외부 네트워크 내 사용자 간 모바일 VPN 지원 방안

김경민° 변해선 이미정
이화여자대학교 컴퓨터학과
{kmk°, ladybhs}@ewhain.net, lmj@ewha.ac.kr

Mobile VPN service for the users in foreign networks

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

요 약

지금까지 모바일 VPN 서비스는 모바일 VPN 사용자가 사내 네트워크 내 CN과 통신하는데 중점적으로 사용되었으나, 모바일 VPN 서비스 사용자가 급증함에 따라 CN이 사내 네트워크 내의 개체가 아닌 외부 네트워크로 이동한 또 다른 모바일 VPN 사용자가 되는 상이한 통신 형태에 대한 모바일 VPN 서비스 지원이 필요해졌다. 기존의 모바일 VPN 서비스를 이러한 형태의 통신에 적용할 경우, 트라이앵글 라우팅 문제로 인하여 효율적인 서비스 지원이 어려워진다. 이에, 본 논문에서는 경로 최적화를 통해 x-HA만을 거치는 라우팅을 제공하고, 변화한 라우팅 경로를 따라 앤드-투-앤드 보안을 효율적으로 제공하기 위해 각 모바일 VPN 사용자가 등록한 x-HA간에 IPsec 터널을 설립, 활용하는 방안을 제시한다.

1. 서 론

VPN(Virtual Private Network) 서비스는 인터넷과 같은 공중망을 이용하여 사설망을 구축하는 기술로 기업 사설망의 보완 혹은 대치 수단으로 널리 사용되고 있다. 그러나 기존의 VPN 서비스는 본점과 지점을 잇는 유선망을 토대로 개발되었으므로, 급증하고 있는 기업 내 모바일 사용자의 VPN 서비스 지원에 미흡하였다. 이에, MIP(Mobile IP)와 같은 이동성 지원 프로토콜과 IPsec(IP Security), SSL(Socket Security Layer)과 같은 터널링 및 암호화 기법을 토대로 모바일 사용자에게 안전한 데이터 전송을 지원하는 모바일 VPN 서비스에 대한 연구가 활발히 진행되었다.

지금까지 연구된 대부분의 모바일 VPN 서비스는 외부 네트워크로 이동한 MN(Mobile Node)과 사내 네트워크인 홈 네트워크(Home Network)에 존재하는 CN(Correspondent Ndoe) 간의 안전한 통신을 지원하는 것으로, 원격 접속 방식의 VPN 서비스와 유사한 형태를 지닌다. 즉, 원격 접속자에 해당하는 MN이 외부 네트워크로 이동하면 MN 자신과 홈 네트워크의 VPN 게이트웨이 사이에 터널을 설립하고, 이 터널을 통해 홈 네트워크 내 CN과 통신함으로써 데이터 전송의 안정성을 보장 받는 형태이다. 이 중, 가장 대표적인 방안은 IPsec(IP Security) 터널을 이용한 MIP기반 모바일 VPN이다. 그러나 이 방안의 경우, 이동성 지원 프로토콜인 MIP와 보안 프로토콜인 IPsec을 동시에 사용하는 데 있어 CoA 모드에 따라 여러 문제가 발생한다[1]. 먼저, MIP에서 CoA(Care-of-Address)로 FA-CoA를 사용하는 경우, FA에서 IPsec으로 암호화 된 MIP 등록 메시지를 복호화 하지 못하여 FA(Foreign Agent)에서 MIP 등록에 실패하는 문제가 발생하는데, 이를 해결하기 위한 방안으로는 x-HA(External Home Agent)를 사용하는 방안이 제시되었다[2,3]. 반면, CoA로 Co-CoA를 사용하는 경우, IPsec 종단 주소 변경에 따라 잦은 IPsec 터널 재설립 문제가 발생하게 되는데, 이를 해결하기 위해서는 IPsec에 이동성을 지원하는 표준 프로토콜인 MOBIKE(IKEv2 Mobility and Multihoming)를 사용하는 방안이 제시되었다[8]. 이에 관한 좀 더 구체적인 내용은 2장 관련 연구에서 기술하였다.

