특집

Mobile VPN

김경민, 변해선, 이미정(이화여자대학교)

I. 서 론

VPN(Virtual Private Network)은 인터넷과 같은 공중망을 사용하여 사설망을 구축하게 해주는 기술 혹은 통신망으로, 회사 사설망의 보완 혹은 대치 수단으로 상당한 호응을 얻은 바 있고, 향후 응용의 등장에 따라 이에 대한 수요가 개인적인 차원으로도 확대될 전망이다. 그런데 무선 통신 기술의 발전과 함께 모바일 사용자가 급격히 증가함에 따라 기존 VPN 서비스는 모바일 사용자가 지역적 제한 없이 VPN 서비스를 제공받을 수 있도록 확대될 필요성이 있다. 이에, MIP(Mobile IP)나 SIP(Session Initiation Protocol)를 사용하여 VPN 사용자의 이동성을 지원하고, IPsec(IP Security) 또는 SSL(Secure Socket Layer)과 같은 터널링 및 암호화 기법을 사용하여 데이터의 안전한 전송을 지원하는 모바일 VPN에 대한 연구가 활발히 이루어지고 있다.

모바일 VPN 서비스를 지원하기 위한 가장 대표적인 방안은 이동성 지원 프로토콜인 MIP와 보안 프로토콜인 IPsec을 함께 사용하는 것이다. IPsec 터널을 이용한 MIP 기반 모바일 VPN은 터널 시작점의 위치에 따라 사용자 기반 모바일 VPN과 네트워크 기반 모바일 VPN으로 나눌 수 있다. 사용자 기반 모바일 VPN은 외부로 이동한 VPN 사용자로부터 VPN 게이트웨이까지 맺어지는 자의적(Voluntary) 터널 기반 VPN이고, 네트워크 기반 모바일 VPN은 사용자에게 이동성을 제공하는 개체인 외부 네트워크의 모바일 에이전트(예, FA 또는 MAP) 혹은 서비스 제공자 네트워크의 종단 라우터로부터 VPN 게이트웨이까지 맺어지는 의무적(Compulsory)적 터널 기반 VPN이다. 자의적 터널로 구현된 사용자 기반 모바일 VPN은 손쉽게 원격접속 VPN을 구현하여 사용할 수 있는 장점이 있으나, MN(Mobile Node)이 터널링과 관련한 키교환, 암호화, 복호화 수행 등을 부담해야 하며, 무선 구간에서의 터널 오버헤드로 인한 자원 낭비 및 성능 저하를 가져올 수 있는 단점이 있다. 반면 네트워크 기반 모바일 VPN은 서비스 제공자의 입장에서 사용자 제어가 쉬워지며, 사용자 입장에서는 보안 제공을 위한 터널 설립과 관련한 기능을 서비스 제공자 디바이스에게 맡김으로써 부담을 줄일 수 있는 장점을 지니나 사용자와 IPsec 터널을 시작하는 서비스 제공자 개체 사이

에 보안이 취약해 지는 단점이 있다.

이 외에도 모바일 VPN 서비스를 제공하는 방법으로, SIP 모바일 VPN과 SSL 모바일 VPN이 존재한다. SIP 모바일 VPN은 실시간 데이터 전송에 사용되는 시그널링 프로토콜인 SIP를 이용하는 모바일 VPN이고, SSL 모바일 VPN은 어플리케이션 계층 보안 프로토콜인 SSL 터널을 통해 안전한 데이터 전송을 제공하는 모바일 VPN 서비스이다. 두 모바일 VPN 방안은 IPsec 터널을 이용한 MIP 모바일 VPN을 사용하는데 발생하는 MIP와 IPsec의 비호환성 문제를 부분적으로 해결할 수 있다는 장점을 가지나, 서비스 제공 어플리케이션이 한정적이라는 단점을 지닌다.

본 고에서는 서론에 이어, 위에 언급한 여러 모바일 VPN의 구현 방법에 대해 소개한다. 구체적으로, IPsec 터널을 이용한 MIP 기반 모바일 VPN, SIP 기반 모바일 VPN, SSL 터널을 이용한 모바일 VPN에 대해 순서대로 기술하고, 그 외 모바일 VPN을 구현하기 위해 고려해야 할 사항에 대해 간단히 살펴본 후, 결론을 맺는다.

