구가 증가함에 따라, 기존의 VPN 서비스는 모바일 사용자가 지역적 제한 없이 VPN 서비스를 제공받을 수 있는 모바일 VPN 서비스로 확대될 필요가 있다. 지금까지 제안된 모바일 VPN 서비스에 대한 연구로는 외부 네트워크로 이동한 MN(Mobile Node)이 안전한 통신을 목적으로 홈 네트워크의 VPN GW와 IPSec 터널을 설립하고, 이동성을 보장받기 위해 HA(Home Agent)에게 이동 사실을 등록하여 MIP(Mobile IP) 터널을 설립하는 형태의 방안들이 주를 이루고 있다[2]. 그런데, 이러한 모바일 VPN 서비스 구조는 외부 네트워크에 있는 MN이 홈 사이트에 있는 CN(Correspondent Node)과 통신하는 경우에 대한 서비스를 제공하는 데는 효율적이나, 사이트-대-사이트 VPN 구조에서 각각 다른 사이트에 있는 하나 이상의 CN과 동시에 통신하는 경우에는 매우 비효율적일 수 있다.

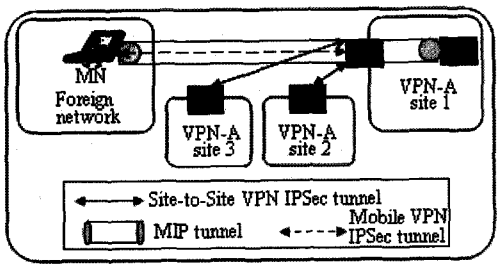


그림 1 VPN 서비스 제공 구조

그림 1은 IPSec 터널로 연결된 CE 기반 IPSec VPN과 모바일 VPN이 함께 구성되어 있는 VPN 구조의 예를 보인 것이다. CE 기반 VPN을 구성하기 위해 VPN A에 속하는 사이트 1,2,3의 GW들이 IPSec 터널로 연결되어 있다. 그리고 사이트 1을 홈 네트워크로 사용하는 사용자가 외부 네트워크에 나가게 되면 이 사용자는 자신의 홈 네트워크인 사이트 1의 GW와 IPSec 터널을 설립하고 HA와 MIP 터널을 설립하여 통신한다[2]. 이 경우 MN이 동일한 VPN의 다른 사이트에 있는 CN과 통신하기 위해서는 데이타가 항상 MN의 홈 네트워크를 우회하여 전달되어야 한다.

이와 같은 문제에 대해 루트 최적화(Route Optimization: RO)를 수행하기 위해서는, MN은 CN이 있는 네트워크의 GW와 IPSec 터널을 별도로 설립해야 한다. 만약, 비디오 회의와 같은 응용서비스를 사용하기 위하여 MN이 사이트 2와 3에 있는 CN와 동시에 통신하기를 원한다면 CN이 있는 각 네트워크의 CE와 IPSec 터널을 설립해야 할 것이다. 즉, MN이 다수의 사이트내의 CN과 통신하는 경우 CE 기반 VPN의 IPSec 터널 설립에 관련된 오버헤드가 더 확대되며, IPSec 터널 설립을 위한 시그널링 오버헤드로 무선 네트워크 자원의 낭비를 가져올 수 있다. 또한, MN에서 VPN 접속을 수행하고 IPSec 터널을 설립, 유지·관리하기 때문에 터널 관리에 대한 사용자 측에서의 복잡성이 증가한다.

이와 같은 터널 관리의 복잡성 및 보안 문제를 해결하기 위한 추가적 오버헤드를 줄이기 위해 Barcelo et al은 CE 기반 모바일 VPN을 제공하는 PPVPN 방안을 제안하였다[3]. [3] 방안은 CE 기반 IPSec 방안을 모바일 VPN 서비스에도 적용하기 위해 확장한 것으로 서비스 프로비저닝 플랫폼(Service Provisioning Platform)의 네트워크 서버를 통해 MN의 MIP 등록요청 메시지를 HA에게 전달하며, SPS의 네트워크 서버가 MN이 이동한 외부 네트워크의 GW와 홈 네트워크의 VPN GW간 IPSec 터널 설립을 프로비전 한다. 이 방안은 IPSec 터널 설립에 관련된 무선 네트워크에서의 자원

낭비 및 MN에서의 터널 설립 및 유지에 관련된 복잡성은 해결하였으나, 패킷이 항상 홈 네트워크를 통해서 전달되므로 종단간 패킷 지연 문제는 여전히 남게 된다. 이 방안에 루트 최적화를 적용하기 위해서는 MN이 홈 사이트 이외의 사이트에 있는 CN과 통신을 원하는 경우 외부 네트워크의 GW가 CN이 있는 네트워크의 GW와 IPSec 터널을 별도로 설립해야 한다.

이에, 본 논문에서는 PPVPN에서 PE 기반 모바일 VPN 서비스를 제공하기 위한 네트워크 구조 및 이동성 지원 프로토콜을 제안하여 IPSec 터널 오버헤드 및 데이타 전달 경로 우회 문제를 동시에 해결하고자 한다. 제안하는 방안은 RFC2547에 제시된 BGP/MPLS VPN 방식을 기반으로 한다. 제안하는 방안에서는 BGP/MPLS VPN 서비스를 제공받고 있는 모바일 사용자의 VPN 접속 및 이동성 유지·관리를 위해 서비스 제공자 측에 PNS(PPVPN Network Server)를 새로이 정의하였다. PNS는 외부 네트워크로 이동한 MN의 이동성을 지원하기 위해 MN과 VPN에 대한 바인딩 정보를 유지한다. 또한 MN이 이동한 외부 네트워크의 GW와 서비스 제공자 네트워크에서 선택된 하나의 PE간 IPSec 터널을 설립하도록 지시하며, 그 PE에게 MN의 VPN 접속에 필요한 정보를 전달하여 해당 PE가 BGP/MPLS VPN 동작에 참여할 수 있도록 한다. [3] 방안에서 MN과 CN간의 데이타 전송이 항상 홈 네트워크를 통해서 전달되어 종단간 패킷 지연이 길어졌던 것과는 달리, 이 방안에서는 MN이 속한 VPN을 서비스하는 PE들이 MN의 이동사실을 알고 있기 때문에 홈 네트워크를 경유하지 않고 MN이 있는 외부 네트워크로 패킷을 전달함으로써 종단간 패킷 지연을 줄일 수 있다. 또한, [3] 방안에서 루트 최적화를 적용하기 위해서는 MN이 이동한 외부 네트워크의 GW와 CN이 있는 각 사이트의 CE간에도 IPSec 터널을 별도로 설립해야 했던 것과는 달리, 제안하는 방안에서 외부 네트워크의 GW는 항상 하나의 PE와만 IPSec 터널을 설립하면 되기 때문에 외부 네트워크의 GW가 유지해야 하는 터널의 수 및 IPSec 터널 설립을 위한 시그널링 오버헤드를 줄일 수 있다.

본 논문의 구성은 다음과 같다. 1장의 서론에 이어, 2장에서는 관련연구로 PPVPN에서의 3계층 CE 기반 VPN과 PE 기반 VPN에 대해 각각 설명하고, 이들이 모바일 VPN 서비스를 제공하기 요구사항을 살펴본다. 3장에서는 PPVPN에서 PE 기반 모바일 VPN 서비스를 제공하기 위해 본 논문에서 제안하는 네트워크 구조와 MN의 이동성을 지원하기 위한 프로토콜에 대하여 자세히 설명하고, 4장에서는 각 모바일 VPN 서비스 제공 형태에 따라 MN의 이동성을 지원할 때 발생하는 오버헤드를 비교한다. 5장에서는 제안하는 방안의 효율성을 살펴보기 위한 시뮬레이션 결과를 제시하고, 마지막으로 6장에서는 이 논문의 결론을 맺는다.

2. 관련연구

2.1 PPVPN에서 3계층 CE 기반 VPN

CE 기반 IPSec VPN은 PPVPN 구조 가운데 3계층 CE 기반 VPN으로 분류할 수 있다[1]. 이 기술은 서비스 제공자의 제어를 통해 구성되는 CE 기반 VPN의 형태로서, VPN 고객은 서비스 제공자에게 VPN 구성에 참여하는 CE의 집합과 VPN 토폴로지 정보를 알려줘야 한다. 서비스 제공자는 이 정보를 기반으로 VPN 데이타베이스를 구성하고, 그 VPN을 관리하고 프로비전한다. 동일한 VPN에 속하는 VPN 사이트들은 CE와 CE 간 설립된 IPSec 터널을 통하여 라우팅 정보와 VPN 트래픽을 교환한다.

PPVPN에서 3계층 CE 기반 VPN에서 모바일 VPN 서비스를 제공하려면, MN을 서비스하는 외부 네트워크의 FA가 CE와 같은 역할을 담당하여 VPN 구성에 참여하고, MN이 속한 VPN의 다른 CE들과 IPSec 터널을 설립해야 한다. 이를 위해, FA는 라우팅 및 IPSec 터널 종단점 기능을 제공할 수 있는 장비여야 하는데, GPRS 네트워크에서의 GGSN, CDMA 네트워크에서 PDSN, 파이어월 기능을 가지고 있는 GW는 FA 기능까지 수행하는 일반적인 혼합형 장비이다.

FA가 임의의 VPN에 새로운 CE와 같이 추가되었을 때, 서비스 제공자는 VPN 설립에 필요한 모든 정보 즉, VPN 구성에 참여하는 CE의 집합, VPN 토폴로지 정보, IPSec 터널 설립에 필요한 인증, 암호화 정보 등을 FA상에 설정해야 하며, FA는 이 정보를 기반으로 동일한 VPN에 속하는 CE들과 IPSec 터널을 설립하여 라우팅 정보 및 VPN 트래픽을 교환한다.

