모바일 IP VPN 환경에서의 이동성 지원에 따른 SA 재협상 방지에 관한 연구

준회원 차 정 석*, 김 태 윤* , 정회원 송 주 석*

A Study on Preventing SA Re-negotiation for Mobility Support in Mobile IP VPN Environment

Jeong-Seok Cha*, Tae-Yoon Kim* ***Associate Members,***
Joo-Seok Song* ***Regular Member***

요 약

IPsec을 이용한 remote access VPN구조에서 VPN client가 이동 중에도 지속적인 VPN서비스를 받기 위해서는 Mobile IP와 VPN을 연동하는 기법이 필요하다. 이러한 경우에 VPN client가 새로운 서브넷으로 handoff하면, VPN client는 새로운 CoA를 획득하게 되며, 주소변경으로 인해 기존의 SA를 이용할 수 없고 새롭게 SA를 재협상 해야한다. SA 재협상 과정은 보안적 측면과는 무관하게 발생하며, 단지 VPN client의 이동 때문에 발생하는 문제점이다. 따라서, handoff가 빈번하게 일어나는 환경에서는 SA 재협상으로 인한 오버헤드가 전체성능을 저하시키게 된다. 이 논문에서는 Mobile IP VPN환경에서 VPN client가 handoff를 하더라도, SA를 재협상하지 않고 지속적인 security service를 받을 수 있도록 하는 새로운 기법을 제시하고 분석하였다.

Key Words : Mobile IP; VPN; SA Re-negotiation.

ABSTRACT

In the remote access VPN architecture which is based on IPsec, if the VPN client wants to be served the VPN service continuously during VPN client's handoff, It needs the techniques to merge VPN with Mobile IP. In this case, if the VPN client roams to new subnet, it acquires new CoA. As a result of changing IP address, existing SA becomes useless and new SA is required. The SA renegotiation process results from handoff of the VPN client and does not result from security aspect. Hence, In the environment which includes many handoffs, overhead by SA re-negotiation deteriorates performance. In this paper, we propose the technique provides that it doesn't need to renegotiate SA and be able to get the security service continuously even though MN's handoff occurs in Mobile IP VPN environment.

Ⅰ. 서 론

최근 몇 년 사이에 인터넷은 가히 놀랄만한 정도로 성장하였고, 그 결과 현재 대부분의 데이터 통신은 인터넷을 통해서 이루어진다고 해도 과언이 아니다. 그러나, 시간이 흐를수록 표준 IP에서는 지원하지 못하는 다양한 IP 응용분야에 대한 요구 및 관심이 증대되었고, 또 인터넷에서 그러한 요구를 수용할 수 있도록 하는 다양한 연구들이 진행되고 있다. 이러한 요구들 중에 IP 이동성 지원을 위한 Mobile IP[1]와, IP에 security service를 제공하는

* 연세대학교 컴퓨터과학 · 산업시스템공학과 정보통신연구실 ({jscha,meganic,jssong}@emerald.yonsei.ac.kr)
논문번호 : 030147-0401, 접수일자 : 2003년 4월 1일

IPsec[2]은 많은 성과를 가져온 분야라고 할 수 있다. Mobile IP는 IP를 지원하는 통신노드가 네트워크에서 고정된 위치에 있지 않고, 이동을 하더라도 지속적인 통신이 가능하도록 하는 개념으로, IETF (Internet Engineering Task Force)에 의해 표준화되었다. IPsec은 보안기능이 취약한 표준 IP에 인증과 기밀성을 제공하고 안전한 통신을 가능하게 하는 IP 계층의 프로토콜로, 역시 IETF에 의해 표준화되었다. IPsec은 또한 최근에 각광받고 있는 VPN(Virtual Private Network)[3]을 구성하기 위한 다양한 방법들 중에 대표적인 방법이라고 할 수 있다.

이 논문에서는 Mobile IP와 VPN에 대하여 간단하게 살펴보고, remote access VPN 환경을 위한 Mobile IP와 VPN의 연동, 그리고 그에 따른 문제점인 MN(Mobile Node)의 handoff에 따른 SA(Security Association) 재협상 문제에 대하여도 알아보기로 한다. 그리고 MN이 handoff하더라도 SA 재협상 없이 지속적인 VPN 서비스를 제공할 수 있는 새로운 기법을 제안하고, 분석하고자 한다.