II. 본 론

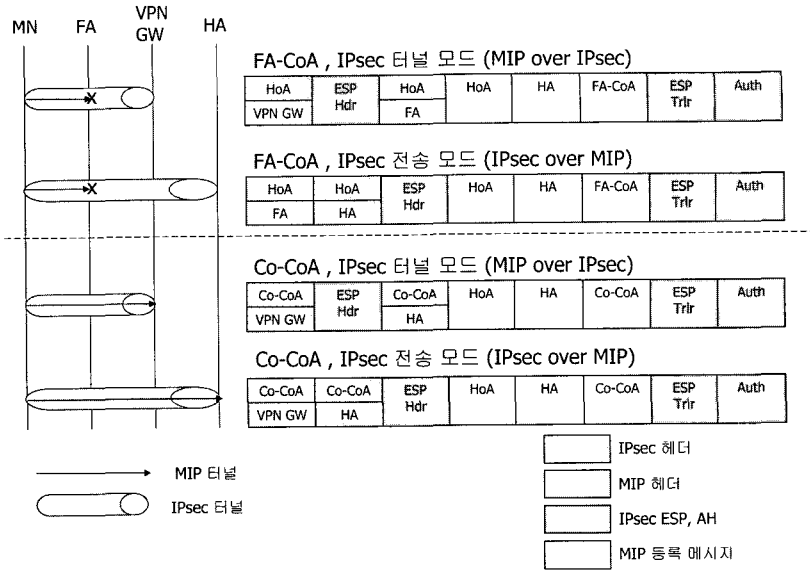
1. IPsec 터널을 이용한 MIP 기반 모바일 VPN

가. MIPv4 기반 모바일 VPN

VPN 사용자에게 안전하고 효율적인 이동성을 지원하는 가장 대표적인 방안은 IPsec 터널을 이용한 MIP 기반 모바일 VPN이다. MIP는 사용자가 홈 네트워크에 있는 경우HoA(Home-of-Address)를 사용하고, 다른 네트워크로 이동했을 때에는 이동한 네트워크에서 할당받은 CoA(Care-of-Address)를 사용하여 통신을 지속할 수 있게 하는 이동성 지원 프로토콜이다. MIP에서 사용하는 CoA는 Co-CoA와 FA-CoA가 있다. Co-CoA는 DHCP 등을 통해서 MN에 직접 할당되는 주소이고, FA-CoA는 MN이 방문한 네트워크 내에서의 FA(Foreign Agent) 주소이다. Co-CoA를 CoA로 사용하는 경우에는 MN이 CoA를 HA(Home Agent)에 등록한 후, HA와 MN간에 설립된 MIP 터널을 통해 데이터가 전송된다. 반면, FA-CoA를 CoA로 사용하는 경우에는 HA와 MN간에 이루어지는 모든 데이터 전송이 중간에 FA를 거치며 FA와 HA사이에 MIP 터널을 사용하게 된다.

IPsec은 모바일 VPN에서 데이터 전송의 안전성을 보장하기 위한 프로토콜로 인증과 데이터의 무결성을 제공한다. IPsec은 터널(tunnel) 모드 또는 전송(transport) 모드로 사용되는 데, 터널 모드는 패킷의 페이로드와 IP 헤더를 모두 암호화 한 후 새로운 IP 헤더를 붙이는 방식이고, 전송 모드는 패킷의 페이로드(payload)만 암호화하는 방식이다. 모바일 VPN에서 IPsec 터널 모드는 MN와 VPN 게이트웨이 간에 IPsec 터널을 맺는다. 이 때 MIP 터널은 FA-CoA를 사용하는 경우, FA와 HA간에 설립되며 Co-CoA를 사용하는 경우, MN과 HA간에 설립된다. 반면, IPsec 전송모드는 MN과 HA사이에 IPsec 터널을 맺으며 MIP터널 또한 MN에서 HA간에 맺어진다.

모바일 VPN을 위해 위와 같이 IPsec과 MIP을 동시에 사용하는 데는 여러 문제점이 존재한다. 먼저, MN이 FA-CoA를 사용하는 경우 IPsec 모드에 상관없이 다음과 같은 문제가 발생한다. MN에서 작성된 MIP 등록 메시지는 IPsec을 이용하여 암호화 되고, 이 IPsec 패킷은 FA에게 전

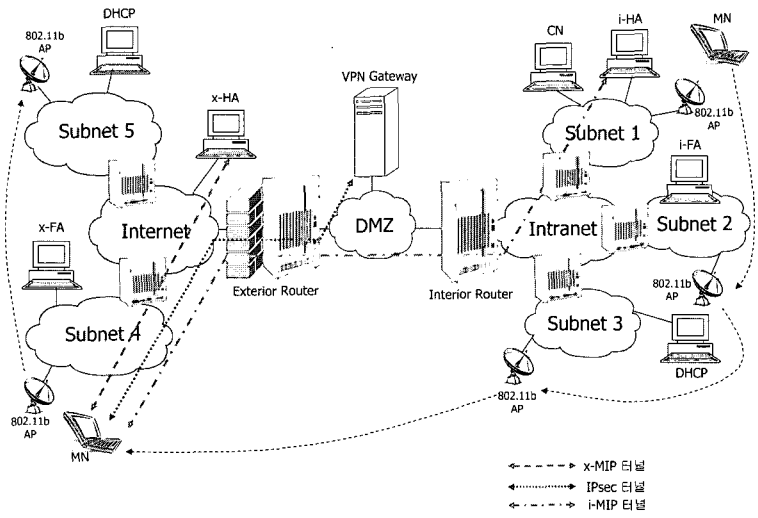


〈그림 1〉 IPsec을 적용한 MIP 등록 메시지 형태

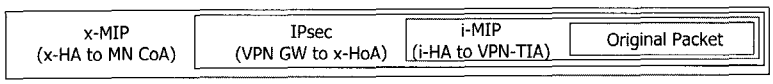
달되는데 FA는 IPsec 터널의 종단점이 아니기 때문에 암호화된 패킷을 복호화할 수 없다. 그러므로 FA에서 MIP 등록에 실패하는 문제가 발생한다. 반면 MN이 Co-CoA를 사용하는 경우, IPsec 터널모드에서는 MIP 등록이 정상적으로 이루어지나 MN이 이동함에 따라 Co-CoA가 변경되어 IPsec을 재설립해야 하는 문제가 생긴다. IPsec 전송모드에서는 MN과 HA 사이에 IPsec이 맺어지는데 이 패킷을 중간에 VPN 게이트웨이가 진입(Ingress) 필터링을 수행하여 삭제하므로 HA에서 MIP 등록에 실패하게 된다. 이 때 VPN 게이트웨이가 IPsec 패킷을 필터링하지 않고 HA에 전달하도록 하는 정책을 지니고 있다면 HA에서 MIP 등록에 성공할 수 있게 된다.