그런데, 이들 기존의 모바일 VPN 서비스 방안들은 CN이 홈 네트워크 내에 존재하는 특정 통신 형태를 전제로 하였으나, 모바일 VPN 사용자가 증가함에 따라 사용자가 요구하는 통신 형태는 더욱 다양해질 것으로 예상된다. 그 중, MN과 CN이 모두 외부 네트워크에 존재하는 통신의 경우, 기존의 모바일 VPN 서비스 방안을 사용하면 일반적으로 라우팅 경로가 길어지므로 서비스 효율이 떨어지는 문제가 발생한다.

이에, 본 논문에서는 MN과 CN이 모두 외부 네트워크에 존재하는 경우에 대해 효율적인 모바일 VPN 서비스 제공 방안을 제안 한다. 제안하는 방안은 보안 강화를 위하여 앤드-투-앤드(End-to-End) 보안을 제공하고, 효율적인 서비스 제공을 위하여 경로 최적화(Route Optimization)를 통한 빠른 데이터 전송 제공을 목표로 한다. 또한, CN이 홈 네트워크에 존재하는 기존의 모바일 VPN 서비스도 동시에 지원하는 것을 전제로 한다.

본 논문의 구성은 다음과 같다. 1장의 서론에 이어, 2장에서는 지금까지 연구되어 온 모바일 VPN 관련 연구에 대하여 소개한 후, 이를 토대로 3장에서 제안하는 방안을 기술하고, 4장에서 결론과 함께 향후 연구 과제를 제시한다.

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

2. 관련 연구

본 장에서는 제안하는 방안의 기초가 되는 x-HA를 사용한 MIPv4 기반 모바일 VPN에 대하여 설명한다.

x-HA는 모바일 VPN에서 MIP 프로토콜과 IPsec 프로토콜을 동시에 사용하는 데에서 발생하는 비호환성 문제를 해결하기 위해 도입된 개체로, 외부 네트워크 내에서 MN에 대한 이동성 지원을 담당하는 HA(Home Agent)이다[2]. x-HA는 할당 방식에 따라 정적 x-HA와 동적 x-HA로 나뉜다. 정적 x-HA는 MN이 외부 네트워크로 이동하기 전에 미리 결정되어 진 x-HA이며, 동적 x-HA는 MN이 외부 네트워크로 이동하였을 때 DHCP, DNS, AAA 등을 통해 동적으로 할당 받는 x-HA이다.

정적 x-HA를 사용하는 모바일 VPN은 외부 네트워크 내에 고정된 하나의 x-HA를 사용하므로, 외부 네트워크로 이동한 모든 모바일 VPN 사용자의 CoA를 x-HA가 자신의 바인딩 캐쉬 내에 유지하게 된다. 그러나 이 경우, 하나의 x-HA가 외부 네트워크에 있는 모든 MN의 이동성을 지원해야 하므로 x-HA가 가지는 오버로드가 커진다. 뿐만 아니라 MN의 위치가 x-HA에서 멀어지게 되면, 핸드오프 및 데이터 전송 지연 시간이 그만큼 길어지게 된다.

이에 비해 동적 x-HA를 사용하는 모바일 VPN의 경우, Diameter MIP를 통해 MN과 가까운 곳에 위치한 x-HA를 할당 받게 되므로 핸드오프 및 데이터 전송 지연 시간이 단축된다[3]. 그러나 동적 x-HA를 사용하여도, MN과 x-HA의 거리를 좁혀 전체적인 데이터 전송 시간을 줄일 수는 있으나 *x-HA*와 *i-HA*를 거쳐 통신이 이루어지는 트라이앵글 라우팅(Triangular Routing) 문제는 해결하지 못한다.

그런데, 트라이앵글 라우팅 문제는 CN이 외부 네트워크로 이동한 모바일 VPN 사용자일 경우, 홈 네트워크 내에 CN이 존재하는 경우에 비해 문제의 심각성이 더욱 커진다.