Barcelo et al은 3계층 CE 기반 VPN에 모바일 VPN 서비스를 결합시키는 방안을 제안하였다[3]. 그림 2는 [3]에서 제안한 모바일 VPN을 서비스하는 구조를 나타낸 것이다. 이 방안에서는 MN을 서비스하는 FA가 MN으로부터 MIP 등록요청 메시지를 받으면 FA는 이

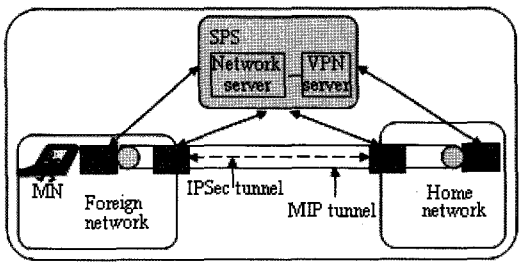


그림 2 Internode 방안에서의 모바일 PPVPN

메시지를 SPS(Service Provisioning Support) 플랫폼의 네트워크 서버에게 전달한다. 네트워크 서버는 HA, FA, GW에서 요청한 작업을 수행하는 네트워크 관리 서버이다. 네트워크 서버는 FA로부터 받은 MIP 등록요청 메시지를 VPN 서버에게 전달한다. VPN 서버는 VPN 서비스를 제공하기 위해 필요한 모든 사용자 정보 및 서비스 정보를 유지하고 있으며, SLA를 기반으로 VPN 서비스를 제공하는 서버이다. VPN 서버는 MIP 등록요청 메시지를 받으면 VPN 서비스를 요청한 MN의 프로파일을 기반으로 MN을 인증한다. 또한, IPSec 터널을 설립할 GW 쌍의 정보를 네트워크 서버에게 요청한다. 네트워크 서버로부터 GW 쌍의 정보를 받으면, 두 GW에게 IPSec 터널을 설립하도록 지시한다. 이때, GW 쌍의 정보는 MN이 이동한 외부 네트워크의 GW와 MN의 홈 네트워크에 있는 GW의 주소이다.

한편, VPN 서버는 MIP 등록요청 메시지를 HA에게 전달한다. HA는 MIP 등록요청 메시지의 응답으로 MIP 등록응답 메시지를 만들어 SPS를 통하여 FA에게 전달하고, FA는 이를 MN에게 전달한다. 즉, [3] 방안에서는 서비스 제공자가 MN의 VPN 접속을 위해 GW 간 IPSec 터널 설립을 지시하고 VPN 접속을 프로비전하나, MN의 이동성을 제공하는 HA가 기존의 MIP 인프라구조에서와 같이 MN의 MIP 등록요청 및 등록응답을 수행한다. 또한, 사이트-대-사이트 CE 기반 IPSec 방안에서 터널 종단점인 CE간 VPN 트래픽 및 VPN 사이트 내의 라우팅 정보를 교환하는 것과는 달리, GW 간 VPN 사이트 내의 라우팅 정보를 교환하지는 않고 오직 VPN 트래픽만 전달한다. 즉, 외부 네트워크의 GW는 VPN 사이트 내의 네트워크 토폴로지나 경로 정보는 알지 못하고, GW의 주소를 목적지로 하여 일반적인 라우팅에 의해 패킷을 전달한다.

2.2 PPVPN에서 3계층 PE 기반 VPN

PPVPN에서 3계층 PE 기반 VPN 서비스를 지원하는 대표적인 기술은 BGP/MPLS와 Virtual Router가 있다[1]. PE 기반 VPN 서비스에서는 고객 사이트의 CE와 서비스 제공자 네트워크의 PE간 접속회선을 통해 연결된다. 접속회선으로는 ATM VC, 프레임 릴레이 VC, 이더넷 인터페이스, 이더넷 인터페이스에서의 VLAN, GRE 터널, L2TP 터널, IPSec 터널 등이 사용된다. 즉, 접속회선은 VPN 사이트와 서비스 제공자 네트워크 쌍방이 모두 지원 가능한 터널의 일종이거나, 데이타 링크 계층에서의 커넥션의 일종이다[1].

BGP/MPLS VPN은 VPN 라우팅 정보를 분배하기 위해 서비스 제공자 네트워크의 PE 간에 MP(Multi Porotocol)-BGP를 사용하고, VPN 트래픽 전송을 위하여 MPLS 기술을 사용하는 모델이다. 그림 3은 BGP/MPLS VPN 모델의 구조를 보여주고 있다. VPN 고객 사이트에 위치하고 있는 CE들은 접속회선(attachment circuit)을 통하여 PE와 연결되어 있고, PE는 CE와 연결한 접속회선 별로 별도의 VRF(Virtual Routing and Forwarding) 테이블을 유지한다. 따라서 CE로부터 들어오는 VPN 트래픽은 해당 인터페이스와 매핑된 VRF 테이블만 참조하게 되므로 VRF는 각 VPN 트래픽을 분리하는 역할을 하게 된다.

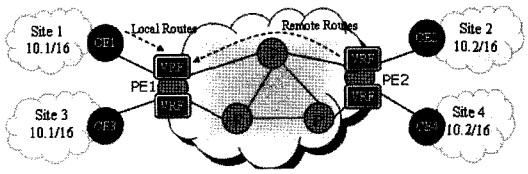


그림 3 BGP/MPLS VPN

BGP/MPLS VPN에서 PE들은 라우팅 정보를 분배하기 위해 BGP를 확장한 MP-BGP 프로토콜을 사용한다. 이때 PE가 MP-BGP 프로토콜을 통해 전달하는 정보로는 VPN-IPv4 주소와 RT(Rout Target) 정보, 레이블 정보이다. VPN-IPv4 주소는 4바이트 IP 주소 앞에 8바이트 RD(Route Distinguisher) 필드를 붙여서 만들어지는 사설망을 위한 주소이다. RD는 동일한 IP 주소 프리픽스를 사용하는 VPN 사용자들 간에 경로를 구분하기 위해 별도의 식별자로 사용된다. RT는 VPN을 구별하기 위해 각각의 VRF에 할당된 정보로서 즉, BGP 라우팅 정보를 수신한 PE가 VRF 테이블에 이 정보를 적용시킬 것인지를 판단할 수 있게 하는 기준이 된다. BGP/MPLS VPN에서 트래픽 전달은 두 개의 레이블 스택을 이용한다. 그 중 하나는 VPN 사이트를 구별하기 위한 VPN 레이블이며, 나머지 하나는 LSP를 위한 MPLS 레이블이다.

BGP/MPLS의 동작 과정은 다음과 같다. 그림 3에서 CE1은 PE1에게 VPN 사이트 1의 IP 주소 프리픽스를 알려준다. PE1은 고객 사이트 1의 프리픽스 정보, CE1로의 인터페이스 번호, VPN 사이트 1를 위해 할당된 MPLS 레이블을 VRF 테이블에 저장한다. 그런 후에, VPN-IPv4 주소를 만들고, 이 주소와 함께 레이블 정보, RT 정보를 MP-BGP 프로토콜을 통하여 모든 PE들에게 전달한다. PE2는 이 메시지를 받으면 RT 정보를 참고하여 동일한 VPN에 속하면 해당 VRF 테이블에 CE1의 프리픽스, 레이블, PE1의 주소를 저장한 후, CE2에게 CE1의 프리픽스 정보를 전달해준다. BGP/MPLS VPN에서의 VPN 트래픽 전달은 PE들 간 설정되어 있는 LSP를 통하여 이루어진다. PE들간 최선 서비스(Best-effort 서비스) 정도만 보장하면 되는 경우,

LSP는 LDP등을 이용하여 설정되며, QoS 보장이나 특정 트래픽 엔지니어링이 요구되는 경우, RSVP 프로토콜을 이용하여 LSP를 설정할 수 있다.

3계층 PPVPN에서 BGP/MPLS VPN을 모바일 VPN과 결합할 경우, MN이 이동한 외부 네트워크의 FA와 PE간 접속회선이 필요하다. 그러나, MN이 이동하는 특성을 가지고 있기 때문에 MN을 서비스하는 FA가 항상 PE와 접속회선을 설립하게 하는 것은 현실적이지 못하다. 따라서, 모바일 VPN 서비스를 지원하기 위해 적합한 접속회선은 데이타 링크 계층에서의 커넥션의 일종으로 설립하기 보다 두 네트워크 계층 쌍방이 모두 사용 가능한 터널의 일종으로 구성하는 것이 적합하다. FA와 접속회선을 설립한 PE는 VPN 구성에 참여해야 하며, 서비스 제공자는 이를 위하여 VPN 구성에 필요한 RT, RD정보 등을 PE에 설정해야 한다. PE는 이 정보를 기반으로 동일한 VPN에 속하는 PE들과 라우팅 정보 및 VPN 트래픽을 교환한다.

Ravi Bhagavathula et al은 BGP/MPLS VPN 기술을 모바일 VPN에 적용하는 방안을 제안하였다[4]. 이 방안은 모바일 네트워크가 외부 네트워크로 이동하는 환경에서 MR이 GW와 같이 동작할 때 BGP/MPLS 기술을 이용하여 모바일 네트워크의 이동성을 지원하는 방안이다. 이 방안에서는 HA와 FA를 PE와 같이 고려하는 경우와 MR을 PE와 같이 고려하는 경우를 제시하였다. HA와 FA를 PE와 같이 고려하는 경우, MR은 FA에 단지 접속만 하면 되고, FA와 HA간 BGP/MPLS 기능을 수행하여 MR의 멤버쉽정보 및 라우팅 정보를 교환하므로, MR과 HA간 터널이 필요하지 않다. 그러나 이와 같은 경우, HA는 PE와 같이 동작해야 하므로 외부 네트워크에서 접근 가능해야 하며, HA가 PE와 같이 VRF 테이블, BGP 라우팅, MPLS 레이블 교환에 참가해야 한다. 또한 FA가 PE와 같이 동작하기 위해 동일한 VPN에 속하는 사이트들의 루트 정보와 VPN-ID, VPN 토폴로지 등의 VPN 정보가 FA에 설정되어야 한다.