IPsec 터널을 이용한 MIPv4 기반 모바일 VPN 서비스를 제공하기 위해 위에 기술한 문제를 해결하는 여러 가지 방안이 제시되었다. 대표적으로 정적(static) x-HA(Extenal Home Agent)를 사용하는 방안이 있다[2]. 이는 외부 네트워크에 하나의 x-HA를 두고 MN이 외부 네트워크로 이동한 경우, x-HA를 통해서 MIP 등록을 수행하도록 하여 MIP가 FA-CoA 모드를 사용하는 경우 MIP 등록에 실패하는 문제를 해결하는 방안이다.

그림 2.(a)는 x-HA를 사용하는 모바일 VPN 구조를 보여준다. 그림 2.(a)에서 MN은 자신의 홈 네트워크인 Subnet 1로부터 외부 네트워크인 Subnet 4로 이동한다. MN이 외부 네트워크의 Subnet 4로 들어오게 되면 MN은 x-MIP 터널을 설립하기 위해 x-HA에게 등록 요청 메시지를 보내는데, 이 때 등록 요청 메시지의 CoA에는 x-FA의 주소를 기록한다. MN이 작성하는 등록 메시지는 홈 네트워크의 VPN 게이트웨이 밖에 있는 x-HA에 등록하기 위한 메시지이므로 IPsec으로 암호화하지 않는다. 그러므로 x-FA에서 IPsec 패킷이 아닌 일반적인 MIP 등록 메시지를 보고 등록 절차를 성공적으로 수행한다. 이 후 VPN 게이트웨이와 x-HoA를 이용하여 IPsec 터



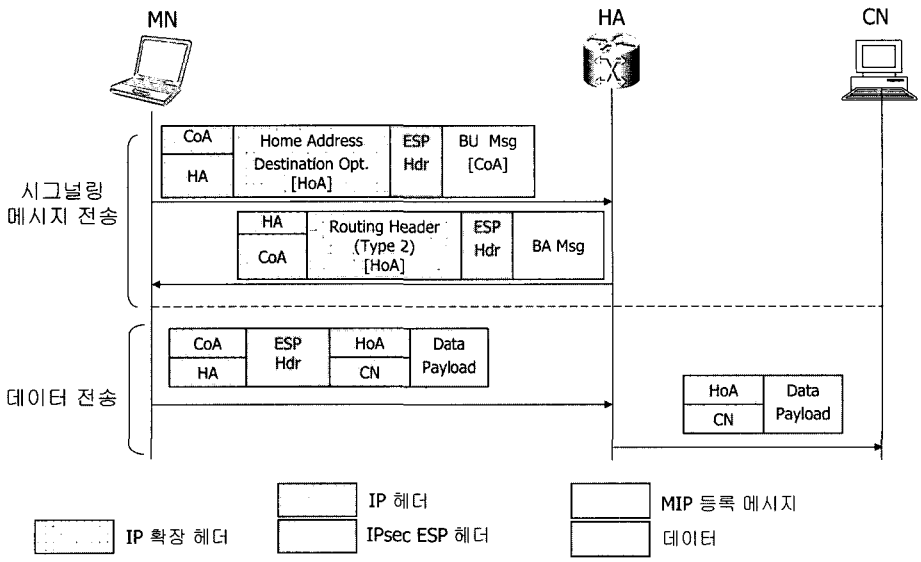
〈그림 2-a〉 x-HA를 사용하는 모바일 VPN 구조



〈그림 2-b〉 외부 네트워크에서 MN이 작성한 데이터 패킷

널을 맺고, MN은 IPsec 터널을 맺을 때 VPN 게이트웨이로부터 할당받은 VPN-TIA (VPN tunnel inner address)를 CoA로 하여 i-HA에 등록한다. 다시 MN이 서브넷 5로 이동하게 되어도 새로운 x-MIP 터널을 설립하기 위한 MIP 등록 메시지는 IPsec 암호화를 이용하지 않으므로 x-FA와 x-HA에 성공적으로 등록 과정을 마친다. x-MIP 터널이 설립된 후, MN은 새로 설립한 x-MIP 터널과 이전 서브넷 4에서 설립한 IPsec 터널과 i-MIP 터널을 이용하여 자신의 홈 네트워크의 서브넷 1에 있는 CN(Correspondent Node)과 통신을 재개한다. 그림 2.(b)는 CN에서 MN으로 전송되는 데이터 패킷으로, i-MIP, IPsec, x-MIP의 3중 터널이 사용되는 것을 보여준다.

그러나 [2]에서 제시한 정적 x-HA를 사용하는 방안은 FA에서 MIP 등록에 실패하는 문제를 해결하였지만 x-HA와 MN의 현재 위치가 멀어지게 되면 핸드오프 지연시간이 길어진다는 문제가 있다. 이 문제를 해결하기 위해 [3]에서는 인증 프로토콜인 Diameter MIP를 통해 동적으로 x-HA를 할당받는 방안을 제안하였다. MN이 외부 네트워크로 이동하면 MN은 Diameter MIP를 통해 AAA(Authentication, Authorization, Accounting) 인증과 함께 MIP 등록을 수행한다. 이 과정에서 MN은 AAAH(AAA Home)로부터 MN의 현재 위치와 가까운 곳에 x-HA를 할당받는다. 할당받은 x-HA의 x-HoA는 AAAH로부터 Diameter MIP 메시지를 통해 i-HA에 전달되며 i-HA는 x-HoA를 MN의 CoA로 등록한다. 등록 과정에 성공한 MN은 할당받은 x-HoA와 VPN 게이트웨이 간에 IPsec 터널을 설립한다. MN이