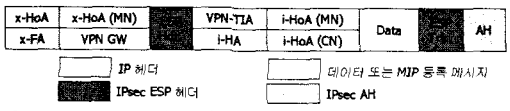

그림 1. x-HA를 사용하는 MIP 기반 모바일 VPN에서 MN이 작성한 데이터 패킷

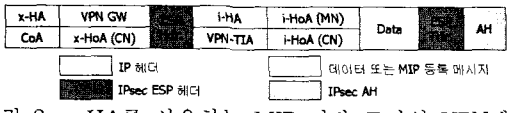

그림 2. x-HA를 사용하는 MIP 기반 모바일 VPN에서 CN이 받는 데이터 패킷

그림 1은 x-HA를 사용하는 MIP 기반 모바일 VPN에서 외부로 이동한 모바일 VPN 사용자 중 하나인 MN이 다른 모바일 VPN 사용자 CN에게 전송하기 위해 작성한 데이터 패킷 포맷이다. MN은 통신 상대인 CN이 외부 네트워크로 이동한 사실을 모르기 때문에 그림 1의 가장 안 쪽 IP헤더에서 볼 수 있듯이 자신의 i-HoA를 소스 주소로 하고 CN의 i-HoA를 목적지 주소로 하는 데이터 패킷을 전송한다. 작성된 데이터 패킷은 i-MIP, IPsec, x-MIP 터널을 통해 i-HA로 전달된다. 데이터 패킷을 전달받은 i-HA는 자신의 바인딩 캐쉬에서 CN의 i-HoA에 대한 바인딩 엔트리를 찾음으로써 CN이 외부 네트워크에 있음을 인지하게 된다. 이 때, CN은 모바일 VPN의 한 사용자이므로 i-HA에 등록된 CN의 CoA는 CN이 VPN 게이트웨이와 맺은 IPsec에 대한 VPN-TIA이다. 그러므로 i-HA는 이를 CN에게 전달하기 위해 VPN-TIA를 목적지 주소로 하는 i-MIP 터널을 사용하여 패킷을 관련 VPN 게이트웨이로 전달하고, VPN 게이트웨이는 이 패킷에 해당 IPsec을 적용하여 외부 네트워크로 내보낸다. x-HoA의 라우팅 정보에 따라 x-HA로 전달된 패킷은 x-HA가 가진 바인딩 정보, 즉 CN의 실제 CoA에 의해 CN에게 전달한다. 그림 2는 CN이 전달받은 데이터 패킷 포맷을 나타낸다.

위 과정을 거치는 동안, MN이 작성한 패킷은 i-HA로 전달되는 동안에 2번, i-HA에서 외부의 CN으로 전달되는 동안에 2번의 트라이앵글 라우팅을 경험하므로 CN이 홈 네트워크에 존재하는 경우에 비해 더 긴 데이터 지연 시간을 가지게 된다. 이는 전체적인 모바일 VPN의 성능을 저하시킨다.

그러므로 이러한 트라이앵글 라우팅을 해결하기 위해 경로 최적화가 지원되어야 한다. 경로 최적화란, 통신 상대 간에 직접 통신이 가능하게 하는 메커니즘으로, MIP에서 HA가 제공하는 BU(Binding Update) 메시지를 통하여 CN이 통신 상대인 MN의 CoA를 획득하고, 이를 자신의 바인딩 캐시에 유지함으로써 MN과 직접 통신하는 것을 말한다.

x-HA를 사용하는 MIP 기반 모바일 VPN에서는 HA 기능을 하는 개체로 i-HA와 x-HA가 존재하며 두 개체 모두 경로 최적화를 위해 통신 상대의 CoA를 제공하는 주체가 될 수 있다. 그러나 각 HA에 등록된 CoA의 종류가 다르므로 어떤 HA를 이용하여 경로 최적화를 지원하느냐에 따라 다른 결과를 가져오게 된다.

먼저, i-HA를 이용한 경로 최적화 지원의 경우, *x-HA의 할당 방식에 따라 i-HA가 가지는 CoA*가 달라지므로 이에 따른 경로 최적화 지원 결과도 달라진다.