II. Mobile IP/VPN overview

이 장에서는 Mobile IP와 VPN에 대하여 간단하게 살펴보기로 한다.

1. Mobile IP overview

Mobile IP는 간단하게 말해서, IP를 사용하는 모바일 노드 MN이 이동 중에도 상대 노드 CN (Correspondent Node)과 지속적인 통신을 할 수 있도록 하는 기법이다. Mobile IP에서 CN이 MN에게

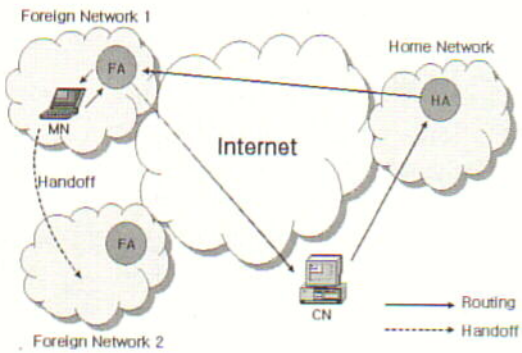

그림 1. Mobile IP의 라우팅

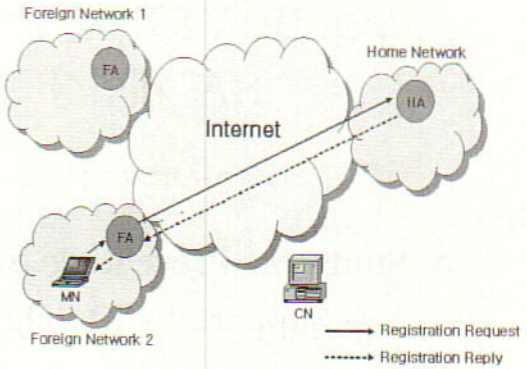

그림 2. MN의 Handoff 발생시 Registration 과정

데이터를 전송할 때에는 MN의 영구적인 home address로 데이터를 전송하기 때문에, 그림 1에서 보는 것과 같이 MN으로 향하는 패킷은 MN의 HA(Home Agent)에 의해 가로채진다. HA는 가로챈 패킷을 MN이 실제로 위치하고 있는 Foreign Network으로 터널링 해주는 방법으로 움직이는 노드인 MN이 지속적으로 CN과 통신을 할 수 있도록 해준다. 이러한 방법이 가능한 이유는 MN이 자신의 접속점이 변경되는 경우(handoff)마다 자신의 CoA(Care-of Address)를 획득하여 이 주소를 HA에 알려주어 HA가 MN의 변하지 않는 home address와 CoA간의 바인딩을 유지할 수 있도록 하기 때문이다. 그림 1에서 MN이 handoff하여 foreign network 2로 이동한 경우에 MN은 새로운 CoA의 바인딩을 위한 registration을 수행하게 되는데, 그림 2는 이러한 registration과정을 나타내고 있다. MN의 CoA는 Foreign Agent CoA와 co-located CoA의 두 가지가 있는데, 전자는 foreign network에 FA(Foreign Agent)가 존재하고 MN은 FA의 IP address를 자신의 CoA로 사용하는 경우이며, 후자는 foreign network에 FA가 존재하지 않고 MN은 DHCP(Dynamic Host Configuration Protocol)와 같은 별도의 메커니즘으로 CoA를 획득하여 사용하는 방법이다. 우리의 연구에서는 FA가 없고 그에 따라 co-located CoA를 사용하는 Mobile IP를 주로 다루게 된다.