MR을 PE와 같이 고려하는 경우는 HA와 FA를 PE와 같이 고려하는 경우보다 더 확장성이 뛰어나다. 왜냐하면, HA와 FA를 PE와 같이 사용하는 방안에서 MR이 이동할 때마다 이동한 외부 네트워크의 FA에 VPN 구성 정보를 설정해야 하는 것과는 달리, MR은 VPN 정보 및 VPN에 속하는 사이트들의 루트 정보를 이미 가지고 있기 때문에 새로운 외부 네트워크로 이동할 지라도 추가적으로 구성정보를 설정해야 할 필요가 없기 때문이다. 그러나, 이 방안에서는 MR이 BGP/MPLS에 참가해야 하므로 MR이 백본 네트워크의 MPLS 노드들과 레이블 교환을 수행해야 하며, MR과 PE들간 BGP 프로토콜이 동작해야 한다. 또한, MR이 모든 MPLS 노드들 간 레이블 교환이 끝날 때까지 MR은 PE로 동작하지 못하므로 VPN 설립하는데 지연이 발생할 수 있다.

3. PPVPN에서 PE 기반 모바일 VPN 서비스 제공 방안

본 장에서는 PPVPN에서 BGP/MPLS 기반 모바일 VPN 서비스를 지원하기 위한 네트워크 구조 및 MN의 이동성을 지원하는 방안에 대해 설명한다. 먼저, PPVPN에서 BGP/MPLS 기반 모바일 VPN 서비스를 지원하기 위한 네트워크 구조 및 구성요소를 설명하고, MN의 VPN 접속 및 서비스 제공자의 VPN 설정 과정과 VPN 트래픽 전송 과정에 대하여 자세히 설명한다.

3.1 PPVPN에서 PE 기반 모바일 VPN을 지원하는 네트워크 구조 및 개체

그림 4는 제안하는 BGP/MPLS 기반 모바일 VPN 서비스를 지원하기 위한 네트워크 구조 및 터널 형태를 보인 것이다. 제안하는 방안에서는 외부 네트워크의 GW가 VPN 사이트를 서비스하는 CE처럼 동작한다. 본 논문에서는 홈 네트워크의 CE와 구분하기 위해 외부 네트워크의 GW를 FCE(Foreign Customer Edge)라고 부른다. 제안하는 구조에서 외부 네트워크는 동적인 VPN 사이트로 볼 수 있으며, 임의의 FCE가 서비스하는 외부 네트워크에 들어와 있는 동일한 VPN에 속하는 MN들은 하나의 동일한 VPN 사이트 내에 존재하는 VPN 사용자들처럼 서비스 된다. 정적인 VPN 사이트와

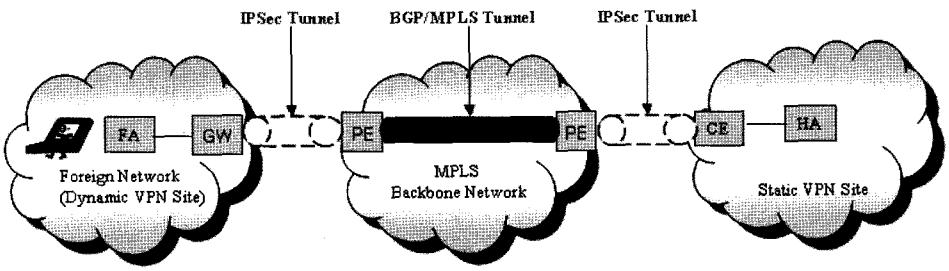


그림 4 BGP/MPLS 기반 모바일 VPN을 지원하는 네트워크에서의 터널 형태

서비스 제공자 네트워크를 연결하는 CE와 PE 구간에는 접속회선에서의 보안을 위하여 IPSec 터널을 이용한다. CE와 PE간 IPSec 터널 이용 방안은 IETF의 L3VPN WG에 의해 표준화가 진행되고 있다[5]. 제안하는 방안에서는 외부 네트워크와 서비스 제공자 네트워크를 연결하는 FCE와 PE 구간의 링크에서도 보안 제공을 목적으로 IPSec 터널을 사용한다. 서비스 제공자 네트워크인 PE와 PE 구간에는 RFC2547에 제시된 BGP/MPLS VPN을 구축한다. 따라서, PE와 PE간 VPN 연결성(Connectivity)를 구축하기 위해 BGP 터널을 사용하고, VPN 사이트간 VPN 트래픽을 전달하기 위해 MPLS 터널을 사용한다. 서비스 제공자 네트워크 구간에서의 보안은 BGP/MPLS VPN이 VPN 별로 VRF 테이블을 구성하기 때문에 VPN 별로 트래픽을 분리할 수 있다는 점에 의존한다.

그림 5는 제안하는 방안에서 MN의 이동성을 지원하는 서비스 구조를 보인 것이다. 제안하는 BGP/MPLS 기반 모바일 VPN 서비스는 서비스 제공자 측의 네트워크 상에 PNS(Provider Network Server) 개체를 새로이 정의하였다. PNS는 네트워크 차원에서 VPN 프로비저닝과 MN의 이동성 지원을 제공한다. 즉, 홈 사이트에 있던 MN이 외부 네트워크로 이동했을 때, PNS는 외부 네트워크의 FCE와 PE간 접속회선으로 IPSec 터널을 설립하도록 지시하고, 그 PE에게 VPN 토폴로지, RT, RD 등의 VPN 설립정보를 제공하여 BGP/MPLS VPN 서비스를 시작하도록 한다.

외부 네트워크의 AAAF(Accounting, Authorization, Authentication Foreign)와 서비스 제공자 네트워크의 AAAP(AAA Provider)는 MN의 인증 및 VPN 서비스 인증을 위해 서로 통신하는 개체이다. UPS(User Profile Server)는 서비스 측면에서의 사용자 프로파일 정보를 유지하고 있는 개체이다. AAAP는 UPS에게 사용자의 프로파일을 요청하고, UPS로부터 받은 정보를 기반으로 MN에게 VPN 서비스를 제공할 것인지를 결정하여 그 결과를 AAAF에게 전달한다.

3.2 Mobile BGP/MPLS VPN 설립 및 접속

그림 6은 외부 네트워크로 이동한 MN이 VPN 접속을 획득하기 위한 MN의 등록과정을 보여준다. 제안하는 방안에서는 MN의 등록과 인증을 위해 Diameter MIPv4 프로토콜[6]의 사용을 가정한다. Diameter MIPv4 프로토콜은 MN의 인증, 권한 부여, 과금 등의 서비스를 제공하기 위한 프로토콜로 IETF AAA WG에 의해 표준화가 완료되었다.

외부 네트워크로 이동한 MN은 자신의 이동 사실을 알리기 위해 MIP 등록요청(Registration Request) 메시지 만든다. 그림 7은 MN이 만든 등록요청 메시지의 구조를 보여주고 있다. MIP 등록요청 메시지의 HA 필드에는 PNS Address를 기입한다. PNS는 MN의 이동성을 지원하고, VPN 접속을 승인하기 위해 서비스 제공자 측에 있는 네트워크 서버이다. MN은 MIPv4에서 HA 주소를 미리 알고 있듯이, PNS 주소를 미리 알고 있다고 가정한다. 제안하는 방안에서는 IPSec 터널을 설립할 FCE 주소를 PNS에게 알리기 위해 MIP 등록요청 메시지에 MN을 서비스하는 외부 네트워크의 GW 즉, FCE의 주소를 명시하는 FCE Address 필드를 새로이 추가하였다. FCE 주소는 MN이 CoA를 할당 받을 때 즉, 에이전트 광고(Agent Advertisement) 메시지를 받았을 때 획득한다고 가정한다.

MN은 서비스 제공자 네트워크의 AAA 서버인 AAAP에게 MIP 등록 인증을 얻기 위해 Diameter MIPv4 프로토콜에서와 같이 MIP 등록요청 메시지에 *Challenge and MN-AAA authentication extension*을 포함한다. *Challenge and MN-AAA authentication extension*는 MIP 등록요청의 재전송방지(replay protection)에 대한 제어 및 MN의 인증을 위해 필요한 정보이다. MN은 또한 MIP 등록요청 메시지에 Home AAA server NAI 대신에 Provider AAA server NAI를 포함하여 AAAP가 MN을 인증할 수 있도록 한다.