정적 x-HA를 사용하는 모바일 VPN에서 i-HA는 MN의 CoA로써 각 MN이 VPN 게이트웨이와 IPsec 터널을 맺을 때 VPN 게이트웨이로부터 할당받은 VPN-TIA를 지닌다. 그러므로 MN이 경로 최적화를 통해 외부 네트워크로 이동한 모바일 VPN 사용자 중 하나인 CN에 대한 CoA를 요청했을 때, i-HA로부터 얻게 되는 주소는 실제로 CN의 VPN-TIA이다. 그러므로 MN은 경로 최적화를 적용하더라도 항상 홈 네트워크의 VPN 게이트웨이를 거쳐 CN에게 데이터를 전송하게 된다.

반면, 동적 x-HA를 사용하는 모바일 VPN에서 i-HA는 각 MN의 x-HoA를 CoA로 유지하고 있으며, MN이 CN의 CoA로써 이를 제공받을 경우, 데이터가 CN의 실질적인 CoA가 등록된 x-HA를 거쳐 전송되므로 정적 x-HA를 사용하는 방안에 비해 라우팅 측면에서 효율적이다.

그러나 이와 같이 i-HA에 CoA로 x-HoA를 가지는 경우, 홈 네트워크 내 여러 VPN 게이트웨이가 존재하게 되면, 패킷이 MN과 IPsec을 맺지 않은 다른 VPN 게이트웨이를 통해 x-HA로 전달될 수 있다. 이 경우, MN으로 전송되는 데이터는 IPsec 암호화에 실패하게 되므로 i-HA에서 CoA로 VPN-TIA를 가지는 경우에 비해 보안이 취약해진다.

마지막으로 모바일 VPN에서 x-HA를 통해 경로 최적화를 지원하는 경우, 정적 x-HA와 동적 x-HA 모두 CN의 실제 CoA를 바인딩 정보로 지니므로 라우팅 측면에서 효율적인 지원이 가능하다. 그러나 이 경우, MN과 CN간에 안전한 데이터 전송을 위해 설립된 IPsec의 종단 주소로 MN과 CN의 CoA가 사용되어지므로 IPsec 터널 재설립 문제가 발생하며, CN이 홈 네트워크 내에 존재할 때와 달리 MOBIKE를 통한 해결이 불가능해진다. 그 이유는 MN과 CN이 모두 모바일 노드로 CoA의 동시 변경이 이루어질 수 있는데, MOBIKE가 IPsec의 종단 주소가 동시 변경되는 경우에 대해 지원되지 않기 때문이다. 이 외에도, 동적 x-HA를 사용한 모바일 VPN에서는 MN과 CN이 등록된 x-HA가 서로 달라 아예 경로 최적화 지원에 실패할 수도 있다.

3. 제안하는 방안

본 논문에서는 2장에서 언급한 문제들을 고려하여, 외부 네트워크 내 CN과 통신하는 MN에게 가장 효율적인 경로 최적화를 제공하는 방안을 제안한다. 제안하는 방안은 정적 x-HA를 사용할 때 발생하는 핸드오프 및 데이터 전송 지연시간을 줄이고, x-HA가 홀로 감당해야 하는 오버로드를 줄이기 위해 동적 x-HA를 사용한 모바일 VPN을 토대로 한다. 그림 3은 제안하는 방안의 네트워크 구조를 표현한 그림이다.

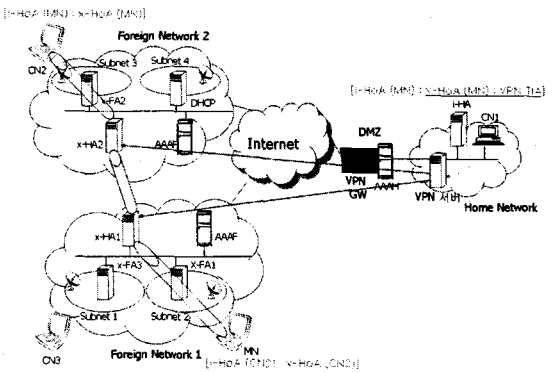

그림 3. 경로 최적화를 지원하는 모바일 VPN 구조

그림 3에서 MN과 CN2는 서로 다른 x-HA에 등록된 모바일 VPN 사용자를 나타낸다. MN이 CN2와 통신하고자 할 때, MN을 지원하는 x-HA1는 CN2를 지원하는 x-HA가 아니므로 CN2에 관한 바인딩 정보를 가지고 있지 않는다. 그러므로 MN은 x-HA1을 통해 CN2에 대한 경로 최적화 지원을 받을 수 없다.