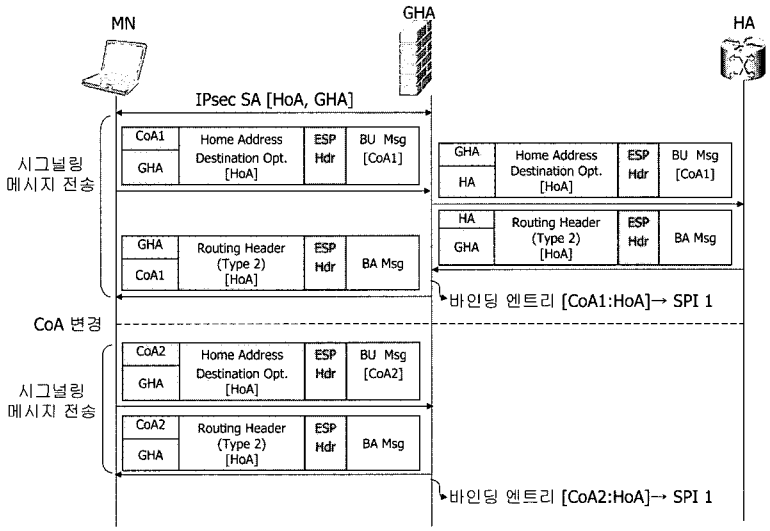
〈그림 3〉 MIPv6에서 MN과 HA 사이에 메시지 흐름과 패킷 형태

동일한 외부 네트워크 내의 다른 서브넷으로 이동했을 경우, x-HA는 변경되지 않으나 x-FA가 변경되므로 x-MIP 터널을 재설립해야 한다. 이때 정적 x-HA를 사용하는 방안과는 달리, x-HA와 MN의 거리가 가까우므로 MN의 핸드오프 지연시간이 줄어든다. 반면 MN이 다른 외부 네트워크로 이동하면 Diameter MIP를 통한 AAA 인증과 함께 상기한 과정을 되풀이함으로 인해 상당히 긴 지연이 발생하게 된다는 문제가 있다.

MN이 Co-CoA를 사용하는 경우, 그림 1의 설명에서 언급한 바와 같이 MN이 이동함에 따라 Co-CoA가 변경되어 IPsec 터널을 재설립하는 문제가 발생한다. 이는 MN의 핸드오프 지연시간을 증가시키므로 모바일 VPN 서비스를 사용하는 데 있어 성능이 저하된다. IPsec 터널을 재설립하는 문제를 해결하기 위한 방법으로 MOBIKE(IKEv2 Mobility and Multihoming)가 제안되었다[4]. MOBIKE는 IETF WG에서 제시된 프로토콜로 IPsec에 이동성 지원을 목적으로 한다. MOBIKE를 이용하는 Co-CoA 모드 모바일 VPN은 CoA가 바뀌더라도 IPsec 터널을 재설립하지 않고, IPsec SA에 바뀐 종단점 주소인 CoA만을 업데이트하여 IPsec 터널의 잦은 재설립으로 인한 핸드오프 지연시간을 줄인다.

나. MIPv6 기반 모바일 VPN

MIPv6는 IPv6 확장(extension) 헤더를 통해 기본적으로 지원되는 IPsec을 이용하여 데이터 안전을 보장한다. MIPv6에서는 FA를 사용하지 않아 Co-CoA를 사용한 모바일 VPN 서비스만 지원하기 때문에 MIPv4 기반 모바일 VPN에서와 같이 FA-CoA를 사용했을 때 생기는 비호환성 문제는 일어나지 않는다. 그러나 Co-CoA를 사용할 때 Co-CoA와 HA간에 IPsec을 설립함으로써 발생하는 IPsec 터널의 잦은 재설립 문제는 여전히 발생할 수 있다. [5]에서는 MN과 HA간에 HoA와 HA 주소로 IPsec을 설립함으로써 위의 문제를 해결하는 방안을 제시한 바 있다.



〈그림 4〉 GHA를 이용한 MIP 등록 메시지 흐름

그림 3은 [5]에 따른 MN과 HA 사이의 메시지 흐름과 패킷 형태를 나타낸다. 이 방안에서 BU(Binding Update) 메시지와 BA(Binding Acknowledge) 메시지는 MN과 HA간에 IPsec 전송모드로 전달되며, 경로 최적화(Route Optimization)를 사용하지 않는 경우의 데이터 및 RR(Return Routability) 메시지는 항상 HA를 거쳐 전송되어야 하므로 IPsec 터널모드로 전달된다.

시그널링 메시지 전송 과정에서 MN은 먼저, MIP 등록을 위하여 BU 메시지를 만든다. 이 때, BU 메시지의 소스 주소는 HoA이고, 목적지 주소는 HA 주소이다. BU 메시지 작성 후, MN은 HoA와 HA 주소를 기반으로 IPsec SA를 찾고, 찾은 SA 정보를 이용하여 BU 메시지를 암호화한다. 또한, IPv6 확장헤더 중 하나인 Destination Options Header내의 Home Address Option 필드 내에 CoA를 추가한다. BU 메시지를 전송하기 전에 MN은 외부 네트워크의 패킷 필터링 제한에 걸리지 않도록 하기 위해 MIP 헤더의 소스 주소인 HoA와 Home Address Option 필드의 CoA를 교환한다. 즉, MN은 최종적으로 MIP 헤더의 소스 주소를 CoA로 하고, 확장헤더에 HoA를 기록한 BU 메시지를 HA에 전달하게 된다. BU 메시지를 받은 HA는 MN과 동일하게 HoA와 HA주소를 기반으로 생성된 IPsec SA를 가지고 있으므로, IPsec으로 암호화된 BU 메시지를 복호화하고 CoA와 HoA에 대한 바인딩 캐쉬 엔트리를 생성한다. 또한 HA는 BU의 응답으로 BA 메시지를 MN에게 전달한다. MN과 CN간 데이터는 MN과 HA사이에 IPsec SA를 이용하여 암호화된 후 HA에게 전달된다. HA는 IPsec 패킷을 복호화하여 본래의 데이터를 얻은 후, 내부 IP 헤더에 있는 CN의 주소를 보고 CN에게 전달한다. 이 방안에서 시그널링 메시지와 전송 데이터의 MIP 헤더 소스 주소로 CoA를 사용하나, IPsec SA를 HoA와 HA주소로 맺음으로써 잦은 CoA가 변경에 의한 IPsec 재설립 문제를 해결하였다.