2. VPN overview

VPN은 회사와 같이 사설망을 설치하여 운영해야 할 필요가 있는 경우에, 사설망을 직접 설치하거나 영구 임대회선을 사용하는 대신에 공중망을 이용해서 저렴한 가격으로 사설망의 기능을 대체할

수 있는 개념이다. 현재 VPN을 구현하는 방법으로

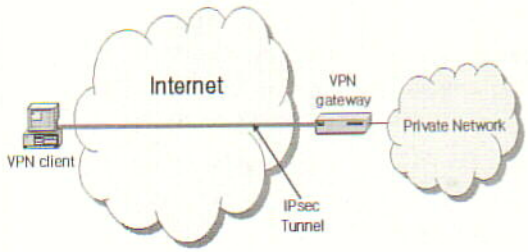

그림 3. remote access VPN 구조

는 크게 IPsec을 이용한 IPsec VPN과 MPLS (MultiProtocol Label Switching)를 이용하는 MPLS VPN으로 구분되고 있다. IPsec은 IP 패킷 자체를 암호화하여 전송하는 것이 가능하므로, 높은 security를 보장해주지만, 프로토콜이 다소 무거운 단점이 있다. 반면에 MPLS는 traffic separation을 제공하여 VPN을 구성하므로, 높은 수준의 security를 보장하지는 않지만, 다양한 QoS를 제공할 수 있는 장점이 있다. 한편, VPN은 구조에 따라서 크게 3가지로 구분되는데, 멀리 떨어진 intranet들을 VPN으로 연결하는 site-to-site VPN과 원격 접속을 통해 intranet에 접근하는 remote access VPN, 마지막으로 business partner나 customer에게 intranet network resource의 일부를 접근하게 하는 extranet VPN이 그것이다. 이 논문에서 우리의 관심은 그림 3과 같은 IPsec에 기반한 remote access VPN 구조에 제한되는데, 그 이유는 remote access 사용자가 이동 중에도 지속적인 VPN 서비스를 받을 수 있는 환경을 다루기 위해서 mobile IP와 VPN의 개념을 연동하여 생각하기 때문이다.

III. Mobile IP와 VPN의 연동

Mobile IP와 VPN은 기본적으로 서로 다른 분야의 개념이지만, VPN을 사용하는 회사들의 증가와 원격지 근무나 출장근무, 이동 근무라는 새로운 요구에 의해 근무자가 VPN client가 되어서 보호된 회사 내부의 데이터를 사용해야 할 필요가 생겼고, 더구나 지속적으로 이동하면서도 VPN service를 이용해야 할 필요도 생기면서 단순한 remote access VPN으로는 이러한 요구를 수용할 수 없으므로, Mobile IP와 VPN을 연동해야 할 필요성이 생기게 되었다. 본 장에서는 우리가 다루려 하는 Mobile IP VPN 환경에 대하여 살펴보고, Mobile

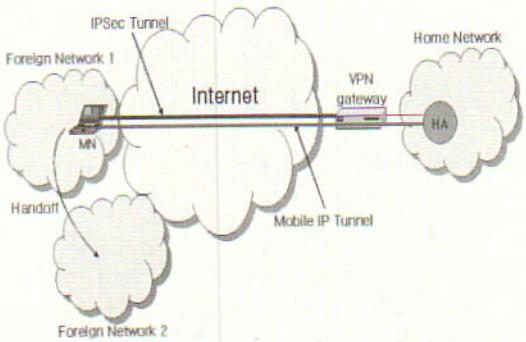

그림 4. Mobile IP VPN 환경

IP와 VPN의 연동에 따른 문제점 및 이를 해결하기 위한 기존의 연구들에 대하여 살펴보고자 한다.

1. Mobile IP VPN 환경

논의되는 Mobile IP VPN 환경은 기본적으로 remote access VPN 구조를 따른다. 그림 4에서와 같이 Mobile IP VPN 환경은 기본적으로 remote access VPN 구조를 따른다. 다만, 사설망인 home network안에 HA가 존재하고, Mobile IP의 MN은 곧 VPN client에 해당된다. Mobile IP VPN 환경에서는 두 개의 터널이 존재하는데, MN과 VPN gateway사이의 security를 위한 IPsec 터널과, MN과 HA사이의 라우팅을 위한 Mobile IP 터널이 그것이다. 또, foreign network에는 FA가 존재하지 않는 모델을 사용하여 모든 MN은 co-located CoA를 가지게 된다. 마지막으로, 논의되는 Mobile IP VPN 환경에서는 일반적인 Mobile IP에서의 CN이 존재하지 않는데, 그 이유는 VPN의 개념 자체가 사설망 내부의 자원에 VPN client가 안전하게 접근하는 개념이므로, MN이 home network 외부에 있는 인터넷상의 임의의 CN과 통신하는 것보다는 사설망인 home network상의 다른 노드와 통신을 하는 것이 VPN의 원래의 개념에 부합하기 때문이다. 결과적으로 그림 4와 같은 Mobile IP VPN 환경에서는 기존의 remote access VPN 구조와는 달리 VPN client(MN)가 handoff하여 새로운 foreign network으로 이동하더라도, 패킷은 Mobile IP의 라우팅을 통해 handoff한 VPN client로 지속적으로 전달될 수 있으므로, VPN client의 이동과는 관계없이 지속적인 VPN 서비스가 보장된다.