제안하는 방안에서는 이렇듯 x-HA에서 해당 노드의 바인딩 정보 부재로 경로 최적화 지원에 실패하는 것을 막기 위해 경로 최적화를 지원하는 HA를 외부 네트워크에 존재하는 모든 모바일 VPN 사용자의 바인딩 정보를 유지하고 있는 i-HA로 한정한다.

또한, 홈 네트워크 내에 여러 VPN 게이트웨이를 사용하는 상황을 고려하여 i-HA에서 가지는 CoA는 VPN-TIA로 하되, 경로 최적화 지원이 요청되었을 때, CN의 위치에 따라 적합한 CoA를 선별하여 제공하는 메커니즘을 제공한다. 이를 위해 MN은 외부 네트워크로 이동하여 VPN 게이트웨이와 IPsec 터널을 맺을 때, i-HA에 MN의 CoA로써 VPN-TIA를 등록하고, x-HoA는 자신에 대한 추가적인 바인딩 정보로 i-HA가 유지하게 한다. 다시 말해, 하나의 MN에 대해 i-HA는 {i-HoA, x-HoA, VPN_TIA}의 튜플을 바인딩 정보로 가진다.

이 후, i-HA는 외부 네트워크로 이동한 MN으로부터 경로 최적화 요청이 들어오게 되면 통신 형태에 따른 적합한 CoA를 제공하기 위해 CN의 위치 판정을 수행하고, 그 결과에 따라 경로 최적화를 지원하는 메시지를 작성한다. 그림 4는 그 과정을 순서도로 표현한 것이다.

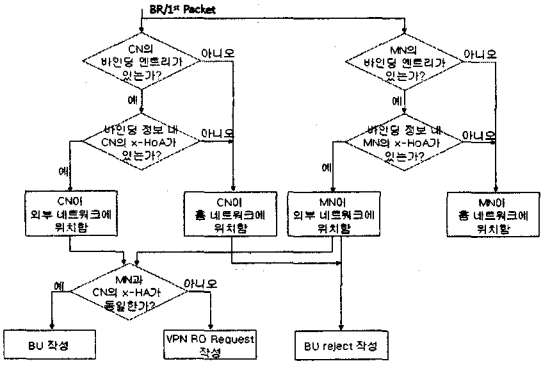

그림 4. i-HA에서의 경로 최적화 관련 메시지 작성 과정

MN에 의해 경로 최적화 지원이 요청되면, i-HA는 먼저 자신의 바인딩 캐쉬에서 CN에 대한 바인딩 엔트리 존재 여부를 검색한다. 바인딩 엔트리가 존재하지 않으면, 이는 CN이 홈 네트워크에 존재하는 고정 노드임을 나타내며, 바인딩 엔트리가 존재하는 경우, 이는 CN의 위치에 상관없이 CN이 모바일 노드임을 의미한다.

바인딩 엔트리가 존재했을 때 i-HA는 다음으로, 바인딩 정보 중 x-HoA의 존재 여부를 확인하여 모바일 노드인 CN의 위치를 판정한다. 만일 CN의 x-HoA가 존재한다면 이는 CN이 외부 네트워크로 이동한 모바일 VPN의 한 사용자임을 나타낸다. CN은 x-HA를 할당받을 때 자신의 x-HoA를 i-HA에 바인딩 정보로 등록해 두기 때문이다. 이와 달리, CN의 바인딩 엔트리가 존재하나 바인딩 정보 내에 x-HoA가 없다면 이는 CN이 홈 네트워크 내에 존재하는 모바일 노드임을 나타낸다.

판정 결과에 따라 MN은 외부 네트워크에 있으나 CN이 홈 네트워크 내에 있다면 i-HA는 BU 메시지에 경로 최적화 지원 거절하기 위해 Lifetime을 0으로 세트하여

MN에게 전달한다. 외부 네트워크에 있는 MN이 홈 네트워크 내에 있는 CN과 통신하기 위해서는 항상 VPN 게이트웨이를 거쳐야 하기 때문이다.