한편, 위에서 기술한 MIPv6 동작을 기반으로

모바일 VPN 서비스를 제공하기 위한 방안으로 GHA(Gateway Home Agent)를 사용하는 방안이 [6]에 제시되었다. [5]에서 제시된 MIPv6 방안을 모바일 VPN 서비스와 접목하기 위해서는 VPN 게이트웨이가 HA와 같은 모바일 지원 기능을 가져야 한다. 따라서 MN은 HA와 VPN 게이트웨이에 각각 BU 메시지를 보내야 한다. [6]에서는 HA와 VPN 게이트웨이 각각에게 BU 메시지를 보내는 오버헤드를 줄이기 위해 MIP의 HA 기능과 VPN 게이트웨이의 기능을 모두 수행하는 개체인 GHA를 사용하여 한 번의 BU 메시지 전송을 통해 바인딩을 생성, 유지하도록 하였다.

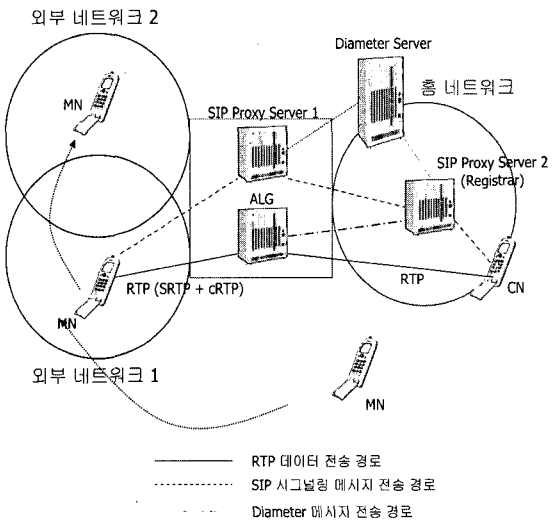
그림 4는 GHA를 사용한 MIPv6 기반 모바일 VPN에서의 MIP 등록 메시지 흐름을 나타내는 그림이다. 시그널링 메시지 전송 과정을 보면 MN이 외부 네트워크로 이동하여 CoA를 획득하면 먼저 GHA로 BU 메시지를 보낸다. 이 때 BU 메시지의 MIP 헤더 소스 주소는 CoA이고, 목적지 주소는 GHA의 주소이다. GHA가 BU 메시지를 받으면 BU 메시지 내의 CoA를 자신의 주소로 업데이트하여 HA로 전송한다. HA는 BU 메시를 받은 후, HoA와 GHA 주소를 CoA로 하는 바인딩 캐쉬 엔트리를 생성하고 BA 메시지를 작성하여 GHA로 전달한다. GHA는 BA 메시지를 받아 CoA와 HoA에 대한 바인딩 캐쉬 엔트리를 생성하는 데 이 때, 바인딩 캐쉬 엔트리는 GHA가 매뉴얼하게 혹은 동적으로 얻은 IPsec SA와 매핑 되도록 한다. GHA가 가진 IPsec SA는 MN과 HA간에 HoA와 HA 주소로 설립된 IPsec SA와 동일하다. 이 과정을 마친 후, GHA는 BU에 대한 응답으로 MN에게 BA를 전달한다.

이 방안에서 MN의 CoA가 변경되어도 GHA와 HA가 가진 IPsec SA는 그대로 유지되고, GHA가 지닌 바인딩 캐쉬 엔트리 내의 CoA만 업데이트된다. 이는 [5]에서와 마찬가지로, MIPv4 기반 모바일 VPN 서비스에서 Co-CoA 모드가 사용되는 경우와 달리 CoA 변경에 대해 IPsec SA를 재협상하지 않으므로 빈번한 IPsec 재설립을 줄인다. 또한, 이 방안은 x-HA를 사용하는 방안과 달리 하나의 HoA만 사용하므로 추가적인 IP 주소가 필요하지 않다. 뿐만 아니라, MN이 GHA와 HA에게 각각 BU를 보내지 않고, MN과 GHA간, MN과 HA간 IPsec을 따로 설립하지 않아도 되므로 시그널링 오버헤드를 줄인다.

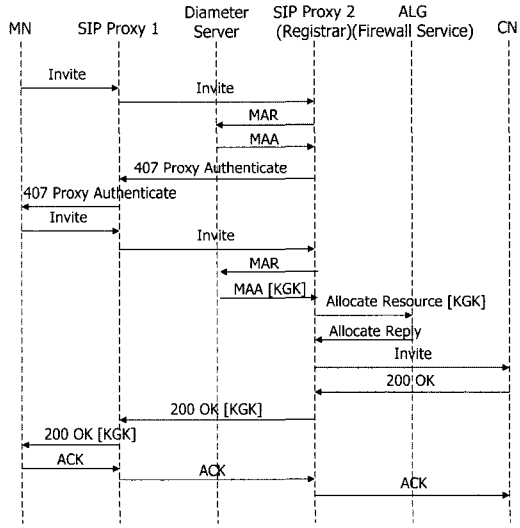
2. SIP 기반 모바일 VPN

SIP는 어플리케이션 계층에서 실시간 데이터를 전송하기 위한 시그널링 프로토콜로 널리 사용되고 있다. 모바일 VPN에서는 VoIP(Voice over IP)와 같은 실시간 데이터 전송 어플리케이션을 위해 SIP를 사용할 수 있다[7]. SIP 기반 모바일 VPN은 MIP기반 모바일 VPN과 달리 IPsec 터널을 사용하지 않고, 그룹키 알고리즘인 MIKEYing(Multimedia Internet KEYing)과 RTP(Real Time Protocol) 패킷 암호화 알고리즘인 SRTP를 이용하여 데이터의 무결성과 기밀성을 보장한다.