2. Mobile IP와 VPN연동의 문제점

그림 4에서와 같은 Mobile IP VPN 환경은 기본

적으로는 동작을 하지만, IPsec 자체가 모바일 환경을 위해 제안된 것이 아니기 때문에 MN이 handoff 할 때에 MN과 VPN gateway간의 SA를 재협상 해야하는 문제가 발생한다. SA는 IPsec에서 secure communication을 하려는 두 개체간의 security 협약으로 단방향성이다. 따라서, 두 개체간에 송/수신이 모두 안전하게 보호되려면, 2개의 SA가 생성되어야 한다. IPsec에서 SA를 고유하게 구분하는 데에 3가지 파라미터를 사용하는데, 그것은 SPI (Security Parameter Index), destination IP address, security protocol(AH or ESP)이고, 이중에 destination IP address가 문제의 원인이 된다. Mobile IP VPN 환경에서, MN은 co-located CoA를 사용하므로 MN과 VPN gateway간의 2개의 SA중에 (MN → VPN gateway) 방향의 SA는 MN이 handoff하더라도 영향을 받지 않는다. 하지만, (VPN gateway → MN) 방향의 SA는 MN이 handoff하면 SA를 구분할 수 있는 파라미터 중, destination IP address가 MN이 handoff하여 획득한 새로운 CoA가 되기 때문에 기존의 SA는 이용될 수 없으므로, (VPN gateway → MN) 방향의 SA는 새로 협상이 되어야 하는 문제가 생긴다. 만일 MN의 handoff가 자주 발생한다면, 그때마다 SA를 새롭게 협상해야 하므로 SA 협상에 따른 오버헤드(키 생성, 교환 등)가 그만큼 더 커질 수 있음을 의미한다. 하지만, 실질적으로 보호된 통신을 하는 두 개체인 MN과 VPN gateway가 변경된 것이 아니므로, 다시 말해 security의 관점에서는 굳이 새롭게 SA를 협상할 필요가 없기 때문에 이동성 지원으로 인한 SA 재협상은 불필요한 오버헤드이고, 개선이 필요하다.

3. 기존의 방법들

앞서 살펴본 MN의 이동성 지원에 따른 SA 재협상을 해결하기 위한 기존의 방법들은 크게 2가지로 분류될 수 있다. 첫째는, 모든 MN들에 unique identifier를 부여하고, SA를 고유하게 식별하는 파라미터 중 destination IP address를 MN에 부여한 unique identifier로 대체하는 방법이다.[4] 이러한 방법은 MN이 이동할 때 단지 IP주소만 변경된다는 사실에 착안하여 고안되었다. 모든 VPN 개체에 고유한 식별자인 unique identifier를 부여하면, 이 정보는 MN이동하더라도 변경되지 않으므로 굳이 SA를 식별하는 파라미터로 변하는 IP주소를 사용하기보다는 변하지 않는 unique identifier를 사용함으로써 SA 재협상을 근본적으로 방지할 수 있게 된다. 그러나, 이러한 접근방법은, IPsec의 많은 부분을 수정해야 하고, unique identifier의 global uniqueness를 확보해야 하는 어려움이 있다. 두 번째 방법은, IPsec 터널이 VPN gateway와 MN의 CoA사이에 형성되어 문제가 발생하는 것이므로, IPsec 터널을 VPN gateway와 변하지 않는 MN의 home address 사이에 형성하여 MN이 이동하더라도 SA 재협상이 불필요하도록 하는 방법이다.[5][6] 이러한 방법은 SA 재협상이 필요한 근본적인 이유였던, destination IP address가 변경되지 않으므로 MN의 이동성 지원에 따른 SA 재협상이 원천적으로 불필요해지는 방법이지만, MN으로부터 송신되는 패킷의 source address가 CoA주소인 co-located CoA를 사용하는 Mobile IP 환경에는 적용할 수 없다. 다시 말해, 이러한 해결 방안은 foreign network에 FA가 존재하는 Mobile IP 환경에서만 사용이 가능하다는 의미이다. 이러한 경우에는 SA 재협상 문제는 없지만 새로운 문제가 발생하는데, 그것은 IPsec ESP가 사용될 때 FA가 MN으로부터 전송되는 패킷의 내용을 알 수 없게 되어 Mobile IP 패킷을 중계할 수 없게 되는 문제이다. 또한 Mobile IPv6[7][8]의 경우에는 foreign network에 FA가 존재하지 않으므로, 이러한 방식의 접근은 Mobile IPv6로의 확장에 문제가 있다.