이와 달리 MN과 CN이 모두 외부 네트워크에 존재한다면 i-HA는 BU 메시지에 CN의 CoA로 x-HoA를 기입하여 MN에게 전달함으로써 경로 최적화를 지원한다.

그림 3에서 MN이 i-HA에게 CN2에 대한 최적화를 요청한 경우, MN은 위 과정을 통해 CN2의 x-HoA를 CN2의 CoA로 획득하고, x-HA2를 거쳐 CN2와의 통신을 계속하게 된다. 이는 VPN 게이트웨이를 거치는 라우팅에 비해 경로가 짧기 때문에 더 빠른 데이터 전송이 가능하다.

그런데, MN이 경로 최적화를 통해 CN2와 통신하게 되면 달라진 라우팅 경로 때문에 VPN 게이트웨이와 맺은 기존의 IPsec 터널을 사용할 수 없게 된다. 그러므로 안전한 통신을 보장하기 위해서는 통신 상대인 CN2와 새로운 IPsec 터널을 설립해야 한다.

이 때, MN은 CN2의 x-HoA와 자신의 x-HoA을 종단 주소로 하여 앤드-투-앤드로 IPsec 터널을 설립할 수 있다. 그러나 이러한 방법은 보안 측면은 강화할 수 있으나, 무선 구간에서 MN이 감당해야 하는 IPsec에 대한 오버헤드를 증가시킨다.

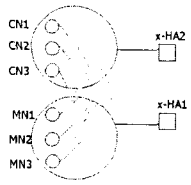

그림 5 (가). 두 MN간 직접 IPsec 터널 설립

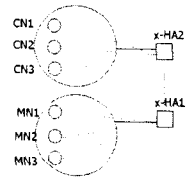

그림 5 (나). MN과 x-HA간 IPsec 터널 설립

그림 5. (가)는 이러한 예를 단적으로 보여준다. 그림 5. (가)에서 MN1은 한 외부 네트워크 내의 CN1, CN2, CN3과 동시에 통신을 진행하고 있으며 x-HoA를 이용하여 통신하고 있는 CN 수만큼의 IPsec 터널을 설립한다. 그런데, CN이 외부 네트워크에 존재하는 통신은 CN이 홈 네트워크에 존재하는 통신에 비해 일반적으로 더 많은 무선 구간을 경험한다. 무선 구간은 유선 구간에 비해 자원 이용에 민감하므로, CN이 외부 네트워크에 존재하는 환경에서 한 MN이 통신하고 있는 CN 수만큼 IPsec 터널을 설립, 유지하는 것은 모바일 VPN 서비스의 전체적인 성능을 저하시킬 수 있다.

그러므로 이를 해결하기 위해 그림 5. (나)와 같이 x-HA를 활용하여 MN이 설립하는 IPsec 터널의 수를 줄이는 방안을 제안한다.

제안하는 방안에서 MN은 외부 네트워크로 이동한 CN과 경로 최적화를 통한 통신을 시작하기에 앞서, 자신이 등록되어 있는 x-HA와 IPsec 터널을 설립해 두고, 이를 활용하여 외부 네트워크 내 CN과 안전한 통신을 지원한다. 그림 5. (나)에서 MN1과 MN2간 통신과 같이, 동일한 x-HA에 등록된 노드 간 통신이라면, 각 MN이 x-HA와 맺은 IPsec 터널만으로 충분히 데이터 전송의 안전성을 보장받을 수 있다. 그러나 MN1과 CN1간 통신과 같이, 서로 다른 x-HA를 통해 지원되는 MN간 통신은 각 MN과 이를 지원하는 x-HA간에 설립된 IPsec 터널만으로는 앤드-투-앤드 보안을 보장받을 수 없다.

앤드-투-앤드 보안을 제공하기 위해서는 각 노드를 지원하는 x-HA간 추가적인 IPsec 터널 설립이 필요하다. 이를 위해 본 방안에서는 모바일 VPN 서비스 가입자가 관리하는 홈 네트워크 내에 VPN 서버를 두고, 이를 이용하여 해당 x-HA간 IPsec 터널을 설립하는 메커니즘을 제안한다. 제안하는 방안에서 VPN 서버는 자신의 디렉토리 내에 모바일 VPN 서비스를 위해 사용되어지는 x-HA의 IP 주소 정보와 해당 x-HA간에 IPsec SA를 맺는데 필요한 부가 정보를 지니고 있는다[10].