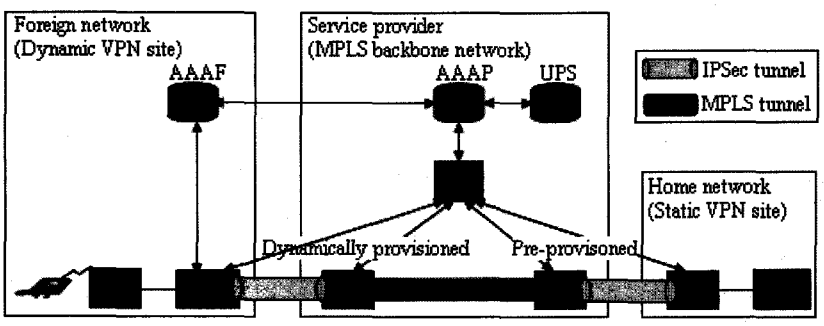


그림 5 BGP/MPLS 기반 VPN에서 MN의 이동성을 지원하는 서비스 구조

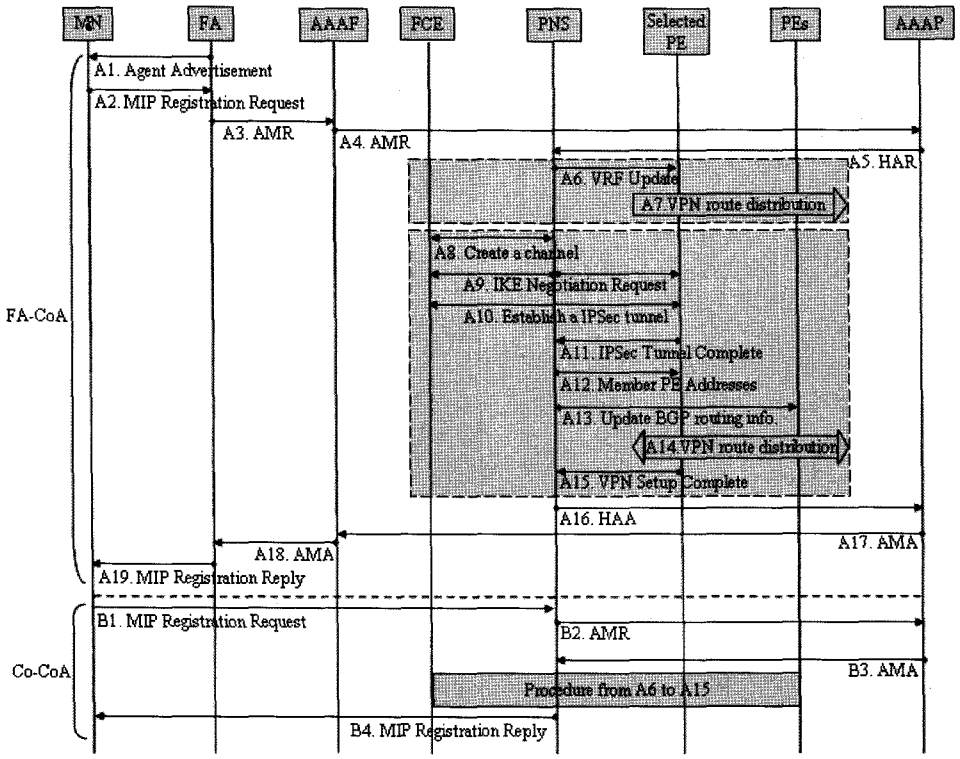


그림 6 BGP/MPLS 기반 모바일 VPN에서의 MN의 등록과정

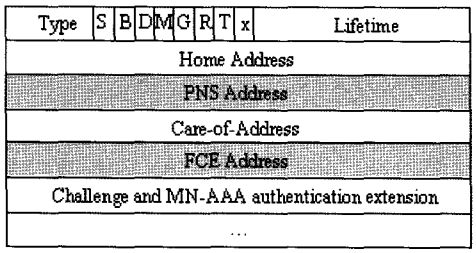


그림 7 수정된 등록요청 메시지 구조

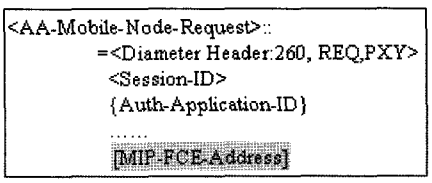


그림 8 수정된 AMR 메시지

Diameter MIPv4에서 사용하는 CoA(Care-of-Address)에는 FA-CoA와 Co-CoA가 있다. FA-CoA는 MN이 방문한 외부 네트워크 내에서의 FA 주소이며, Co-CoA는 DHCP 등을 통해서 MN이 직접 할당받은 주소이다. MN이 FA-CoA 기반으로 동작하는 경우, MN은 MIP 등록요청 메시지를 FA에게 보낸다(그림 6의 A2). FA는 MIP 등록요청 메시지를 받으면 그 메시지에 들어있는 정보를 기반으로 하여 AMR(AA-Mobile-Node-Request) 메시지를 만들고, AMR 메시지를 AAAF에게 보낸다(그림 6의 A3). AMR 메시지는 Diameter MIPv4 프로토콜에서 MN의 인증과 접근권한을 요구하기 위한 메시지이다. 제안하는 방안에서는 MN이 보낸 MIP 등록요청 메시지의 FCE 주소를 PNS에게 전달하기 위해 AMR 메시지에도 *MIP-FCE-Address*를 새로이 추가하였다. 그림 8은 수정된 AMR 메시지를 보여준다.

AMR 메시지를 받은 AAAF는 AMR 메시지를 또 다른 Diameter 서버에게 전달할 것인지, 자신이 처리해야 하는 것인지를 결정하기 위해 목적지 AAA 서버의 NAI를 검사한다[7]. 제안하는 방안에서 AMR 메시지는 AAAF에 의해 최종적으로 서비스 제공자 네트워크의 AAAP에게 전달된다(그림 6의 A4). AAAP는 AMR 메시지의 *MN-AAA authentication extension*을 보고 MN-AAA security association[8]을 사용하여 MN의 등록요청 메시지를 인증한다. 인증이 승인되면, AAAP는 PNS에게 MN의 등록을 요청하기 위해 HAR(Home-Agent-MIP-Request) 메시지를 보낸다(그림 6의 A5). PNS는 HAR 메시지를 받으면, MN의 VPN 접속 및

이동성 지원을 위한 절차를 시작한다.

한편, MN이 Co-CoA 모드로 동작하는 경우, MN은 MIP 등록요청 메시지를 PNS에게 직접 보낸다(그림 6의 B1). PNS는 MIP 등록요청 메시지를 받으면, *MIP-Feature-Vector AVP*에 *Co-Located-Mobile-Node* 비트를 설정한 AMR 메시지를 만든 후, 이 메시지를 AAAP에게 보낸다(그림 6의 B2). AAAP는 AMR 메시지를 받으면 MN을 인증 한 후, 이에 대한 응답으로 AMA 메시지를 만들어 PNS에게 보낸다(그림 6의 B3). PNS는 AMA 메시지를 받으면 MN의 VPN 접속 및 이동성 지원을 위한 절차를 시작한다.

PNS는 MN에 대한 이동성 및 보안을 포함한 VPN 정보를 관리하기 위하여 VST(VPN Service Tunnel) 테이블을 유지한다. 그림 9는 PNS에서 유지하고 있는 VST 테이블의 구조를 나타낸다. VST 테이블에는 VPN 그룹별로 이동한 MN의 HoA, CoA, FCE, PE의 바인딩 정보를 유지하는 *MN-to-FCE 바인딩 리스트* (*MN_to_FCE_Binding list*), PE와 FCE 혹은 CE 간 보안 정보를 유지하는 *PE_FCE/CE 보안 리스트* (*PE_FCE/CE_Security list*), PNS가 FCE 혹은 CE 간 필요한 상호 인증, 관리 데이타를 암호화 하기 위한 암호화 정보를 포함하고 있는 *PNS_FCE/CE 보안 리스트*(*PNS_FCE.CE_Security list*), VPN 구성에 필요한 RT과 RD 정보를 유지하는 *RT/RD 정책* (*RT/RD_policy*), 풀 메시, 메시 또는 성형 등의 VPN 구성형태별로 해당 토폴로지 정보를 유지하는 *VPN 토폴로지* (*Topology*) 등이 있다. 각 VPN에 대해 고정적으로 할당되어 있는 *RT/RD_policy*를 제외하고, 나머지 앤트리들은 MN이 자신의 위치를 변경하여 새로운 FCE에 접촉하여 등록을 요청하여 등록과정을 수행하는 중에 변경된다.

MN의 VPN 접속 및 이동성 지원을 위한 절차는 다음과 같다. 먼저, PNS는 AAAP로부터 HAR 메시지를 받거나(FA-CoA 모드인 경우), AMA 메시지를 받으면(Co-CoA 모드인 경우), MN의 VPN 접속 요청을 처리하기 위해 MN을 서비스할 적합한 PE를 선택해야 한다. PNS가 PE를 선택하는 방법은 정적 PE 선택 방법과 동적 PE 선택 방법으로 나뉠 수 있다. 정적 PE 선택 방법은 서비스 제공자 네트워크에 미리 지정해 둔 PE가 MN을 위한 VPN 서비스를 수행하는 것이다. 즉, MN의 프로파일이나 VPN 그룹 별 정책을 기반으로 정적 PE를 지정해 두고, MN의 등록 및 VPN 접속 요청이 들어왔을 때 이를 서비스하는 것이다. 동적 PE 선택 방법은 MN의 프로파일에 적합한 서비스를 제공할 수 있는 PE 중 FCE와 가장 가까운 곳에 있는 PE가 MN을 위한 VPN 서비스를 수행하도록 지정하는 것이다.

PE 선택 메커니즘에 의해 하나의 PE가 선택되면, PNS는 VST 테이블의 *PE_FCE/CE 보안 리스트*에서 MN을 서비스 할 FCE와 선택된 PE 사이에 IPSec 터널이 설립되어 있는지를 검사한다. FCE와 PE간 매핑 정보를 발견했다면, FCE와 PE간 이미 IPSec 터널이 설립되어 있고, 그 PE는 MN이 속한 VPN을 위한 VRF 테이블이 존재하며 BGP/MPLS 동작을 수행하고 있다는 것을 의미한다. 따라서, 이 경우에는 FCE와 PE 간 IPSec 터널 설립을 수행할 필요가 없고, PNS는 PE에게 *VRF Update* 메시지를 보내어 MN의 HoA를 알려주고(그림 6의 A6), PE는 PNS로부터 받은 HoA를 설립된 IPSec 터널과 매핑한 후, 해당하는 VRF 테이블에 추가한다.