표 1. 기존 방법들 및 제안하는 기법의 간략한 비교

	SA 재협상을 하는 경우	unique identifier 사용[4]	Home Address 사용[5][6]	제안하는 기법
적용성 (현재환경)	좋다	나쁘다 (IPsec 수정필요)	나쁘다 (IPsec ESP사용시 문제발생)	좋다
적용성 (IPv6환경)	좋다	나쁘다 (IPsec 수정필요)	불가능하다 (IPv6에는 FA가 없기때문)	좋다
handoff에 따른 overhead	크다	작다	작다	작다

표 1은 기존의 방법들과 본 논문에서 제안하는 기법간의 간략한 비교를 나타내고 있다. SA 재협상을 하는 경우는 Mobile IP와 VPN을 단지 연동만 하는 경우로 handoff에 따른

overhead를 줄일 수가 없다. 기존의 방법들은 현재 환경에 아무런 변경 없이 적용하기 어렵고, 단지 우리가 제안하는 기법만이 handoff에 따른 오버헤드를 줄이면서, 동시에 현재 및 IPv6 환경에서도 큰 변경 없이 적용이 가능함을 알 수 있다.

Ⅳ. 제안하는 기법

새롭게 제안하는 기법은 앞서 설명한 Mobile IP VPN 환경에서 MN이 handoff하더라도 SA 재협상을 하지 않고 기존의 SA를 이용할 수 있도록 하는 데에 초점을 맞추고 있다.

1. 관련된 개체에 추가할 기능들

1) MN : MN은 handoff하면, 새로운 CoA를 얻지만, handoff하기 이전의 CoA도 cache로 유지해야 한다. 그리고, MN은 registration request message를 전송할 때 이것이 handoff에 의한 새로운 CoA의 바인딩을 목적으로 한 것이면, registration request message에 새롭게 제안하는 MN-VPN G/W authentication extension을 덧붙이고, IPsec processing 후에 IP 헤더의 TOS(Type of Service)필드의 최하위 비트를 1로 설정하여 전송한다.

2) VPN gateway : VPN gateway는 수신한 패킷에 대하여 IP 헤더의 TOS 필드를 조사하고 최하위 비트가 1로 설정되어 있으면, 그 패킷은 IPsec processing(e.g. decapsulation 및 ESP 복호화)후에 VPN gateway가 처리해야할 MN-VPN G/W authentication extension이 포함된 패킷으로 인지한다. 이러한 패킷을 수신한 VPN gateway는 MN-VPN G/W authentication extension을 자신이 알고 있는 기존의 (VPN gateway → MN) 방향의 SA의 정보로 검증한다. 그 결과 MN-VPN G/W authentication extension이 유효하다면, VPN gateway는 MN-VPN G/W authentication으로부터 얻을 수 있는 MN의 이동전 CoA와 SPI로 IPsec의 security database인 SPD(Security Policy Database)와 SAD(Security Association Database)의 MN의 이동전 CoA를 MN의 이동한 후의 CoA로 update한다.

3) HA : HA는 Registration request message에 MN-VPN G/W authentication extension이 포함되어 있더라도 단순히 무시하면 된다.

2. 시나리오

1) co-located CoA를 가지는 MN이 새로운 foreign network으로 이동한다.

2) MN은 자신의 접속점이 변경된 것을 알고, 새로운 CoA를 획득한다.