그림 5는 SIP 기반 모바일 VPN 구조를 나타내며, 그림 6은 그림 5에서 예로 든 SIP기반 모바일 VPN 구조에서 MN이 외부 네트워크 1로 이동했을 때의 메시지 흐름을 나타낸다. 먼저, MN은 외부 네트워크 1로 이동하게 되면 INVITE 메시지를 통해 외부 네트워크에서 할당받은 새로운 접촉주소(contact address)를 SIP 프록시 서버 1을 거쳐 SIP 등록서버(Registrar)인 SIP 프록



〈그림 5〉 SIP 기반 모바일 VPN 구조

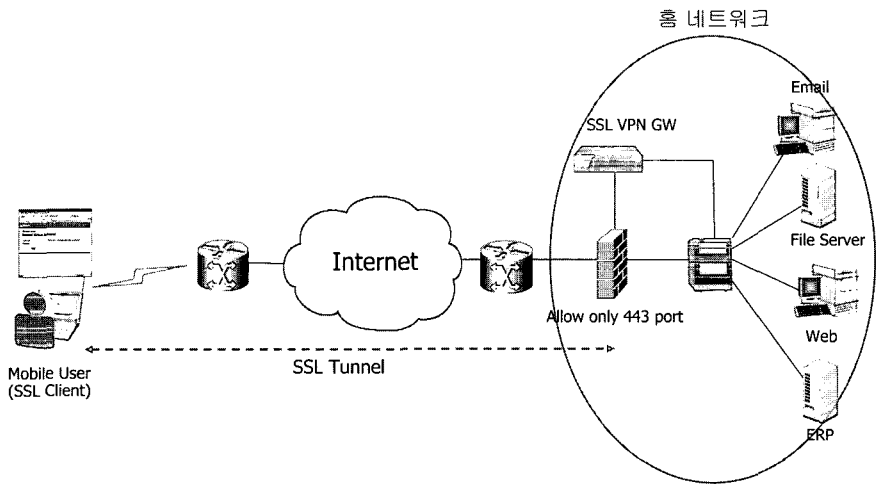


〈그림 6〉 SIP 기반 모바일 VPN에서의 메시지 흐름

시 서버(Proxy Server) 2에 등록한다. SIP 등록서버는 INVITE 메시지를 받은 후 Diameter를 사용하여 INVITE 메시지를 보낸 MN의 인증을 시도한다. Diameter 서버는 MN의 인증 결과와 함께 SDP(Session Description Protocol)를 이용하여 KGK(Key Generation Key)를 SIP 등록서버에 전달한다. 이를 전달받은 SIP 등록서버는 ALG(Application Level Gateway)에게 자원예약 명령어(resource reservation command)를 이용하여 KGK를 전달하고, 또한 MN에게 SDP를 이용하여 인증 결과와 함께 KGK를 전달한다. ALG와 MN이 전달받은 KGK는 그룹키 알고리즘인 MIKEYing 알고리즘에 의해 생성되는 키로 KEK(Key Encryption Key)를 만들어내기 위한 키이다. KEK는 일정 세션동안 데이터를 암호화, 복호화하는 데 사용되는 키이다. MN이 SIP 메시지인 200 OK를 통해 KGK를 획득하면 이에 대한 응답으로 CN에게 ACK를 보내어 시그널링 과정을 완료한다.

실제 데이터는 시그널링 메시지와 달리 MN에서 ALG를 거쳐서 CN으로 전송되는데, 이 때 ALG는 홈 네트워크의 게이트웨이 역할을 수행하고, 외부로 이동한 MN과 ALG간 데이터는 KEK를 통해 암호화되어 전송되므로 MN과 CN간의 안전한 통신을 보장받는다.

SIP 기반 모바일 VPN의 대표적인 특징 중 하나는 MIP 기반 모바일 VPN을 사용할 때 발생하는 트라이앵글 라우팅 문제(triangular routing problem)가 일어나지 않으므로 데이터 전송 지연시간을 줄일 수 있다는 점이다. 뿐만 아니라, IPsec 헤더에 의한 오버헤드가 줄어들기 때문에 무선 구간에서의 데이터 전송 성능도 향상된다. 그러나 SIP 기반 모바일 VPN에서도 여전히 핸드오프 지연시간이 길어질 수 있다는 문제는 발생한다. MN이 이동하여 새로운 접촉 주소를 획득하면 이를 SIP 등록 서버에 등록하고 CN을 re-INVITE하는 과정을 수행하므로 핸드오프 지연시간이 발생하는데 이 때 SIP 등록서버와 MN과의 거리가 멀어지면 핸드오프 지연시간이 더욱 길어질 수 있기 때문이다.



