Provider Provisioned VPN에서 이동성 지원 방안

변해선° 이미정
이화여자대학교 컴퓨터학과
ladybhs@ewhain.net°, lmj@ewha.ac.kr

Mobility Support on Provider Provisioned VPN

Haesun Byun° Meejeong Lee
Ewha Womans University, Department of Computer Science and Engineering

요 약

본 논문에서는 PPVPN(Provider Provisioned VPN)에서 PE(Provider Edge) 기반 모바일 VPN 서비스를 제공하기 위한 네트워크 구조 및 이동성 지원 프로토콜을 제안한다. 제안하는 방안은 RFC2547에 제시된 'BGP/MPLS VPN' 기술을 기반으로 하며, BGP/MPLS VPN 서비스를 제공받고 있는 모바일 사용자가 외부 네트워크로 이동했을 때, 모바일 사용자의 VPN 접속 및 이동성을 지원하기 위해 서비스 제공자 측에 PNS(PPVPN Network Server)를 새로이 도입하였다. PNS는 모바일 사용자와 VPN을 매핑하는 바인딩 정보를 유지하며, 모바일 사용자를 서비스하는 외부 네트워크의 GW와 서비스 제공자 네트워크의 PE간 접속회선으로 IPSec 터널을 설립하도록 지시하고, 그 PE에게 모바일 사용자의 VPN 접속에 필요한 정보를 제공하여 그 PE가 BGP/MPLS 동작에 참여하도록 한다.

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 관리자를 대신하여 VPN 설립부터 관리까지 모든 책임을 담당하는 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.

한편, 호텔, 공항 등의 공공장소에 무선 LAN의 설치가 증가하고, 모바일 기기의 다양화와 무선 기술의 발전으로 모바일 사용자가 급격히 증가하고 있다. 이러한 모바일 기술의 발전과 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 GW(Gateway)와 IPSec(IP Security) 터널을 설립하고, 이동성을 보장받기 위해 HA(Home Agent)에게 이동 사실을 등록하여 MIP(Mobile IP) 터널을 설립하는 형태의 방안들이 대부분이었다. 이러한 모바일 VPN 서비스 구조는 외부 네트워크에 있는 MN이 홈 네트워크에 있는 CN(Correspondent Node)과 통신하는 경우 효율적일 수 있으나, 사이트-대-사이트 VPN 구조를 고려했을 때 동일한 VPN에 속하지만 MN의 홈 네트워크 아닌, 다른 사이트에 있는 CN과의 통신에 있어서는 비효율적일 수 있다.

그림 1은 CE 기반 IPSec 터널로 연결된 사이트-대-사이트 VPN과 모바일 VPN이 함께 구성되어 있는 VPN 구조의 예를 나타낸 그림이다. 그림 1에서 VPN-A의 사이트 1, 2, 3은 사이트-대-사이트 VPN을 구성하기 위해 각 사이트 간 랜-투-랜으로 연결하고, CE 간 IPSec 터널이 설립되어 있다. 사이트 1을 홈 네트워크로 사용하는 MN은 외부 네트워크에 나가 있는 동안 사이트 1의 CE와 IPSec 터널을 설립하고 HA와 MIP 터널을 설립하여 통신한다. MN은 자신과 동일한 VPN에 속하지만 홈 네트워크 이외의 사이트에 있는 CN과 통신을 요구할 수도 있다. 그러나, MN이 단지 홈 네트워크에 있는 CE와만 IPSec 터널을 설립한 경우, 동일한 VPN의 다른 사이트에 있는 CN과 통신함에 있어서 데이터가 항상 MN의 홈 네트워크를 통해서 전달되므로 데이터 지연이 발생할 수 있다.

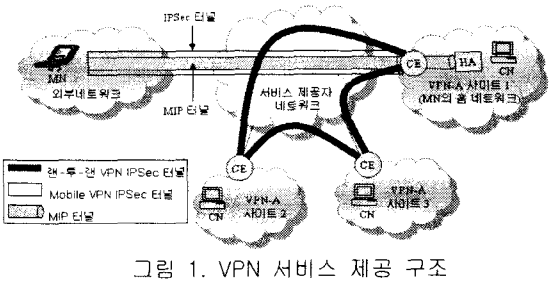

그림 1. VPN 서비스 제공 구조

이와 같은 문제를 해결하기 위하여 RO(루트 최적화:Route Optimization)를 수행하는 경우, MN은 CN이 있는 네트워크의 CE와 IPSec 터널을 별도로 설립해야

본 논문은 산업자원부의 산업기술개발사업(한국산업기술평가원)과 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 육성.지원사업의 지원으로 수행된 연구결과입니다.