PNS가 VST의 *PE_FCE/CE 보안정보 리스트*에서 FCE와 PE 간 매핑 정보를 발견하지 못했다면, PNS는 FCE와 선택된 PE간 IPSec 터널을 설립하도록 해야 한다. 이를 위해 먼저, PNS는 FCE와 각각의 *안전한 원격 구성 채널*(secure remote configuration channel)을 설립하기 위하여 상호 인증 정보와 암호화 정보를 교환한다(그림 6의 A8). 각각의 *안전한 원격 구성 채널*이 설립 완료되면 PNS는 이 보안정보를 *PNS_FCE/CE 보안 리스트*에 추가한다. PNS는 PE와 FCE에게 *IKE Negotiation Request* 메시지를 보낸다(그림 6의 A9). 이때, PNS가 PE에게 보내는 정보는 MN의 HoA, RD, RT인데, 이 정보는 PE가 VRF 테이블을 업데이트 할 때 그리고 동일한 VPN을 서비스하는 다른 PE들에게

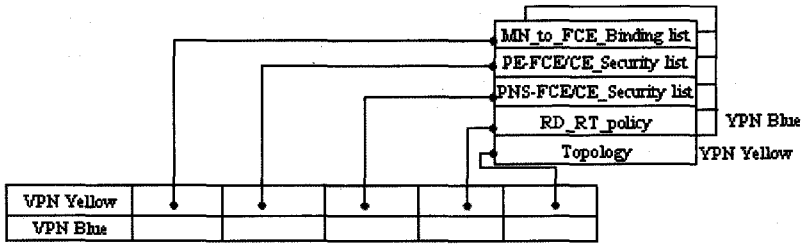


그림 9 PNS에서의 VST 테이블구조

경로 정보를 분배할 때 사용된다. PNS가 FCE에게 보내는 정보는 MN의 HoA, CoA이다. 이 정보는 FCE가 PE와 IPSec 터널을 맺었을 때 그 IPSec 터널과 HoA, CoA 주소를 매핑하기 위해 사용된다.

IKE Negotiation Request 메시지를 받은 PE와 FCE는 둘 간의 IPSec 터널을 설립하기 위해 IKE Negotiation을 수행한다(그림 6의 A10). FCE와 PE간 IPSec 터널 설립이 완료되면 PE는 IPSec 터널이 설립되었다는 것을 PNS에게 알려주기 위해 *IPSec Tunnel Complete* 메시지를 만들어 PNS에게 보낸다(그림 6의 A11). PNS는 *IPSec Tunnel Complete* 메시지를 받으면 PE가 특정 VPN에 대하여 서비스를 제공하기 위해 새롭게 가입한 PE인지를 확인한다. PE가 그 FCE와 설립한 IPSec 터널은 없지만 이미 해당 VPN을 위해서 서비스하는 또 다른 FCE 혹은 CE와 이미 IPSec 터널을 맺고 있어서 VPN 서비스를 제공하고 있을 수도 있다. 새롭게 설립된 IPSec 터널이 해당 VPN을 위해 처음 서비스를 제공하는 것이라면 PE는 그 VPN에 새롭게 조인하는 PE가 된다. 이러한 경우, PNS는 새로이 조인하는 PE에게 *Member PE Addresses* 메시지를 보내어 동일한 VPN을 서비스하는 다른 PE들의 주소를 알려준다(그림 6의 A12). 또한 동일한 VPN을 서비스하는 다른 PE들에게 BGP routing update 정보를 업데이트하도록 알려서 새로운 PE가 VRF 테이블을 업데이트할 수 있도록 한다(그림 6의 A13).

PE와 FCE간 IPSec 터널이 설립된 후에, PE는 MN의 HoA와 설립된 IPSec 터널을 매핑한 후, 해당하는 VRF 테이블에 추가한다. VRF 테이블이 업데이트되면 이 VPN 루트 정보들은 PE들 간의 MP-BGP 세션에 의해 분배된다(그림 6의 A7). PE는 MN의 HoA를 VPN-IP 주소로 만든 후, RT, RD정보와 함께 MP-BGP를 통해 동일한 VPN을 서비스하는 PE들에게 전달한다. 동일한 VPN을 서비스하고 있는 PE들은 VRF 테이블에 MN의 라우팅 정보를 추가한 후, CE에게 라우팅 정보를 전달한다. HA가 자신의 CE와 교환한 라우팅 정보를 통해 MN이 현재 외부 네트워크에 존재한다는 것을 알게 되면, HA는 이동성 캐시 테이블에서 MN의 CoA를 CE의 주소로 변경한다.

PE가 특정 VPN을 서비스하는 PE로 새롭게 추가된 경우라면, 동일한 VPN을 서비스하는 다른 PE들은 VRF 테이블에 들어있는 루트 정보들을 새롭게 추가된 PE에게 전달해야 한다(그림 6의 A14). 앞에서 설명한 것과 같이, PNS는 새로운 PE가 추가되었음을 PE들에게 알린다(그림 6의 A13). 새롭게 추가된 PE는 BGP 루트 정보를 받으면, 해당 VRF 테이블에 그 정보를 추가하고 (그림 6의 A12)를 통해 받은 정보를 기반으로 VPN 루트 정보가 자신과 다른 PE들간 모두 분배되었는지를 결정하여, VPN 루트 분배가 모두 완료되었다면 즉, VRF 테이블 생성(또는 업데이트) 및 BGP/MPLS 업데이트가 완료되면 *VPN Setup Complete* 메시지를 PNS에게 보낸다(그림 6의 A15).

PNS는 *VPN Setup Complete* 메시지를 받으면 VST 테이블의 *MN_to_FCE 바인딩 리스트*에 MN과 FCE의 바인딩 정보를 추가하고, *PE_FCE/CE 보안 리스트*에 VPN Setup Complete에 명시된 보안 정보를 기록한다. 만약, PE가 임의의 VPN을 서비스하도록 새롭게 조인한 PE라면 그 PE를 VPN 토폴로지에 추가하기 위해 *Topology*도 변경되어야 한다.

마지막으로, PNS는 FA-CoA 모드인 경우, HAR 메시지의 MIP-Reg-Request AVP를 처리한 후, MIP-Reg-Reply AVP를 인캡슐 한 HAA(Home-Agent-MIP-Reply) 메시지를 만들어 AAAP에게 보낸다(그림 6의 A16). AAAP는 HAA 메시지를 받으면 AMR 메시지에 대한 응답으로 AMA 메시지를 만들어 AAAF 및 FA를 통해 MN에게 보낸다(그림 6의 A17, A18, A19). Co-located CoA 모드인 경우 PNS는 MIP 등록응답 메시지를 MN에게 직접 보낸다(그림 6의 B4).

그림 10은 PE가 유지하고 있는 VRF 테이블에 MN을 위한 라우팅 정보가 포함된 예를 보이고 있다. PE는 VPN 서비스를 제공하기 위해 각 VPN 그룹별로 분리된 VRF 테이블을 유지하고, 각 VRF에는 VPN 사이트에 대한 경로 정보를 저장하고 있다. 외부 네트워크로 이동한 MN은 무선 네트워크 내에서의 보안을 제공받기 위해 FCE와 IPSec 터널을 설립해야 한다. 만약, MN이 FA-CoA를 사용하는 경우에는 MN과 FA, FA와 FCE 간 IPSec 터널을 설립해야 한다. 단, FA-CoA를 사용하는 경우에도 동일한 장비가 FA와 FCE 기능을 모두 수행하고 있다면 MN과 FCE간에만 IPSec 터널을 설립하면 된다.

3.3 VPN 데이타 패킷의 전달

본 절에서는 송신자와 수신자간 VPN 패킷 송수신 과정에 대해 자세히 설명한다. 송신자과 송신자간 패킷 송수신 환경은 송신자와 수신자가 동일한 사이트의 멤버인 경우와 서로 다른 사이트의 멤버인 경우로 나눌 수 있다. 각 경우는 다시 송신자와 수신자가 모두 홈 네트워크에 있는 경우, 송신자는 홈 네트워크에 있고 수신자가 외부 네트워크에 있는 경우, 송신자가 외부 네트워크에 있고 수신자가 홈 네트워크에 있는 경우, 송신자와 수신자가 모두 외부 네트워크에 있는 경우로 나뉜다. 송신자와 수신자가 동일한 사이트의 멤버인지 아닌지에 관계없이 각각 홈 네트워크에 있는 경우, 송신자와 수신자간 통신은 MIP를 사용하여 동작하는 것과 동일하므