〈그림 7〉 SSL 터널을 이용한 모바일 VPN 구조

3. SSL 터널을 이용한 모바일 VPN

IPsec 터널은 IP 계층에서 터널링을 수행하는 데 반해 SSL 터널은 어플리케이션 계층에서 터널링을 수행한다. SSL(Secure Socket Layer)은 웹 서버와 웹 브라우저 간에 안전한 통신을 제공하기 위한 보안 표준 프로토콜로 현재 사용되고 있는 일반적인 웹 브라우저에 기본적으로 탑재되어 SSL 클라이언트와 서버 간에 상호 인증을 수행하고 SSL 터널을 설립한다. 모바일 VPN 서비스를 제공하는 데에 이러한 SSL 터널이 사용될 수 있다.

그림 7은 SSL 터널을 이용한 모바일 VPN 구조를 보여준다. 이러한 구조를 기반으로 모바일 VPN을 사용하기 위해 외부로 이동한 사용자는 먼저, 자신의 ID와 패스워드를 이용하여 SSL VPN 게이트웨이에게 인증을 시도한다. 인증이 성공적으로 이루어지면 사용자는 SSL 클라이언트로써 세션키를 획득하게 된다. SSL 클라이언트가 홈 네트워크 내의 어플리케이션 서버와 통신하기 위해서는 우선, 획득한 세션키로 자신과 SSL VPN 게이트웨이 간에 SSL 터널을 맺고, SSL VPN 게이트웨이에서 디터널(Detunnel)된 후 통신하고자 하는 해당 어플리케이션 서버에 접속하여 원하는 서비스를 제공받는다.

SSL 터널을 이용한 모바일 VPN은 사용자 디바이스에 IPsec과 같은 모듈을 별도로 추가하지 않고 SSL을 탑재한 웹 브라우저를 통해 제공되는 클라이언트리스(Clientless) 서비스이기 때문에 사용자의 부담이 적어진다. 또한 어플리케이션 계층에서 암호화를 제공하기 때문에 IPsec 터널을 이용한 MIP 기반 모바일 VPN에서 일어나는 VPN 게이트웨이를 통과하는 데 일어나는 비호환성 문제도 일어나지 않는다. 그러나 어플리케이션 계층에서 암호화가 이루어지기 때문에 하위 계층에서 사용하는 프로토콜에도 제약을 받으며 사용할 수 있는 어플리케이션 종류에도 제약이 있다.

4. 그 외의 모바일 VPN 관련 이슈

지금까지, 모바일 VPN 서비스를 제공하기 위

해 필수적으로 요구되는 사용자 이동성과 데이터 전송의 안정성을 지원하는 방안들에 대하여 기술하였다. 그 밖에도 모바일 VPN 서비스를 제공하기 위해서는 이종망간 연동, QoS (Quality of Service) 제공 등과 같은 이슈에 대한 고려가 필요하다.

사용자가 인트라넷을 벗어나서 경험할 수 있는 외부 네트워크는 지사의 LAN, 무선 네트워크(WLAN Network), 셀룰러 네트워크(Cellular Network) 등 여러 접속 네트워크가 존재하므로 사용자는 외부로 이동하였을 때 어떠한 네트워크로 이동하던지 관계없이 자신이 원하는 모바일 VPN 서비스를 지속적으로 받을 수 있어야 한다. 그러기 위해서 모바일 VPN 서비스에서 이종망간 연동에 대한 고려가 필요하다. 대표적인 이종망인 무선 네트워크와 셀룰러 네트워크 간의 연동 방법으로는 타이트 인터워킹(Loose Interworking)과 루즈 인터워킹(Tight Inteworking)이 있다. 타이트 인터워킹은 무선 네트워크와 셀룰러 네트워크 간에 직접적인 인터페이스를 가지도록 하여 두 네트워크 간 직접 데이터 전송을 수행하는 연동 구조이다. 반면, 루즈 인터워킹은 별도로 존재하는 무선 네트워크와 셀룰러 네트워크가 인터넷을 통해 상호 연동되는 구조로 주로 가입자 관리 수준의 연동을 통해 AAA(Authentication, Authorization, Accounting) 서비스와 MIP를 이용한 이동성을 제공한다. 루즈 인터워킹으로 구현된 모바일 VPN 서비스는 서비스 제공자에게 기존 망을 그대로 사용하도록 하여 초기 투자 부담을 줄일 수 있다.

MN이 이종망간 핸드오버를 수행하면 핸드오프 지연시간이 발생하는데 핸드오프를 수행하는 동안 전송된 패킷은 손실될 수 있다. 이 문제를 해결하기 위해 [8]에서 make-before-break 방식이 제안되었는데 이는 이동할 네트워크와 연결을 마친 후, 이전 네트워크와의 연결을 해지하는 방법이다. 제안된 make-before-break 방식을 이용하여 패킷 손실 없이 데이터를 전달 받는다 하여도 셀룰러 네트워크에서 무선 네트워크로 이동하는 경우, 셀룰러 네트워크에서의 패킷 전송 속도가 무선 네트워크보다 느리기 때문에 전송된 패킷 순서가 올바르지 않을 수 있으므로 이를 보완하는 메커니즘이 필요하다.

모바일 VPN 서비스 제공을 위한 대표적인 이슈 중 또 다른 하나는 QoS 지원이다. 모바일 VPN에서 QoS지원을 위해서는 기존의 IP-VPN에서 QoS 지원을 위해 사용하던 Diffserv 또는 RSVP 메커니즘을 사용할 수 있다. Diffserv는 트래픽을 몇 개의 클래스로 구분하고, 클래스 기반으로 서로 다른 QoS를 지원하는 방법이고, RSVP는 Intserv기반으로 QoS를 제공하는 방법 중 하나로 특정 어플리케이션의 데이터 플로우별로 데이터 경로 상의 각 노드에 자원을 예약하고 QoS를 제공하는 방법이다. 유선 IP-VPN과 달리 모바일 VPN에서는 사용자가 이동하므로 사용자 이동성을 고려하도록 기존의 QoS 프로토콜을 수정하여 사용해야 한다[9].