한다. 만약, 비디오 회의와 같은 응용서비스를 사용하기 위하여 MN이 사이트 2와 3에 있는 각각의 CN과 동시에 통신하기를 원한다면 CN이 있는 네트워크의 CE와 각각의 IPSec 터널을 설립해야 할 것이다. 이는 많은 수의 사이트를 갖는 VPN에서 MN이 동일한 VPN에 속하는 다수의 사이트내의 CN과 통신하는 경우, 터널의 수가 크게 증가하여 확장성 문제를 가지게 된다. 또한 IPSec 터널 설립을 위한 시그널링 오버헤드로 무선 네트워크 자원의 낭비를 가져올 수 있으며, MN 스스로 VPN 접속을 수행하고 IPSec 터널을 설립, 유지·관리하기 때문에 터널 관리에 대한 복잡성이 증가한다.

이에, 본 논문에서는 PPVPN에서 PE 기반 모바일 VPN 서비스를 제공하기 위한 구조 및 이동성 지원 프로토콜을 제안한다. 제안하는 방안은 RFC2547에 제시된 BGP/MPLS VPN 방식을 기반으로 한다. BGP/MPLS VPN[1]은 PE 기반 사이트-대-사이트 VPN을 지원하는 대표적인 PPVPN에서 3계층 VPN 기술이다. 제안하는 방안에서는 BGP/MPLS VPN 서비스를 제공받고 있는 모바일 사용자의 VPN 접속 및 이동성을 유지·관리하기 위해 서비스 제공자 측에 PNS(PPVPN Network Server)를 새로이 도입하였다. PNS는 외부 네트워크로 이동한 MN의 이동성을 지원하기 위해 MN과 VPN에 대한 바인딩 정보를 유지한다. 또한 외부 네트워크의 GW와 서비스 제공자 네트워크에서 선택된 하나의 PE간 IPSec 터널을 설립하도록 지시하며, 그 PE에게 MN의 VPN 접속에 필요한 정보를 전달하여 그 PE가 BGP/MPLS VPN 동작에 참여하도록 한다. 제안하는 방안에서 외부 네트워크의 GW는 하나의 PE와 IPSec 터널을 설립하면 되기 때문에 MN이 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 PE 기반 VPN 기술 중 하나인 BGP/MPLS VPN에 대해 설명한다. 3장에서는 본 논문에서 제안하는 서비스 구조와 MN의 이동성을 지원하는 프로토콜에 대하여 자세히 설명하고, 4장에서는 시뮬레이션 결과를 살펴보고 결론을 맺는다.

2. 관련 연구

PPVPN에서 가장 대표적인 3계층 CE 기반 VPN은 IPSec 터널을 이용한 VPN 기술이다. 이 기술은 서비스 제공자의 제어를 통해 구성되는 CE 기반 VPN으로, VPN 고객은 서비스 제공자에게 VPN 구성에 참여하는 CE의 집합과 VPN 토폴로지 정보를 알려줘야 한다. 서비스 제공자는 이 정보를 기반으로 VPN 데이터베이스를 구성하고, 그 VPN을 관리하고 프로비전한다. 동일한 VPN에 속하는 VPN 사이트들은 CE와 CE간 VPN 터널을 통하여 라우팅 정보와 VPN 트래픽을 교환한다. 이때, CE와 CE 간 설립되는 VPN 터널로는 IPSec 터널이 사용된다.

3계층 PPVPN에서 CE 기반 모바일 VPN에 대한 대표적인 연구로는 M-CE IPSec 방안이 있다[2]. 그림 2는 M-CE IPSec 방안에서 모바일 VPN을 서비스하는 구조를 나타낸 그림이다. 이 방안에서는 MN을 서비스하는 FA가 MN으로부터 MIP RR(Registration Request) 메시지를 받으면 FA는 이 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 RR 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 RR 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. 한편, VPN 서버는 MIP RR 메시지를 HA에게 전달한다. HA는 MIP RR 메시지의 응답으로 MIP RP(Registration Reply) 메시지를 만들어 SPS를 통하여 FA에게 전달하고, FA는 이를 MN에게 전달한다.

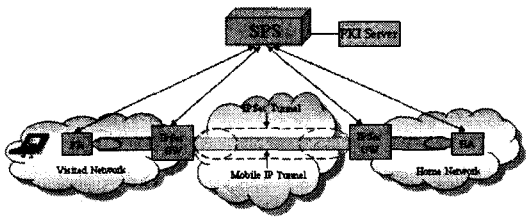

그림 2. M-CE IPSec 방안에서의 모바일 PPVPN

이 방안에서는 외부 네트워크의 GW가 MN을 대신하여 홈 네트워크의 GW와 IPSec 터널을 설립한다. 그러나 서론에서 설명한 바와 같이, MN이 여러 사이트내의 CN과 통신하고 있다면 MN이 있는 외부 네트워크의 GW는 통신하고자 하는 CN이 있는 모든 GW와 IPSec 터널을 설립해야 하는 단점을 가지고 있다.