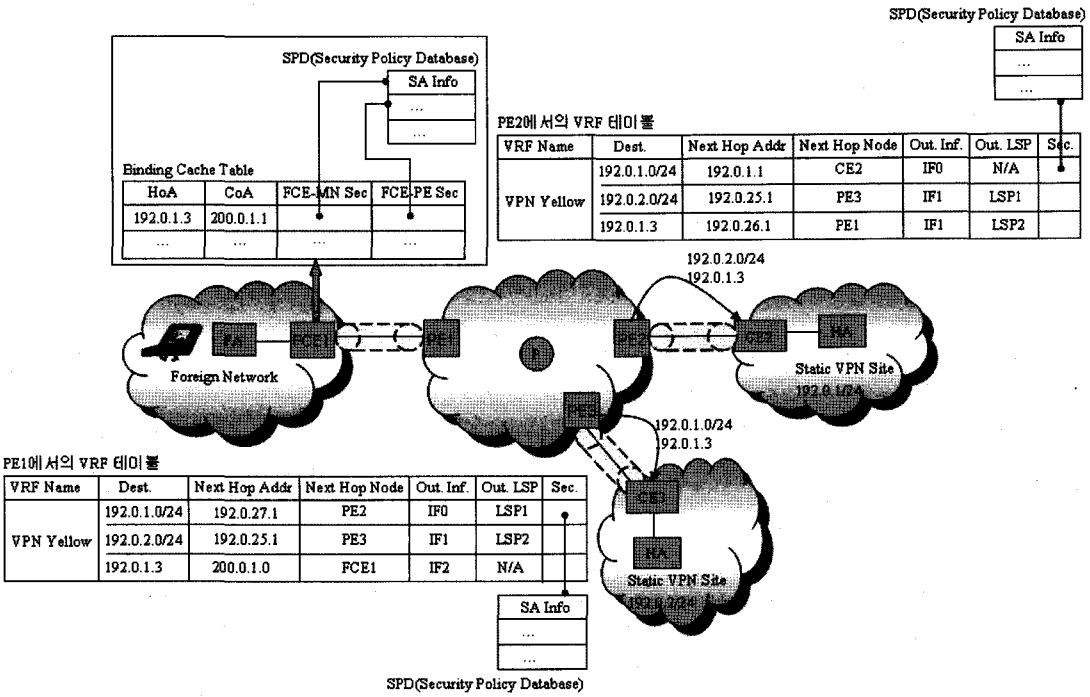


그림 10 PE가 유지하고 있는 VRF 테이블에 MN을 위한 라우팅 정보가 포함된 예

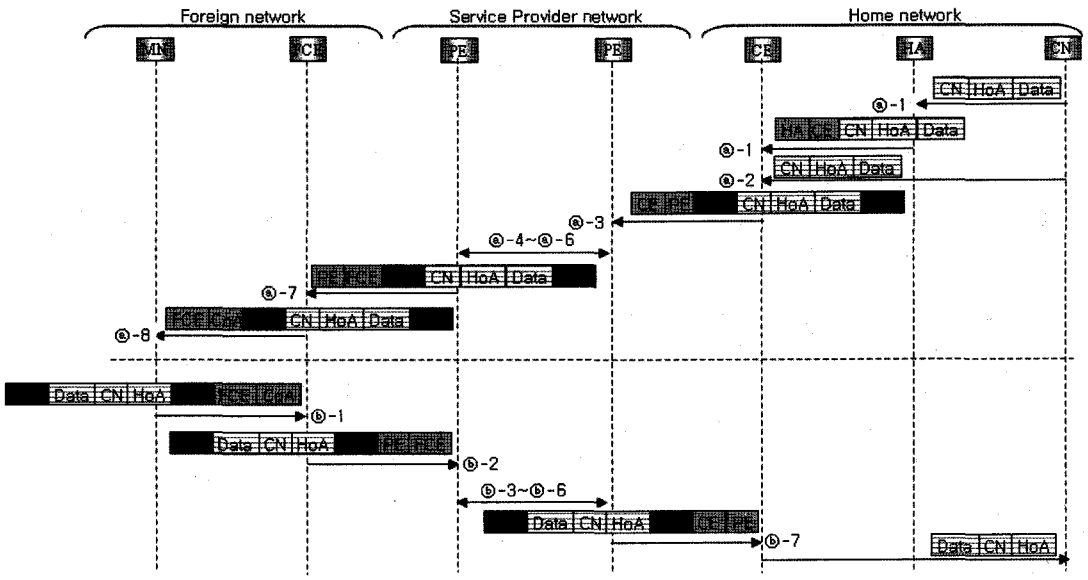


그림 11 MN의 데이타 송수신 과정

로 본 절에서는 송신자와 수신자가 각자의 홈 네트워크에 있는 경우의 데이타 송수신 과정은 생략한다. 그림 11은 나머지 경우에 대해 VPN 데이타 송수신 과정을 보여주고 있다.

• 송신자와 수신자가 동일한 사이트의 멤버인지 아닌지에 관계없이, 송신자가 홈 네트워크에 있고, 수신자가 외부 네트워크에 있는 경우:

ⓐ-1 송신자와 수신자가 동일한 사이트의 멤버이고, 홈 네트워크에 있는 송신자가 외부 네트워크로 이동한 수신자에게 패킷을 송신하는 경우;

송신자와 수신자가 동일한 사이트의 멤버이기 때문에 송신자의 패킷은 수신자의 HA에게 전달된다. 수신자의 HA가 패킷을 받았을 때, HA는 바인딩 캐시 테이블을 검사하여 수신자가 홈 네트워크에 있는지 외부 네트워크에 있는지를 판단한다. 수신자가 외부 네트워크에 있다면 HA는 수신자의 CoA인 CE로 패킷을 전달한다.

ⓐ-2 송신자와 수신자가 서로 다른 사이트의 멤버이고, 홈 네트워크에 있는 송신자가 외부 네트워크로 이동한 수신자에게 패킷을 송신하는 경우;

수신자가 송신자 사이트의 멤버가 아니므로 송신자의 패킷은 사이트 밖으로 전달되어야 한다. 따라서, 패킷은 송신자 네트워크의 CE에게로 전달된다.

ⓐ-3 CE는 VPN 패킷을 받으면 PE와 미리 설립한 IPSec 터널을 통해 PE에게 VPN 패킷을 전달한다.

ⓐ-4 PE는 CE로부터 VPN 패킷이 유입되면 VPN 패킷이 들어온 인터페이스 정보에 따라 VPN을 식별하고, 해당 VRF를 결정한 후 VRF 테이블에서 패킷의 목적지 주소와 일치하는 정보가 있는지 검색한다. PE는 패킷의 목적지 주소에 대하여 longest matching prefix로 VPN 패킷을 전달할 목적지 PE를 찾는다. 여기에서 CE로부터 VPN 패킷을 받은 PE는 진입 PE가 되고, 목적지 PE는 진출 PE가 된다.

ⓐ-5 진입 PE는 획득한 진출 PE 주소와 매핑되어 있는 FIB(Forwarding Information Base)와 LIB(Label Information Base)를 참조하여 LSP를 위한 MPLS 레이블(Outer Label)과 진출 PE에서 출력 인터페이스를 구분하기 위한 내부 레이블(Inner Label)를 추출한 후, 두 개의 레이블을 스태킹하여 다음 홉으로 전송한다.

ⓐ-6 MPLS 백본 네트워크의 코어 라우터들은 MPLS 레이블만으로 패킷을 스위칭 하기 때문에 VPN에 투명하게 전송한다.

ⓐ-7 VPN 패킷이 진출 PE에 유입되면 PE는 MPLS 레이블을 제거하고 내부 레이블로 VRF를 결정해 VRF 테이블을 룩업한다. VRF 테이블에서 목적지 주소에 대한 인터페이스를 검색하고 IPSec 터널을 통해 VPN 패킷을 FCE에게 전달한다.

ⓐ-8 FCE는 바인딩 엔트리에서 HoA와 매핑되는 CoA를 검색하고 그 CoA로 패킷을 전달한다. 이때 FA-CoA 인 경우 CoA는 FA의 주소이며, FA와 설립한 IPSec 터널을 통해 패킷을 전달하며 FA는 다시 수신자와 설립한 IPSec 터널을 통해 패킷을 전달한다. Co-CoA인 경우, CoA는 수신자가 할당받은 주소이며 수신자와 설립한 IPSec 터널을 통해 수신자에게 직접 패킷을 전달한다.

- 송신자와 수신자가 동일한 사이트의 멤버인지 아닌지에 관계없이, 송신자가 외부 네트워크에 있고, 수신자가 홈 네트워크에 있는 경우:

ⓑ-1 외부 네트워크로 이동한 송신자는 소스 주소로 자신의 HoA, 목적지 주소로 수신자의 HoA를 입력한다. FA-CoA 경우, 송신자는 이 패킷을 FA와 설립한 IPSec 터널을 이용하여 FA에게 전달하고, 다시 FA는 FCE와 설립한 IPSec 터널을 이용하여 FCE에게 전달한다. Co-CoA 경우, 송신자는 직접 FCE와 설립한 IPSec 터널을 이용하여 FCE에게 패킷을 전달한다.

ⓑ-2 FCE가 VPN 패킷을 받으면, 패킷을 디캡슐화한 후, 바인딩 캐시 테이블에서 HoA와 매핑 되는 PE를 검색한 후, PE와 미리 설립된 IPSec 터널을 통해 VPN 패킷을 전달한다.

ⓑ-3 PE가 FCE로부터 VPN 패킷을 받으면 IPSec 터널 정보를 기반으로 VRF를 결정한 후 VRF 테이블에서 목적지 주소와 일치하는 정보가 있는지 검색한다. PE는 패킷의 목적지 주소에 대하여 longest matching prefix로 VPN 패킷을 전달할 목적지 PE를 찾는다. 여기에서 FCE로부터 VPN 패킷을 받은 PE는 진입 PE가 되고, 목적지 PE는 진출 PE가 된다.

ⓑ-4와 ⓑ-5 백본 네트워크에서의 패킷 전달 과정은 ⓐ-5와 ⓐ-6의 과정과 동일하다.

ⓑ-6 VPN 패킷이 진출 PE에 유입되면 PE는 MPLS 레이블을 제거하고 내부 레이블로 VRF를 결정해 VRF 테이블을 룩업한다. VRF 테이블에서 목적지 주소에 대한 인터페이스를 검색하고 IPSec 터널을 통해 VPN 패킷을 CE에게 전달한다.

ⓑ-7 CE는 사이트 내에서의 라우팅에 의해 수신자에게 패킷을 전달한다.

- 송신자와 수신자가 동일한 사이트의 멤버인지 아닌지에 관계없이, 송신자와 수신자가 모두 외부 네트워크에 있는 경우:

송신자가 보내는 패킷은 ⓑ-1~ⓑ-5의 과정을 통해 송신하게 되고, 수신자가 받는 패킷은 ⓐ-7, ⓐ-8의 과정을 통해 수신하게 된다.

4. VPN 타입에 따른 MN의 이동성을 지원하는 방안의 안전성 및 오버헤드 비교

본 장에서는 [2]의 사용자 기반 모바일 VPN, [3]의 CE 기반 모바일 VPN, 본 논문에서 제안한 방안과 같은 PE 기반 모바일 VPN에 대하여 최적화된 경로를 통해 데이타를 전달하기 위해 설립되어야 하는 IPSec 터널과 관련한 오버헤드 및 안전성에 대하여 설명한다.