3) MN은 CoA를 새롭게 획득하였으므로, HA에게 자신의 새로운 CoA를 알려주기 위해 registration request message를 보내는데, MN-VPN G/W authentication extension을 포함해서 보내고, IPsec processing(e.g. ESP encapsulation) 후에 IP 헤더의 TOS 필드의 최하위 비트를 1로 설정하여 전송한다.

4) VPN gateway는 수신한 패킷의 TOS 필드의 최하위 비트가 1임을 보고, 수신한 패킷이 새로운 CoA 등록을 위한 MN으로부터의 registration request message임을 알게 된다.

5) VPN gateway는 정상적인 inbound packet processing 절차에 따라서 패킷을 IPsec processing(e.g. ESP decapsulation) 하고, payload내의 MN-VPN G/W authentication extension의 유효성을 검증한 뒤, security database(SPD, SAD)의 MN의 이동 전 CoA를 새로운 CoA로 update한다.

6) VPN gateway는 패킷을 HA로 전달해서, registration request가 정상적으로 수행되도록 하며, HA는 registration request message내의 MN-VPN G/W authentication extension을 단순히 무시한다.

3. MN-VPN authentication extension

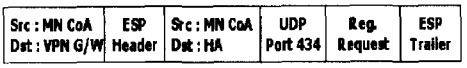

그림 5. MN이 보내는 registration request의 예

형식

MN으로부터 HA로 향하는 registration request 패킷은 그림 5와 같다. MN이 곧 VPN client이기 때문에 registration request를 포함하는 원래의 패킷이 외부의 ESP encapsulation으로 보호되어 원래의 목적지인 HA가 아닌, IPsec 터널을 통해 VPN

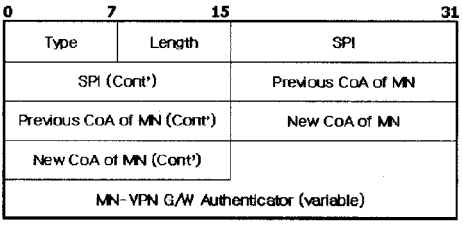

그림 6. MN-VPN G/W authentication extension

gateway로 보내진다. UDP payload에 실리는 registration request message에는 Mobile IP에 원래 정의 되어있는 3가지 authentication extension이 있는데, 그것은 MN-HA, MN-FA, FA-HA사이의 인증을 위해서 이다. 이중에 MN-HA authentication extension은 mandatory하게 포함되어야 하지만, 나머지는 선택적으로 사용된다. 우리는 기존의 extension과는 별도로 MN과 VPN gateway간의 SA 재협상을 방지하기 위해 그림 6과 같은 MN-VPN authentication extension을 제안하였다. Type 필드는 값 35를 가지고, extension이 MN-VPN G/W authentication extension임을 나타내고, Length필드는 MN-VPN G/W Authenticator 길이에 12byte를 더한 값으로 extension이 끝나는 길이를 가리킬 수 있도록 한다. SPI는 MN이 이동하기 전의 (VPN gateway → MN) 방향의 SA를 식별하는 데에 사용하는 SPI값이다. Previous CoA of MN과 New CoA of MN은 각각 MN이 handoff하기전의 CoA와 handoff하고 난 뒤의 CoA를 나타낸다. MN-VPN G/W Authenticator 필드는 MN이 이동하기 전의 (VPN gateway → MN) 방향의 SA에서 사용하는 알고리즘과 키에 의해 생성된 인증 값이다. MN으로부터 HA로 향하는 registration request message에 그림 6과 같은 extension을 추가하여 보내면, VPN gateway는 패킷을 보낸 MN이 기존의 (VPN gateway → MN) 방향의 SA를 사용하던 MN임을 인증할 수 있게 되어 security database의 주소 update만으로 SA의 재협상이 없이 기존의 SA를 사용할 수 있게 된다.