3. 제안하는 방안

그림 3은 제안하는 PE 기반 모바일 VPN 서비스를 지원하기 위한 네트워크 구조 및 터널 형태를 나타내는 그림이다. 제안하는 방안에서는 외부 네트워크의 GW가 VPN 사이트를 서비스하는 CE와 같이 동작한다. 본 논문에서는 홈 네트워크의 CE와 구분하기 위해 외부 네트워크의 GW를 FCE(Foreign Customer Edge)라고 부른다.

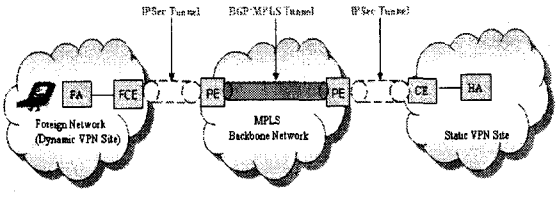

그림 3. PE 기반 모바일 VPN을 지원하는 네트워크에서의 터널 형태

제안하는 구조에서 외부 네트워크는 동적인 VPN 사이트로 볼 수 있으며, 동일한 VPN에 속하는 MN들이 동일

한 FCE가 서비스하는 외부 네트워크에 들어와 있다면 VPN 사이트 내에 VPN 사용자가 있는 것으로 간주할 수 있다. 정적인 VPN 사이트와 서비스 제공자 네트워크를 연결하는 CE와 PE 구간에는 접속회선과는 별도로 보안을 제공하기 위하여 IPSec 터널을 이용한다. CE와 PE간 IPSec 터널 이용 방안은 이미 IETF의 L3VPN WG에 의해 표준화가 진행되고 있다[3]. 외부 네트워크와 서비스 제공자 네트워크를 연결하는 FCE와 PE 구간에는 접속회선과 보안 제공을 목적으로 IPSec 터널을 사용한다. 서비스 제공자 네트워크내의 PE와 PE 구간에는 RFC2547에 제시된 BGP/MPLS VPN을 기반으로 한다.

그림 4는 PE 기반 VPN에서 MN의 이동성을 지원하는 서비스 구조를 보인 그림이다. 제안하는 서비스 구조는 서비스 제공자가 모바일 VPN 사용자들의 이동성을 지원하고 VPN을 관리하는 PPVPN 기반에서 동작한다. 이를 위해, 서비스 제공자 측의 네트워크에 PNS 개체를 새로이 도입하였다. PNS는 네트워크 서비스 제공자 측에 있는 장비로써 네트워크 차원에서의 VPN 프로비저닝과 MN의 이동성을 제공한다. 즉, 홈 네트워크에 있던 MN이 외부 네트워크로 이동했을 때, PNS는 외부 네트워크의 FCE와 PE간 접속회선으로 IPSec 터널을 설립하도록 지시하고, 그 PE에게 VPN 토폴로지, RT(Route Target)와 RD(Route Distinguish)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 사용자 프로파일 정보를 유지하고 있는 개체이다.

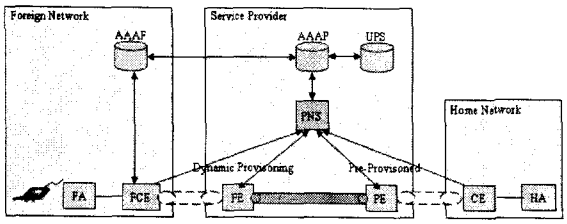

그림 4. PE 기반 모바일 VPN을 지원하는 네트워크에서의 터널 형태

3.1 MN의 등록 및 VPN 구동 절차

그림 5는 PE 기반 모바일 VPN에서의 MN의 등록과정을 보여준다. 제안하는 방안에서는 MN의 등록과 인증을 위해 Diameter MIPv4 프로토콜[4]을 사용한다. Diameter MIPv4 프로토콜은 MN의 인증, 권한 부여, 과금 등의 서비스를 제공하기 위한 프로토콜로 IETF AAA WG에 의해서 표준화가 완료되었다.

외부 네트워크로 이동한 MN은 자신의 이동 사실을 알리기 위해 MIP RR 메시지 만든다. 제안하는 방안에서는 PPVPN 기반으로 MN의 이동성을 지원하기 위해 MIP RR 메시지의 구조를 그림 6과 같이 수정하였다. 그림 6에서 음영으로 표시된 부분이 MIP RR 메시지의 수정된 필드를 나타낸다. *Home Address*는 MN의 홈 주소이다. *PNS Address*는 MN의 이동성 및 VPN 접속을 지원하는 서비스 제공자 측의 네트워크 서버의 주소이며, MIPv4의 HA 주소 대신에 사용된다. MN은 MIPv4에서 HA 주소를 미리 알고 있듯이, PNS 주소를 미리 알고 있다고 가정한다. *FCE Address*는 MN을 서비스하는 외부 네트워크의 GW 즉, FCE의 주소이다. 이 주소는 서비스 제공자 네트워크의 PE와 IPSec 터널을 설립할 FCE 주소를 PNS에게 알리기 위해 사용되며, MN이 CoA를 할당 받을 때 같이 획득한다고 가정한다.