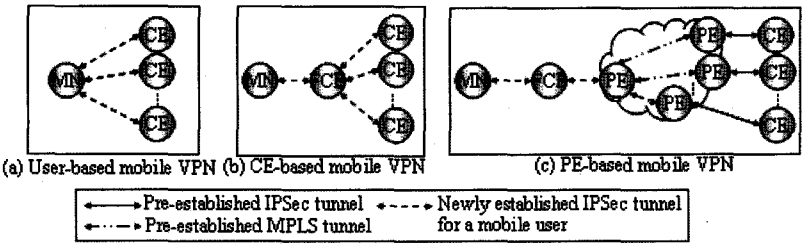


그림 12 모바일 VPN의 접속 형태

그림 12는 모바일 VPN 접속 형태에 따른 터널 설립 형태를 보여주고 있다. 사용자 기반 모바일 VPN에서 IPSec 터널은 MN과 CE간에 설립된다. 만약 MN이 여러 VPN 사이트의 CN과 통신하고자 한다면 MN은 CN이 있는 모든 사이트의 CE와 IPSec 터널을 설립해야 하며, IPSec 터널을 설립하고자 하는 모든 CE의 주소를 알고 있어야 한다. 따라서, MN에서의 IPSec 터널 관리 오버헤드가 크다.

CE 기반 모바일 VPN에서 IPSec 터널은 종단간 보안을 제공하기 위하여 MN과 FCE, FCE와 CE간에 설립된다. MN은 여러 VPN 사이트의 CN과 통신하더라도 현재 자신이 위치한 외부 네트워크의 FCE와 하나의 IPSec 터널만 설립하면 된다. 반면, MN을 서비스하는 FCE는 MN이 통신하고자 하는 모든 사이트의 CE와 IPSec 터널을 설립해야 한다. 동일한 VPN에 속하는 MN들이 동일한 사이트로 접속을 원한다면 FCE는 그 MN들의 서비스 요청을 군집(Aggregate)하여 서비스를 제공할 수 있으므로 FCE가 유지하는 터널의 오버헤드는 사용자 기반 모바일 VPN 보다 적다. 그러나, FCE가 CE와 IPSec 터널을 설립하도록 하기 위해 MN이 CE의 주소를 FCE에게 알려주는 경우, 사용자 기반 모바일 VPN에서와 같이, MN은 IPSec 터널을 설립하고자 하는 모든 CE의 주소를 알고 있어야 한다. [3] 방안에서와 같이 서비스 제공자가 IPSec 터널 설립의 대상을 프로비전 하는 경우라면 FCE가 MN의 등록요청 메시지를 적합한 SPS으로 전달 할 수 있도록 FA상에 SPS 에이전트 모듈이 동작하고 있어야 한다.

PE 기반 모바일 VPN에서는 MN과 FCE, FCE와 PE 간에 각각 IPSec 터널이 설립된다. CE 기반 모바일 VPN에서와 마찬가지로, MN은 여러 VPN 사이트의 CN과 통신하더라도 자신을 서비스하는 FCE와 하나의 IPSec 터널만 설립하면 된다. 그러나 CE 기반 모바일 VPN과는 달리, MN이 통신하고자 하는 CN이 여러 사이트에 있는 경우일지라도 MN을 서비스하는 FCE는 하나의 PE와만 IPSec 터널을 설립하면 되므로 세가지 모바일 VPN 형태 중에서 가장 터널 오버헤드가 적다. 또한 본 논문에서 제안하는 PE 기반 모바일 VPN의 경우, MN은 단지 서비스 제공자의 네트워크 서버의 주소만 알고 있으면 되고, CN이 있는 네트워크의 모든 CE의 주소를 알 필요가 없다. PE 기반 모바일 VPN에서 단점으로는, MN이 이동해서 새로운 등록을 할 때마다 PE 간 BGP/MPLS 메시지 교환이 이루어져서 해당 VPN을 서비스하고 있는 모든 PE의 라우팅 테이블이 갱신되어야 한다. 이와 함께, CE 기반과 PE 기반 모바일 VPN 모두 분리된 IPSec 터널이 설립된다는 단점을 가지고 있다.

안전성측면에서는, MN과 통신하는 상대노드(Correspondent Node)가 CE 뒤(사이트 내)에 있다고 가정할 때, 세 VPN 접속 형태에서 모두 MN과 CE 사이의 전 구간에 IPSec 터널이 설립되므로 모두 동일한 안전성을 보장받을 수 있다. 또한, 제안하는 방안에서 FCE는 CE와 같은 역할을 수행하지만, IPSec 터널 설립에 관련된 정보 이외에 실제적으로 VPN의 어떠한 관련정보(라우팅 및 VPN 구성 정보)도 갖고 있지 않으므로 안전성이 유지된다. 단, 선택된 PE(그림 10에서 PE1)의 경우, VPN 라우팅 및 VPN 구성 정보를 가져야 하므로 VPN 서비스 제공자와 선택된 PE를 갖고 있는 서비스 제공자가 서로 다른 경우, PE는 PNS와 신뢰(trust)관계를 가져야 한다.

5. 시뮬레이션

제안하는 BGP/MPLS 기반 모바일 VPN 구조 및 이동성 지원 프로토콜의 성능을 평가하기 위해 Opnet Modeler 11.0를 이용하여 시뮬레이션을 수행하였다. 제안하는 방안의 구현을 위해 Diameter MIPv4 응용에 기반하여 등록 메시지 전송 및 프로세싱이 이루어지도록 MIP 프로세스 모델에 Diameter MIPv4 프로세스 모델을 추가하였고, PE가 PNS로부터 VRF 업데이트 메시지나 멤버 PE 주소 메시지를 받았을 때 VRF 테이블을 업데이트하도록 BGP 프로세스 모델을 수정하였다. 본 논문에서는 제안하는 방안(이하, M-BGP/MPLS), [3]에서 제안한 CE-기반 모바일 VPN 방안(이하,

M-CE IPSec without RO), 그리고 CE-기반 모바일 VPN에서 루트 최적화를 수행하는 방안(이하, M-CE IPSec with RO) 에 대해 핸드오프 지연, 핸드오프 동안의 평균 처리률, 종단간 패킷 지연을 비교하였다.

그림 13은 시뮬레이션에서 사용된 네트워크 모델을 보여주고 있다. PNS와 AAAP를 가지고 있는 서비스 제공자 플랫폼 및 VPN 사이트 1, 두 개의 외부 네트워크가 각각 IP/MPLS 백본 네트워크에 연결되어 있다. 시뮬레이션에서는 먼저 MN2가 외부 네트워크 2로 이동하고 MN2의 이동이 완료된 후에 MN1이 외부 네트워크 1로 이동하도록 하였으며, MN1이 MN2에게 100Kbps의 속도로 FTP 트래픽을 전송하도록 하였다. 하나의 사이트 내에서의 전송 지연시간은 0.1msec로 가정하였고, 사이트간의 전송 지연 시간은 1msec~0.5sec까지 변화시켜보면서 실험하였다.

그림 14는 MN1이 외부 네트워크 1로 이동했을 시, MN1이 경험한 핸드오프 지연을 보여주고 있다. M-CE IPSec with RO 방안의 경우, 외부 네트워크1의 GW1이 홈 네트워크의 GW와 먼저 IPSec 터널을 설립한 후에, 루트 최적화된 경로로 MN2에게 데이타를 전달하기 위해 외부 네트워크2의 GW2와 IPSec 터널 설립이 완료될 때까지의 시간을 MN1이 경험한 핸드오프 지연으로 측정하였다. 그림 14에서 보는 바와 같이, M-CE IPSec with RO 방안에서는 핸드오프 완료 시점까지 두 번의 IPSec 터널을 설립하므로 핸드오프 지연이 가장 길다. 한 번의 IPSec 터널 설립만 필요로 하는 M-CE IPSec with RO 방안과 FCE와 근접한 PE간 IPSec 터널을 설립하고, PE들간 BGP를 이용한 루트정보를 분배하는 M-BGP/MPLS 방안에서의 핸드오프 지연은 거의 비슷하다.

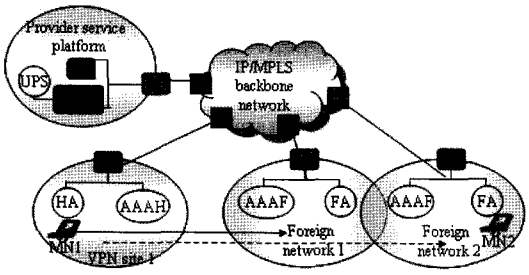


그림 13 시뮬레이션 네트워크 모델

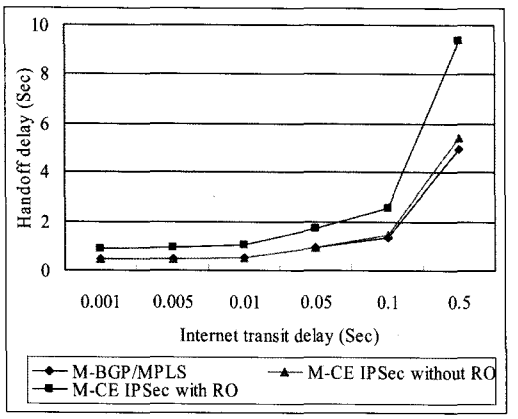


그림 14 핸드오프 지연

비교하는 세 개의 방안에서 핸드오프 지연을 발생시키는 주된 원인은 M-BGP/MPLS 방안의 경우, PE들간 라우팅 테이블 갱신을 위한 루트 정보를 교환하는데 걸리는 시간이고, M-CE IPSec without/with RO 방안의 경우, IPSec 터널을 설립하는데 걸리는 시간이다. 그림 15는 BGP/MPLS 메시지 교환을 위해 걸리는 시간과 IPSec 터널 설립을 위해 걸리는 시간이 핸드오프 지연에 얼만한 영향을 주는 가에 대해 보이고 있다. 그림 15에서 실선은 핸드오프 동안에 루트 정보 교환과 IPSec 터널 설립을 위해 걸린 시간이고, 점선은 그 이외의 나머지 핸드오프 처리를 하기 위해 걸린 시간이다. M-BGP/MPLS 방안이 루트 정보를 분배하기 위한 제어 메시지의 수가 IPSec 터널 설립을 위한 제어 메시지의 수보다 상대적으로 많을지라도, 하나의 PE로부터 루트 정보를 분배하기 위해 걸리는 시간이 다른 PE들과 병렬로 이루어지기 때문에 루트 정보를 교환하는데 걸린 지연 시간이 IPSec 터널 설립을 위한 컨트롤 메시지를 교환하는데 걸린 지연 시간보다 크지 않음을 볼 수 있다. 그러나 루트 정보를 교환과 IPSec 터널 설립을 제외한 컨트롤 메시지를 전달 할 때 발생하는 지연은 M-BGP/MPLS 방안이 두 M-CE IPSec 방안보다 약간 큼을 볼 수 있다.