III. 결 론

본론에서 소개한 IPsec 터널을 이용한 MIP 기반 모바일 VPN과 SIP 기반 모바일 VPN, SSL 터널을 이용한 모바일 VPN은 대부분 사용자 기반 모바일 VPN이다. 서론에서 언급한 바와 같이 IPsec 터널을 이용한 MIP 기반 모바일 VPN 중에서 의무적(Compulsory)터널을 구성하는 경우도 존재하나 이는 MN과 VPN 게이트웨이 간에 형성되는 IPsec 터널의 형태에 따른 구분이므

로 완전한 네트워크 기반의 모바일 VPN이라고 볼 수는 없다. 지금까지 모바일 VPN에 관한 연구가 이렇게 사용자 기반 모바일 VPN으로 활발히 이루어진 이유는 모바일 VPN에서 통신 형태가 외부에 존재하는 개개의 MN이 홈 네트워크 내의 CN과 통신하는 방식으로 원격 접속(Remote Access) VPN 서비스와 유사했기 때문이다. 그러나 무선 네트워크의 진화와 함께 MN이 급속히 증가하고 있는 현재 추세로 보아 모바일 VPN 서비스를 이용하는 사용자의 통신 형태에도 변화가 예상된다. 예를 들어 외부 네트워크로 이동한 MN들이 동적으로 VPN 사이트를 형성하거나 VPN 사용자들이 모바일 네트워크를 형성하여 이동하는 형태의 통신이 있을 수 있다. 이러한 형태의 통신에 있어서 VPN 고객의 관리자가 직접 VPN을 관리하고 유지하는 것은 VPN 고객에게 큰 부담이 될 수 있다. 따라서 서비스 제공자가 VPN을 관리하고 유지하는 형태인 PPVPN(Provider Provisioned VPN) 개념을 모바일 VPN 서비스를 제공하기 위해 확장하는 것이 필요하다.

또한, 지금까지 모바일 VPN 서비스는 외부로 이동한 사용자가 홈 네트워크인 인트라넷 내의 CN과 안전하고 효율적인 통신을 지원하는 것이 대부분이었다. 그러나 통신하고자 하는 두 사용자가 모두 외부 네트워크에 존재하는 경우에도 모바일 VPN 서비스가 지원되어야 한다. 이런 경우, 일반적인 MIP 기반 모바일 VPN을 사용하면 홈 네트워크 내의 HA를 통해서 CN으로 데이터가 전송되는 트라이앵글 라우팅(triangular routing)이 발생한다. 이는 데이터 전송 지연시간이 길어지는 원인이 되므로 두 사용자 간에 직접 통신이 이루어져 데이터 전송 지연시간을 줄일 수 있도록 하는 방안에 대한 연구가 필요하다.

참고 문헌

[1] F. Adrani, H. Levkowerz, "Problem statement: Mobile IPv4 Traversal of Virtual Private Network Gateways", RFC 4093, August 2005.

[2] S. Vaarala, E. Klovning, "Mobile IPv4 Traversal Across IPsec-based VPN gateways", Internet Draft, November 2005

[3] Yi-Wen Liu, Jyh-Chen Chen, Li-Wei Lin, "Dynamic External Home Agent Assignment in Mobile VPN", VTC2004-Fall., 2004 IEEE 60th, Vol. 5, pp. 3281-3285, Los Angeles, USA, 26-29 September 2004.

[4] Berioli, M., Trotta, F., "IP Mobility Support for IPsec-based Virtual Private Networks: an architectural solution", Global Telecommunications Conferences, 2003. GLOBECOM '03. IEEE, Vol 3. pp. 1532-1536, San Francisco, USA, 1-5 December 2003.

[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] H. Ohnishi, K. Suzuki, Y. Takagi, "Mobile IPv6 VPN using Gateway Home Agent", Internet Draft, October 2002.

[7] Shun-Chao Huang, Zong-Hua Liu, Jyh-Cheng Chen, "SIP-Based Mobile VPN for Real-Time Applications", Wireless Communications and Networking Conference, 2005 IEEE, Vol. 4, pp. 2318-2323, New Orleans, USA, 13-17 March 2005.

[8] Feder, P.M., Lee, N.Y., Martain-Leon, S., "A Seamless Mobile VPN Data Solutions for CDMA2000, UMTS, and WLAN Users", 3G Mobile communication Technologies, 2003., 4th International Conference on (Conf. Publ. No. 494), pp. 210-216, London, UK, 25-27 June 2003.

[9] H. Chaskar., "Requirements of Quality of Service Solution for Mobile IP", RFC 3583, September 2003.

저자소개

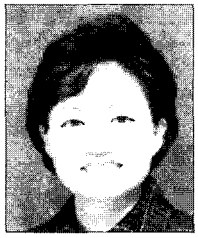
김 경 민

2001년 - 2005년 이화여자대학교 컴퓨터학과 학사
2005년 - 현 재 이화여자대학교 대학원 컴퓨터학과 석사과정
주관심분야 Mobile VPN, VPN, 인터넷 Qos 지원, 무선 네트워크

변 해 선

1997년 - 2001년 광주대학교 컴퓨터학과 학사
2001년 - 2003년 이화여자대학교 과학기술대학원 컴퓨터학과 석사
2003년 - 현 재 이화여자대학교 과학기술대학원 컴퓨터학과 박사과정
주관심분야 광대역 통합망, VPN, 모바일 VPN, 인터넷에서의 QoS 지원

저자소개



이 미 정

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