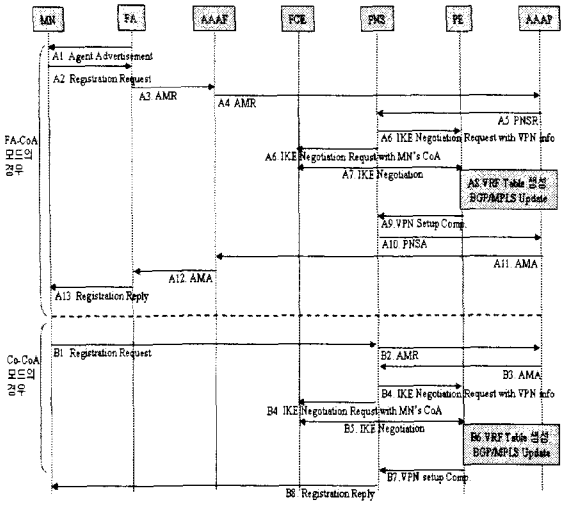

그림 5. PE 기반 모바일 VPN에서의 MN의 등록과정

MN은 *PNS Address*에 PNS 주소를 입력하고, *FCE Address*에 획득한 FCE 주소를 입력하여 MIP RR 메시지를 만든다. 이때, MN은 서비스 제공자 네트워크의 AAAP에게 MIP 등록 인증을 얻기 위해 Diameter MIPv4 프로토콜에서와 같이 MIP RR 메시지에 *Challenge and MN-AAA authentication extension*을 포함한다. *Challenge and MN-AAA authentication extension*은 MIP RR의 재전송방지(replay protection)에 대한 제어 및 MN의 인증을 위해 필요한 정보이다.

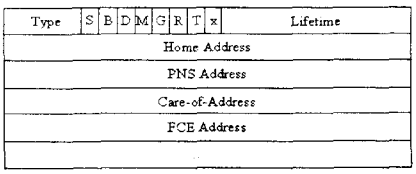

그림 6. 수정된 MIP RR 메시지 구조

MN이 FA-CoA 기반으로 동작하는 경우, MN은 MIP RR 메시지를 FA에게 보낸다(그림 5의 A2). FA는 MIP RR 메시지를 받으면 새롭게 AMR(AA-Mobile-Node-Request) 메시지를 만든다. Diameter MIPv4 프로토콜에서 AMR 메시지는 MN의 인증과 접근권한을 요구하기 위한 메시지이다. 제안하는 방안에서는 FCE 주소를 PNS에게 전달하기 위해 AMR 메시지에 *MIP-FCE-Address*를 새로이 추가하였다. 그림 7은 수정된 AMR 메시지를 보여준

다. FA는 AMR 메시지를 AAAF에게 보낸다(그림 5의 A3).

<AA-Mobile-Node-Request>::=<Diameter Header:260, REQ,PXY>
<Session-ID>
{Auth-Application-ID}
.....
[MIP-FCE-Address]

그림 7. 수정된 AMR 메시지

AMR 메시지를 받은 AAAF는 AMR 메시지를 또 다른 Diameter 서버에게 전달할 것인지, 자신이 처리해야 하는 것인지를 결정하기 위해 [5]에서 제시된 것과 같이 동작하여 결정한다. AMR 메시지는 AAAF에 의해 최종적으로 서비스 제공자 네트워크의 AAAP에게 전달된다(그림 5의 A4). AAAP는 *MN-AAA authentication extension*을 보고 MN-AAA security association[6]을 사용하여 MN의 등록요청 메시지를 인증한다. 인증이 성공되면, PNS에게 PNSR(Provider-Network-Server-MIP-Request) 메시지를 보낸다(그림 5의 A5). PNSR 메시지는 Diameter MIPv4에서의 HAR(Home-Agent-MIP-Request) 메시지를 재명명한 메시지로, PNS에게 MIP 등록을 요청하기 위해 사용된다. PNS는 PNSR 메시지를 받으면, MN의 VPN 접속 및 이동성 지원을 위한 절차를 시작한다.