그림 16은 MN1이 핸드오프를 시작한 후 25초 동안의 평균 처리율을 인터넷 지연에 따라 보인 것이다. 25초는 세 방안 중 핸드오프 지연이 가장 긴 M-CE IPSec with RO 방안에서 핸드오프가 완료되기까지의 시간이다. M-CE IPSec with RO 방안의 핸드오프 지연이 가장 길었음에도 불구하고, 세 방안 모두 평균 처

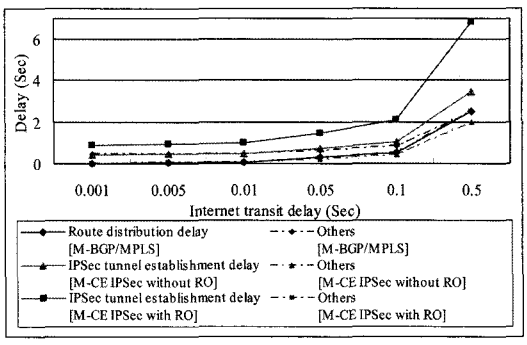


그림 15 핸드오프 지연의 컴포넌츠

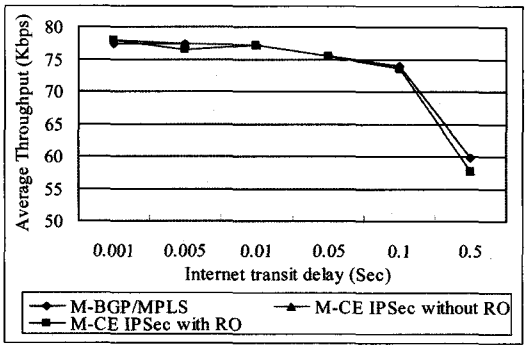


그림 16 핸드오프 동안의 평균 처리율

리율이 거의 비슷함을 볼 수 있다. 그 이유는 외부 네트워크 1의 GW1이 외부 네트워크 2의 GW2와 IPSec 터널을 설립하기 전까지 MN1의 패킷이 홈 네트워크를 경유하여 전달되기 때문이다.

그림 17은 종단간 패킷 지연을 보인 그림이다. 이 실험에서의 인터넷 지연은 0.05sec이다. MN1이 핸드오프하기 전, 세 방안에서의 종단간 패킷 지연이 거의 비슷하다가 핸드오프 이후에 M-CE IPSec without RO 방안의 종단간 패킷 지연이 더 길다는 것을 볼 수 있다. 그 이유는 M-CE IPSec without RO 방안에서는 패킷이 항상 MN2의 홈 네트워크를 통해 전달되기 때문이다. M-CE IPSec with RO 방안의 경우, 외부 네트워크 1의 GW1과 외부 네트워크 2의 GW2가 IPSec 터널을 설립하기 전까지 패킷이 MN2의 홈 네트워크를 통해 전달되어 종단간 패킷 지연이 길다가 GW1과 GW2간 IPSec 터널이 설립이 완료되면 GW1과 GW2간 패킷을 직접 전송하게 되므로 M-BGP/MPLS 방안과 비슷한 종단간 패킷 지연을 보인다. M-BGP/MPLS 방안의 경우, BGP/MPLS 프로토콜을 통해 PE들간 MN의 이동 사실을 알려주기 때문에 홈 네트워크를 경유하지 않고 PE간 직접 패킷을 전달하므로 마치 RO를 적용한 것과 같은 효과를 얻을 수 있다.

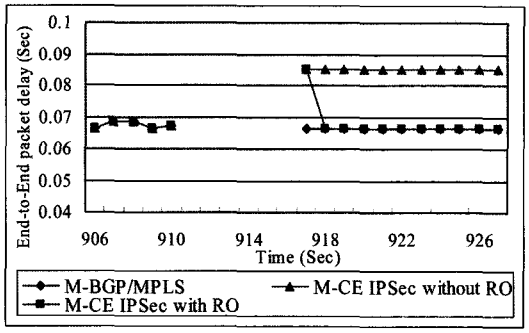


그림 17 종단간 패킷 지연

6. 결 론

본 논문에서는 PPVPN의 BGP/MPLS VPN을 기반으로 모바일 VPN 서비스를 지원하기 위한 네트워크 구조 및 이동성 지원 프로토콜을 제안하였다. 제안하는 네트워크 구조에 의해 서비스 제공자는 기존의 BGP/MPLS VPN 기반 하에 이동 VPN 사용자를 프로비전할 수 있다. 모바일 VPN 사용자는 핸드오프 시나리오에 관계없이, 즉, 동일한 VPN의 다른 사이트로 이동하는 경우, 다른 VPN의 다른 사이트로 이동하는 경우, 일반 인터넷 지역으로 이동하는 경우에 상관없이 동일한 서비스 구조 및 프로토콜로 VPN 서비스를 제공받을 수 있다.

제안하는 방안은, 모바일 VPN 사용자가 통신하고자 하는 모든 사이트의 CE와 직접 IPSec 터널을 설립하는 사용자 기반 모바일 VPN이나, 모바일 VPN 사용자가 있는 외부 네트워크의 GW가 사용자가 통신하고자 하는 CN(들)이 있는 네트워크의 GW(들)과 IPSec 터널을 설립하는 M-CE IPSec with RO 방안과는 달리, 모바일 VPN 사용자가 있는 외부 네트워크의 GW가 하나의 PE와만 IPSec 터널을 설립하면 되므로 터널 설립 오버헤드를 줄일 수 있다. 또한 모바일 VPN 사용자가 통신하고자 하는 모든 사이트의 CE와 직접 IPSec 터널을 설립하지 않아도 되므로 무선 네트워크에서의 자원 낭비도 줄일 수 있으며, M-CE IPSec without RO 방안과 같이 모바일 VPN 사용자와의 통신에 있어서 항상 홈 네트워크를 거치지 않아도 되므로 종단간 패킷 지연이 짧다. 시뮬레이션을 통해, 제안하는 방안이 M-CE IPSec with RO 방안과 비슷한 종단간 패킷 지연을 보이면서, 핸드오프 지연에 있어서는 핸드오프 시 루트 최적화를 위한 추가적 IPSec 터널을 설립하지 않는 M-CE IPSec without RO와 비슷함을 볼 수 있었다.

참 고 문 헌

[1] R. Callon et al., "A framework for Layer 3 Provider-Provisioned Virtual Private Networks (PPVPNs)," *RFC4110*, July 2005.

[2] S. Vaarala(Ed.), "Mobile IPv4 traversal across IPsec-based VPN gateways," <draft-ietf-mobileip-vpn-problem-solution-03.txt>, Sept. 2003.

[3] Francisco Barcelo et al., "Design and Modelling of Internode: A Mobile Provider Provisioned VPN," Mobile Networks and Applications 8, pp.51~60, 2003.

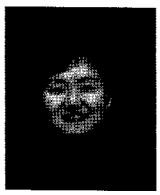
[4] Ravi Bhagavathula et al., "Mobility: A VPN Perspective," IEEE MWSCAS Aug. 2002.

[5] Eric C. Rosen et al., "Architecture for the Use of PE-PE IPsec Tunnels in BGP/MPLS IP VPNs," draft-ietf-l3vpn-ipsec-2547-05.txt, August 2005.

[6] P. Calhoun et al., "Diameter Mobile IPv4 Application," RFC4004, August 2005.
[7] Calhoun et al., "Diameter Base Protocol," RFC 3588, September 2003.
[8] Perkins et al., "Mobile IPv4 Challenge/Response Extensions," RFC 3012, November 2000.

변 해 선

2001년 광주대학교 컴퓨터학과 졸업(학사). 2003년 이화여자대학교 과학기술대학원 컴퓨터학과 졸업(공학석사). 2003년~현재 이화여자대학교 컴퓨터학과 박사과정. 관심분야는 VPN, Mobile VPN, QoS, BcN and NGN



이 미 정

1983년~1987년 이화여자대학교 전자계산학 학사. 1987년~1989년 University of North Carolina at Chapel Hill 컴퓨터학 석사. 1990년~1994년 North Carolina State University 컴퓨터공학 박사. 1994년~현재 이화여자대학교 공과대학 컴퓨터학과 교수. 관심분야는 고속 통신 프로토콜 설계 및 성능 분석, 멀티미디어 전송을 위한 트래픽 제어, 인터넷에서의 QoS 지원, 무선 이동 네트워크, Ad-hoc 네트워크, 광대역 통합망, 가상사설망