V. 분 석

새롭게 제안된 SA 재협상 방지 기법은 MN으로부터 송신되는 registration request message에 extension을 더하고, VPN gateway가 이 정보를 이용하여 security database를 update하는 방법으로 수행된다. registration request message를 이용하는 이유는 우선적으로 오버헤드를 줄일 수 있다는 장점과 registration request가 HA에 의해 받아들여지면, 그 순간부터 기존의 (VPN gateway → MN) 방향의 SA는 소용없게 되고 새로운 SA가 필요해 지기 때문이다. 여기에서는 제안한 기법에 대하여 다음과 같이 메시지 교환, security 관점, 마지막으로 Mobile IPv6로의 확장에 대한 측면으로 구분하여 분석해 보기로 한다.

표 2. 메시지 교환 비교

	SA 재협상을 하는 경우	제안된 기법
ISAKMP SA를 위한 메시지 교환	6개(main mode) 또는 3개(aggressive mode)	0개
IPsec SA를 위한 메시지 교환	3개(quick mode)	0개

1. 메시지 교환

표 1은 단순히 Mobile IP와 VPN을 연동하여 MN이 handoff할 때마다 SA를 재협상하는 경우와 제안한 아이디어간의 메시지 교환을 비교한 것이다. SA 재협상을 하는 경우에는 ISAKMP(Internet Security Association and Key Management Protocol)[9][10] SA까지 협상한다면, 적어도 6개~9개의 메시지가 MN과 VPN gateway사이에 교환되어야 한다. IPsec SA만 재협상 한다고 해도, 적어도 3개의 메시지가 교환되어야 한다. 하지만, 새로 제안한 기법은 MN이 handoff하면 당연히 수행해야할 registration request에 extension을 덧붙이는 방식으로 VPN gateway에게 필요한 정보를 알려주므로, SA 재협상을 위한 메시지 교환은 일어나지 않는다. 다만, 제안된 기법은 security database의 update를 위한 오버헤드가 있고, 기존의 MN과 VPN gateway에 추가적인 기능이 요구된다. 그림 7은 동일한 조건에서 제안된 기법과 SA 재협상을 하는 경우의 handoff 빈도에 따른 오버헤드를 비교한 결과이다. 제안된 기법은 MN-VPN G/W authentication extension만을 처리하면 되므로 fast handoff 환경일 때에도 SA 재협상으로 인한 오버헤드가 매우 작다는 것을 알 수 있다. 반면에, SA 재협상을 하는 경우는 ISAKMP SA(main mode)와 IPsec SA(quick mode)를 위해 총 9번의 메시지가 handoff시마다 발

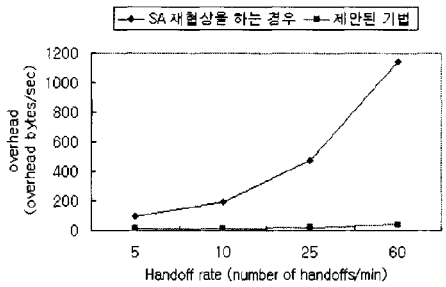

그림 7. handoff 빈도에 따른 오버헤드 비교

생하기 때문에 handoff 빈도가 늘어날수록 SA 재협상으로 인한 오버헤드가 매우 크게 증가한다.

2. security

새롭게 추가된 MN-VPN G/W authentication extension은 기존의 registration request message에 추가되어 전송되므로, MN의 이동과는 무관하게 유효한 (MN → VPN gateway) 방향의 SA에 의해 ESP로 보호되어 전송될 수 있다. 따라서, 비교적 높은 security를 보장받을 수 있다. 하지만, 제안하는 방법이 VPN gateway에게 MN-VPN G/W authentication extension이 포함된 패킷을 알려주기 위해 IP 헤더의 TOS 필드를 이용하기 때문에, VPN gateway가 DoS(Denial of Service) 공격의 대상이 될 수 있다. 이 경우에는 VPN gateway가 inbound packet processing 정책을 통해서, 정상적으로 VPN gateway와 협상한 SA가 존재하지 않는 패킷에 대해서는 패킷을 drop시키는 방법으로 해결이 가능하다.

3. Mobile IPv6로의 확장

Mobile IP VPN 환경을 co-located CoA를 사용하는 MN만으로 제한하였기 때문에, 제안한 기법을 MN의 CoA로써 항상 co-located CoA를 사용해야 하는 Mobile IPv6환경으로 확장해서 적용하는 데에 그다지 큰 제약사항이 없다. 또한, TOS 필드를 사용하는 것은 IPv6 헤더에 TOS 필드가 없기 때문에 유사한 Traffic Class 필드를 이용하여 해결이 가능하다. 다만, IP주소의 길이가 차이가 나기 때문에 구체적인 extension의 내용은 수정이 불가피하다.