MN이 Co-CoA 모드로 동작하는 경우, MN은 MIP RR 메시지를 PNS에게 보낸다(그림 5의 B1). PNS는 MIP RR 메시지를 받으면, MIP-Feature-Vector AVP에 *Co-Located-Mobile-Node* 비트를 설정하여 AMR 메시지를 만든 후, 이 메시지를 AAAP에게 보낸다(그림 5의 B2). AAAP는 AMR 메시지를 받으면 MN을 인증 한 후, 이에 대한 응답으로 AMA 메시지를 만들어 PNS에게 보낸다(그림 5의 B3). PNS는 AMA 메시지를 받으면 MN의 VPN 접속 및 이동성 지원을 위한 절차를 시작한다.

MN의 VPN 접속 및 이동성 지원을 위한 절차는 다음과 같다. 먼저, PNS는 AAAP로부터 PNSR 메시지를 받거나(FA-CoA인 경우), AMA 메시지를 받으면(Co-CoA인 경우), MN의 VPN 접속 요청을 처리하기 위해 MN을 서비스할 적합한 PE를 선택해야 한다. PNS가 PE를 선택하는 기준은 로드밸런싱이나 MN와 PE의 거리, 정적/동적 PE 선택 방법 등을 고려하여 선택하는 것으로 가정한다.

하나의 PE가 선택되면, PNS는 그 PE와 FCE 간 IPSec 터널을 설립하도록 해야 한다. PNS는 PE와 FCE에게 각각의 IKE Negotiation Request를 보내기 전에 VST(VPN Service Tunnel) 테이블을 검사한다. VST 테이블은 MN에 대한 이동성 및 보안을 포함한 VPN 정보를 관리하기 위하여 PNS에서 유지하는 테이블이다.

그림 8은 PNS에서 유지하고 있는 VST 테이블의 구조를 나타낸다. VST 테이블은 VPN 그룹별로 이동성 바인딩 엔트리(BCE_ptr), PE와 FCE/CE 간 보안 정보 엔트리(PEFE_ptr), PNS와 FCE/CE간 보안 정보 엔트리(PNFE_ptr), RT/RD 정책 정보 엔트리(RRE_ptr), VPN 토폴로지 정보(Topology) 등을 유지한다. 이동성 바인딩 엔트리에는 이동한 MN의 HoA, CoA, FCE, PE의 바인딩 정보를 유지하고 있다. PE와 FCE/CE 간 보안 정보 엔트리에는 두 노드 간 SA를 유지하기 위해 필요한 보안 정보가 들어 있다. PNS와 FCE/CE간 보안 정보 엔트리에는 PNS가 FCE와 CE를 관리하기 위해 필요한 상호 인증, 암호화 정보 등을 포함하고 있으며, RT/RD 정책 정보 엔트리에는 VPN 구성에 필요한 RT과 RD 정보를 유지하고 있다. VPN 토폴로지 정보는 VPN의 구성 형태로 풀 메시, 메시 또는 성형 구조인지를 기록하고 있다.

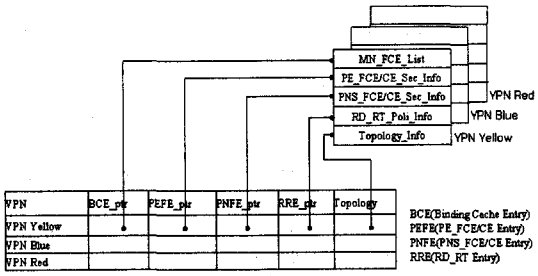

그림 8. PNS에서의 VST 테이블 구조

PNS는 VST 테이블의 PE와 FCE/CE 간 보안 정보 엔트리에서 MN을 서비스 할 FCE와 선택된 PE 사이에 IPSec 터널이 설립되어 있는지를 검사한다. FCE-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 PE간 IPSec 터널 설립을 수행할 필요가 없고, PNS는 선택된 PE에게 VPN 설립에 필요한 정보를 전달하지 않아도 된다. 단지, PE는 PNS로부터 MN의 HoA를 받아 설립된 IPSec 터널과 매핑한 후, 해당하는 VRF 테이블에 추가한다.

PNS가 VST에서 FCE PE 간 매핑 정보를 발견하지 못했다면, PNS는 FCE와 선택된 PE간 IPSec 터널을 설립하도록 해야 한다. PNS는 PE에게 VPN 설립에 필요한 정보 즉, MN의 HoA, RD, RT 등과 함께 IKE Negotiation Request 메시지를 보내고, 또한 FCE에게 MN의 HoA, CoA와 함께 IKE Negotiation Request 메시지를 보내어 PE와 FCE간 IPSec 터널을 설립하도록 지시한다(그림 5의 A8과 B5). FCE와 PE간 IPSec 터널 설립이 완료되면 PE는 MN의 HoA와 설립된 IPSec 터널을 매핑한 후, 해당하는 VRF 테이블에 추가한다.