한편, i-HA는 그림 4에 기술한 과정을 통해 MN과 CN이 외부 네트워크에 존재한다고 판별되면, MN과 CN의 x-HoA를 비교하여 두 노드를 지원하는 x-HA가 동일한지 확인한다. x-HA가 동일한 경우, i-HA는 바로 CN의 x-HoA를 CoA로 갖는 BU 메시지를 MN에게 전달하지만, x-HA가 다른 경우, i-HA는 두 x-HA간에 추가적인 IPsec 터널을 설립하기 위해 VPN RO Request 메시지를 작성하여 VPN 서버에게 전달한다. 이 메시지를 받은 VPN 서버는 IKE Nego Request 메시지를 통해 해당 x-HA에 IPsec 터널을 맺기 위한 부가 정보를 전달함과 동시에 IPsec 커널을 구동시켜, x-HA간에 IPsec 터널을 맺도록 한다.

i-HA는 VPN 서버로부터 VPN RO Request 메시지에 대한 응답 메시지를 받기 전까지는 MN에게 경로 최적화를 위한 BU 메시지를 전달하지 않는다. 그 이유는 x-HA간 IPsec 터널 설립이 완성되기 전에 이 경로를 통해 데이터가 전송되는 것을 방지하기 위해서이다.

그림 6은 그림4에서 MN과 외부 네트워크로 이동한 순간부터 CN2와 경로 최적화를 통한 통신이 이루어지까지의 과정을 메시지 흐름과 함께 표현한 것이다.

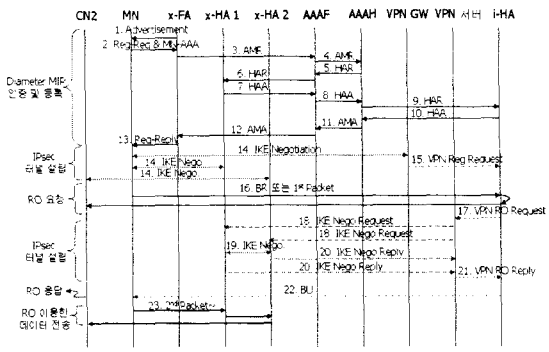

그림 6. 경로 최적화를 지원하는 모바일 VPN에서의 메시지 흐름

그림 6에서 1~14는 MN이 외부 네트워크로 이동하였을 때 Diameter MIP를 통하여 x-HA를 할당받고 VPN 게이트웨이와 IPsec 터널을 설립하는 과정으로, 기존의 동적 x-HA을 사용한 모바일 VPN과 동일하다. 15 이후는 경로 최적화 지원을 위한 과정으로, 이를 지원하기 위한 메시지 흐름을 나타낸다. 기존의 동적 x-HA를 사용하는 방안에서는 MIP 등록 과정에서 외부로 이동한 MN이 홈 네트워크의 VPN 게이트웨이와만 IPsec 터널을 설립하고 있었으나 본 방안에서는 MN이 14와 같이 자신이 등록한 x-HA와 미리 IPsec 터널을 설립하여 외부 CN과의 안전한 통신에 대비한다. 또한 보안 제공의 일관성을 위해 Diameter MIP를 통해 x-HoA로 등록된 i-HA내 MN의 CoA를 VPN-TIA로 갱신하기 위해 VPN 게이트웨이에서 15와 같이 VPN Reg Request 메시지를 작성하여 i-HA에게 알린다. 각 MN이 외부 네트워크로 이동하여 MIP 등록과 초기 IPsec 터널 설립을 완료하면 데이터 전송을 시작하는데, 이 때 MN은 CN2로 보내는 첫 번째 패킷 혹은 BR(Binding Request) 메시지를 통해 i-HA에게 경로 최적화를 요청한다. i-HA는 첫 번째 패킷을 자신의 바인딩 정보를 통해 CN2에게 전달함과 동시에 CN2의 위치를 파악하여 경로 최적화 지원 여부와 추가적인 IPsec 터널 설립 여부를 결정한다. x-HA간 IPsec 터널 설립이 필요하다고 판단하면 VPN 서버에 의해 각 x-HA간 IPsec 터널이 설립되도록 한다. 17~21은 x-HA간 IPsec 터널을 설립하고, 그 결과를 i-HA에게 알리는 과정을 나타낸다. i-HA는 x-HA간 IPsec 터널 설립이 완료됨을 알리는 VPN RO Reply 메시지를 받은 후에야 22와 같이 BU 메시지를 통해 MN에게 CN2의 CoA로 x-HoA를 전달한다. 이로써, 경로 최적화 지원을 위한 모든 과정이 완료된다. 이 후, MN에서 CN2로 전송하는 패킷은 MN과 x-HA1 사이에 설립된 IPsec 터널과 x-HA1과 x-HA2 간에 설립된 IPsec 터널, x-HA2과 CN2 사이에 설립된 IPsec 터널을 거쳐 전달된다.