VI. 결 론

새롭게 제안한 SA 재협상 방지 기법은 MN이 handoff하여 새로운 CoA를 획득하여도 SA 재협상을 하지 않고, 기존의 SA를 이용하여 지속적으로 VPN service를 이용할 수 있다. MN의 handoff가 자주 발생한다면, SA 재협상을 하지 않고, 기존의 SA를 이용하는 것은 효과적인 방법이다. Mobile IP registration request message에 새로운 extension을 추가하고 VPN gateway가 이 정보를 이용하여 security database를 update함으로써, 기존의 SA를 이용할 수 있고 SA 재협상은 불필요해 진다. 다만, MN과 VPN gateway에 부가적으로 새로운 기능이 추가되어야 하는 것은 문제가 된다. 마지막으로, 제안한 방법은 Mobile IPv6환경에서도 큰 변화 없이 적용이 가능하다.

참 고 문 헌

[1] C. Perkins, "IP Mobility Support for IPv4", *RFC 3344*, August 2002.

[2] S. Kent, R. Atkinson, "Security Architecture for the Internet Protocol", *RFC 2401*, November 1998.

[3] Ruixi Yuan, W. Timothy Strayer, "Virtual Private Networks : Technologies and Solutions", *Addison-Wesley*, 2001.

[4] Sanchez E, Edwards R, "Optimisation of the establishment of secure communication channels in wireless mobile network", *in Proceedings of the International Parallel and Distributed Processing Symposium (IPDPS'02)*, 2002.

[5] Farid Adrangi, Prakash Iyer, Kent Leung, Milind Kulkarni, Alpesh Patel, Qiang Zhang, Joe Lau, "Problem Statement and Requirements for Mobile IPv4 Traversal Across IPsec-based VPN Gateways", *Internet Draft draft-ietf-mobileip-vpn-problem-statement-req-00.txt*, July 2002.

[6] Barton M, Atkins D, Lee J, Narain S, Ritcherson D, Tepe K.E, Wong K.D, "Integration of IP Mobility and Security for Secure Wireless Communications", *in Proceedings of IEEE International Conference on Communications*, ICC 2002, Volume 2, pp. 1045-1049, 2002.

[7] S. Deering, R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", *RFC 2460*, December 1998.

[8] David B. Johnson, Charles E. Perkins, Jari Arkko, "Mobility Support in IPv6", *Internet Draft draft-ietf-mobileip-ipv6 -19.txt*, October 2002.

[9] D. Morghan, M. Schertler, M. Schneider, J. Turner, "Internet Security Association and Key Management Protocol (ISAKMP)", *RFC 2408*, November 1998.

[10] D. Harkins, D. Carrel, "The Internet Key Exchange (IKE)", *RFC 2409*, November 1998.

차 정 석(Jeong-Seok Cha) 준회원

2002년 2월 : 연세대학교 컴퓨터과학과 학사

2002년 3월~현재 : 연세대학교 컴퓨터과학·산업시스템공학과 석사과정

<주관심분야> Mobile IP, IPv6, Ad-hoc routing, Ad-hoc mulitcasting, WCDMA/UMTS, CDMA2000

김 태 윤(Tae-Yoon Kim) 준회원

2002년 8월 : 연세대학교 전산학과 학사

2002년 9월~현재 : 연세대학교 컴퓨터과학·산업시스템공학과 석사과정

<주관심분야> Wireless security, Authentication, Network security

송 주 석(Joo-Seok Song) 정회원

1976년 : 서울대학교 전기공학과 학사

1979년 : 한국과학원 전기 및 전자공학과 석사

1988년 : Univ. of California, Berkeley 전산과학 박사

1979~1982년 : 한국 전기통신 연구소 전임 연구원

1982년 : 중앙 전기 주식회사 개발자문

1988~1989년 : Naval Postgraduate School 조교수

1989년~현재 : 연세대학교 컴퓨터과학과 교수

<주관심분야> ATM 트래픽 제어, PCS, MPLS, 정보보호, 암호학