그림 9는 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.

이러한 VPN 라우팅 정보는 PE들 간의 MP-BGP 세션에 의해 분배된다. 이를 위해, PE는 MN의 HoA를 VPN-IP 주소로 만든 후, RT, RD정보와 함께 MP-BGP를 통해 동일한 VPN을 서비스하는 PE들과 교환한다. 동일한 VPN을 서비스하고 있는 PE들은 VRF 테이블에 MN의 라우팅 정보를 추가한 후, CE에게 라우팅 정보를 전달한다. HA가 CE와 교환한 라우팅 정보를 통해 MN이 현재 외부 네트워크에 존재한다는 것을 알게 되면, MN

의 HA는 이동성 바인딩 테이블에서 MN의 CoA를 CE의 주소로 변경한다.

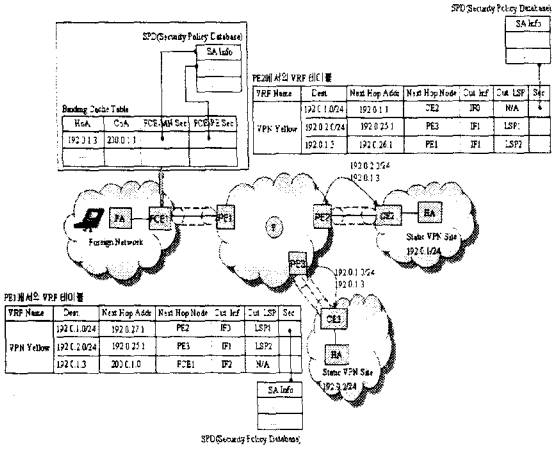

그림 9. PE가 유지하고 있는 VRF 테이블 예

PE는 VRF 테이블 생성(또는 업데이트) 및 BGP/MPLS 업데이트가 완료되면 VPN Setup Complete 메시지를 PNS에게 보낸다(그림 5의 A9, B7). PNS는 VPN Setup Complete 메시지를 받으면 FA-CoA 모드인 경우, PNSR 메시지의 *MIP-Reg-Request AVP*를 처리한 후, *MIP-Reg-Reply AVP*를 인캡슐 한 PNSA(Provider-Network-Server-MIP-Reply) 메시지를 만들어 AAAP에게 보낸다(그림 5의 A10). PNSA 메시지는 Diameter MIPv4에서의 HAA(Home-Agent-MIP-Reply) 메시지를 재명명한 메시지이다. AAAP는 PNSA 메시지를 받으면 AMR 메시지에 대한 응답으로 AMA 메시지를 만들어 AAAF 및 FA를 통해 MN에게 보낸다(그림 5의 A11,12,13). Co-located CoA 모드인 경우 PNS는 MIP RP 메시지를 MN에게 보낸다(그림 5의 B8).

3.2 VPN 트래픽 전달 과정

홈 네트워크에 있는 CN이 외부 네트워크로 이동한 MN에게 패킷을 전달하는 동작 과정에 대해 설명한다.

ⓐ HA가 MN을 목적지로 하는 패킷을 받았을 때, 이동성 바인딩 테이블을 검사하여 MN이 홈 네트워크에 있는지 외부 네트워크에 있는지를 판단한다. MN이 외부 네트워크에 있다면 HA는 MN의 CoA로 패킷을 전달한다. MN이 외부 네트워크로 나가 있는 동안 HA에서 유지하고 있는 MN의 CoA는 CE의 주소이다.

ⓑ CE는 HA로부터 VPN 패킷을 받으면, PE로부터 받은 라우팅 정보를 기반으로 작성된 라우팅 테이블에서 MN이 다른 사이트에 있다는 것을 판단하고, PE와 미리 설립한 IPSec 터널을 통해 PE에게 VPN 패킷을 전달한다.

ⓒ PE는 CE로부터 VPN 패킷이 유입되면 VPN 패킷이 들어온 인터페이스 정보에 따라 VPN을 식별하고, 해당 VRF를 결정한 후 VRF 테이블에서 MN의 주소와 일치하는 정보가 있는지 검색한다. PE는 MN의 HoA를 이용하여 longest matching prefix로 VPN 패킷을 전달할 PE를 찾기 때문에 MN의 홈 네트워크가 아닌 MN이 이동한 외부 네트워크와 연결된 PE의 주소를 획득한다. 여기에서 CE로부터 VPN 패킷을 받은 PE는 진입 PE가 되고, 외부 네트워크와 연결된 PE는 진출 PE가 된다.

ⓓ 진입 PE는 획득한 진출 PE 주소에 대해 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 레이블 스태킹으로 추가하여 다음 홉으로 전송한다.