본 방안에서 MN이 i-HA에게 경로 최적화 지원을 요청하고, i-HA이 이를 지원하는 BU 메시지를 MN에게 제공하기까지는 x-HA간 IPsec 터널 설립 때문에 지연시간이 발생한다. 그러나 이 시간 동안 데이터는 기존의 라우팅 경로를 따라 전송되고 있기 때문에 모바일 VPN 서비스의 전체적인 성능에 큰 영향을 미치지는 않는다.

4. 결론 및 향후 과제

본 방안은 기존의 모바일 VPN 서비스에 대해 확장된 서비스를 제공하고자 외부 네트워크에 존재하는 두 모바일 VPN 서비스 사용자 간에 효율적인 일 대 일 통신을 지원하는 방안을 제안하였다. 제안한 방안에서, i-HA는 경로 최적화를 통해 상대 노드의 x-HoA를 제공하여, 효율적인 라우팅이 가능하게 하고, VPN 서버로 하여금 MN과 CN이 등록한 x-HA간에 IPsec 터널을 설립하도록 한다. MN과 CN은 각자 자신이 등록한 x-HA과 맺은 IPsec 터널과 VPN 서버에 의해 설립된 x-HA간 IPsec 터널을 이용함으로써 주어진 경로에 알맞은 앤드-투-앤드 보안을 제공받는다.

제안하는 방안을 통해 MN과 CN간 데이터 전송 지연시간의 단축과 각 MN이 가지는 무선 구간에서의 오버헤드 감소를 예상하며, 이에 대한 성능을 평가하기 위해 OPNET Modeler 11.0을 사용하여 시뮬레이션을 진행 중이다.

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", draft-ietf-mip4-vpn-problem-solution-02.txt, 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, September 2004

[4] P. Calhoun, T. Johansson, C. Perkins, T. Hiller, P. McCann, "Diameter Mobile IP Application", RFC 4004, August 2005

[5] P. Eronen, "IKEv2 Mobility and Multihoming Protocol (MOBIKE)", RFC 4555, June 2006

[6] Charles Parkins, David B. Johnson, "Route Optimization in Mobile IP", draft-ietf-mobilip-optim-11.txt, September 2001

[7] Fayza A. Nada, "On Using Mobile IP Protocols", 2006 Science Publication, pp. 211-217, 2006

[8] Ashutosh Dutta, Tao Zhang, Sunil Madhani, Kenichi Tanjuchi, Kensaku Fujimoto, Yashuhiro Katsube, Yoshihiro Ohba, Henning Schulzrinne, "Secure Universal Mobility for Wireless Internet", ACM SIGMOBILE Mobile Computing and Communications Review, Vol. 9, Issue 3. July 2005

[9] Choyi, V.K., Barbeau. M, "Low-latency Secure Mobile Communications", Wireless And Mobile computing, Networking And Communications 2005. (Wimob'2005), Vol . 2, pp. 38-42, August 2005

[10] 변해선, 이미정, "성형 VPN 구조에서의 주문형 터널 생성 메커니즘", 한국정보과학회 논문지, 정보통신, Vol. 32, no.4, pp. 452-461, August, 2005