ⓔ MPLS 백본 네트워크의 코어 라우터들은 MPLS 레이블만으로 패킷을 스위칭 하기 때문에 VPN에 투명하게 전송한다.

ⓕ VPN 패킷이 진출 PE에 유입되면 PE는 MPLS 레이블을 제거하고 내부 레이블로 VRF를 결정해 VRF 테이블을 룩업한다. VRF 테이블에서 MN에 대한 인터페이스를 검색하고 MN과 관련하여 FCE와 맺은 IPSec 터널을 통해 VPN 패킷을 FCE에게 전달한다.

ⓖ FCE는 바인딩 엔트리에서 HoA와 매핑되는 CoA를 검색하고 그 CoA로 MN의 패킷을 전달한다.

4. 시뮬레이션 결과 및 결론

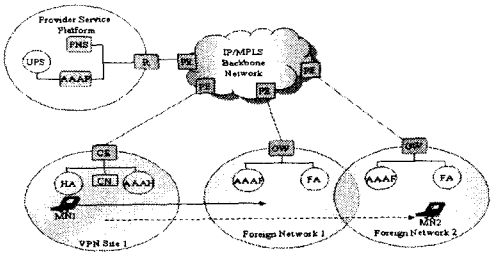

그림 10. 시뮬레이션 네트워크 모델

본 논문의 성능평가를 위해 Opnet Modeler 11.0을 이용하여 시뮬레이션을 수행하였다. 구체적으로 Diameter MIPv4 응용에 기반하여 등록 메시지 전송 및 프로세싱이 이루어지도록 MIP 프로세스 모델을 수정하였고, PE 라우터가 PNS로부터 IPSec 터널 설립 메시지 및 VPN 설립에 관련한 메시지를 받았을 때 VRF 테이블을 생성 또는 업데이트하도록 BGP 프로세스 모델을 수정하였다.

본 논문에서는 제안하는 방안(M-BGP/MPLS)과 관련 연구에서 설명된 M-CE IPSec with RO방안, M-CE IPSec without RO 방안에 대해 MN의 핸드오프 지연, 처리률, 종단간 패킷 지연을 비교하였다. M-CE IPSec with RO 방안의 경우, 외부 네트워크1의 GW1이 외부 네트워크2의 GW2와 IPSec 터널 설립이 완료되기 전까지 통신을 시작하지 않는 것으로 가정하였다.

그림 10은 시뮬레이션에서 사용된 네트워크 모델을 보이고 있다. PNS와 AAAP를 가지고 있는 서비스 제공자 플랫폼 및 VPN 사이트 1과 두 개의 외부 네트워크가 각각 IP/MPLS 백본 네트워크에 연결되어 있다.

그림 11은 MN2가 외부 네트워크로 이동을 완료한 이후, MN1과 통신하는 도중 MN1이 외부 네트워크 1로 이

동하는 상황에서, 인터넷 지연에 따른 MN1의 핸드오프 지연을 보여주고 있다. 그림 11에서 보는 바와 같이, 인터넷 지연이 길어질 때 M-CE IPSec with RO방안에서의 핸드오프 지연이 M-CE IPSec without RO 방안과 M-BGP/MPLS 방안보다 더 커짐을 볼 수 있다. M-CE IPSec without RO 방안과 M-BGP/MPLS 방안은 인터넷 지연이 0.1초일 때까지 MN 핸드오프 지연이 거의 비슷하다가 0.1초 이후부터 조금씩 차이가 발생한다. 세 방안에서 각각 핸드오프 지연의 차이는 M-BGP/MPLS 방안에서의 BGP/MPLS 메시지 교환에 따른 지연과 두 M-CE IPSec 방안에서의 IPSec 터널 설립에 따른 지연의 차이에서 발생한다. 그림 12는 두 방안에서 각각 BGP/MPLS 메시지 교환과 IPSec 터널 설립이 핸드오프 지연에 얼만한 영향을 주는 가를 보이고 있다. M-CE IPSec with RO방안의 경우, MN1이 이동한 외부 네트워크 1의 GW은 MN1의 홈네트워크의 GW와 IPSec 터널을 맺음과 동시에, 별도로 MN2가 있는 외부 네트워크 GW와 IPSec 터널을 설립해야 하므로 IPSec 터널 설립 지연이 핸드오프 지연이 크게 영향을 미친다. IPSec 터널 설립 메시지와 BGP/MPLS 메시지를 제외한 나머지 메시지의 전달을 위한 지연은 약간의 차이는 있지만 세 방안이 거의 비슷함을 볼 수 있다.

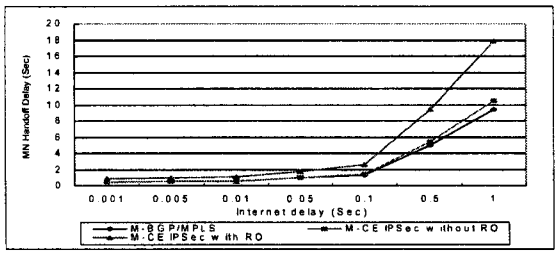

그림 11. MN의 핸드오프 지연

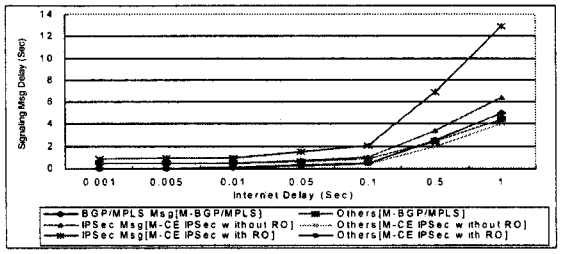

그림 12. 메시지별 핸드오프 지연

그림 13는 MN1이 이동했을 시, 패킷 처리율 변화를 보여준다. M-BGP/MPLS 방안과 M-CE IPSec without RO 방안이 M-CE IPSec with RO 방안보다 핸드오프 지연이 작기 때문에 핸드오프 후 패킷을 더빨리 수신한다.

그림 14는 종단간 패킷 지연을 보이고 있다. M-CE IPSec without RO 방안은 두 노드간 통신할 때 항상 홈 네트워크를 거쳐 통신하기 때문에 종단간 패킷 지연이 길다. M-CE IPSec with RO 방안의 경우, RO를 적용하여 종단간 패킷 지연은 M-BGP/MPLS 방안과 비슷하나, M-BGP/MPLS 방안보다 패킷을 수신하기 시작하는 시점이 느리다. 반면, M-BGP/MPLS 방안의 경우, PE간 MN의 위치를 알기 때문에 RO를 이용하지 않고도 홈 네트워크를 거치지 않고 PE간 직접 패킷 전달이 가능하므로 마치 RO를 적용한 것과 같은 효과를 얻을 수 있다.

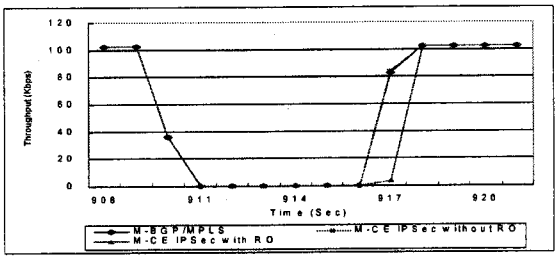

그림 13. 노드 이동 시, 패킷 처리율 변화

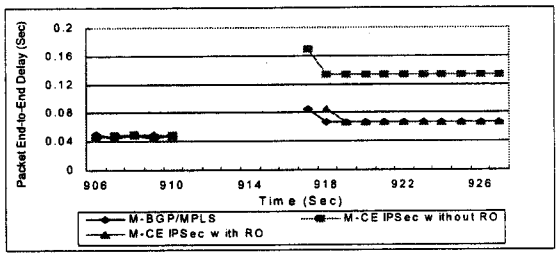

그림 14. 종단간 패킷 지연

본 논문에서는 PPVPN에서 PE 기반 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 프로비전 할 수 있으므로 부가서비스 제공을 위한 수익 모델로 사용할 수 있다. 모바일 VPN 사용자는 핸드오프 시나리오에 관계없이, 즉, 동일한 VPN의 다른 사이트에 이동하는 경우, 다른 VPN의 다른 사이트로 이동하는 경우, 일반 인터넷 지역으로 이동하는 경우에 상관없이 동일한 서비스 구조 및 프로토콜로 VPN 서비스를 제공받을 수 있으며, 모바일 VPN 사용자가 통신하고자 하는 모든 사이트의 CE와 직접 IPSec 터널 설립을 하지 않아도 되므로 유지·관리해야 하는 터널의 수를 줄일 수 있다. 또한 터널 설립으로 인한 무선 네트워크에서의 자원 낭비도 줄일 수 있다.

참고문헌

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

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

[3] Eric C. Rosen, Jeremy De Clercq, Yves T'Joens, "Architecture for the Use of PE-PE IPsec Tunnels in BGP/MPLS IP VPNs", draft-ietf-l3vpn-ipsec-2547-05.txt, August 2005

[4] P. Calhoun, T. Johansson, C. Perkins, T. Hiller, P. McCann, "Diameter Mobile IPv4 Application", RFC4004, August 2005

[5] Calhoun, P., Loughney, J., Guttman, E., Zorn, G., and J. Arkko, "Diameter Base Protocol", RFC 3588, September 2003

[6] Perkins, C. and P. Calhoun, "Mobile IPv4 Challenge/Response Extensions", RFC 3012, November 2000