모바일 IPv6 환경에서 IPSec-VPN의 이동성 지원과 연동 방안

Mobility Management and Interworking ofIPSec-VPN in Mobile IPv6 Networks

박종원 민상원 양훈기 신현철

(광운대학교 전자통신공학과, 석사과정) (광운대학교 전자통신공학과, 부교수) (광운대학교 전파공학과, 부교수)

Key Words : Mobile IPv6, VPN, IPSec, IKE

목 차

Ⅰ. 서 론

인터넷기술의 성장과 더불어 이에 기반을 둔 어플리케이션의 개발과 속도와 품질을 제공하기 위한 하부 전송망 기술 모두 빠른 속도로 발전하고 새로운 기술이 도입되고 있다. 그러나 현재 인터넷의 기반을 이루는 IPv4기술은 많은 문제점들이 제기되고 있으며 이를 극복하기 위한 많은 연구와 기술개발이 이루어지고 있다. 하지만 이러한 노력들 역시 기존의 IPv4에서 크게 벗어나지 않고 이를 응용하는데 그치고 있는 실정이다. 이에 따라 개발자들은 좀 더 근본적인 문제해결과 새로운 서비스 도입을 위해 IPv6라는 새로운 IP기술을 내놓게 되었고 나아가 무선 환경에서 MN(Mobile node)의 이동성을 지원할 수 있는 Mobile IPv6[1][2]를 등장시켰다. MIPV6는 MN이 다른 노드로 이동하더라도 지속적인 통신이 가능하게 하며 binding 과 tunneling을 이용한다. 보안이 필요한 모든 메시지들에 대해서는 IPSec(IP Security)[3][4]를 이용한다. IPSec은 기존의 IP의 보안의 취약점을 보완하고 안전한 IP패킷 전송을 위한 방법을 제공한다.

또한 IPsec은 요즘 대두되고 있는 VPN(Vitual Private Network)과 연동되어 터널링을 구현하는데도 사용된다. 이렇게 하면 VPN에서의 취약점인 보안 문제를 해결할 수 있다.

따라서 본 논문에서는 Mobile IPv6 에서 IPSec-VPN을 사용할 경우 MN이 다른 노드로 이동할 때 VPN gateway와 서비스 제공자 간에 SA(Security Association) 가 동작되지 않는 점을 해결하기 위한 방안을 제안하고자 한다. 논문의 2장에서는 IP의 이동성 지원을 위한 Mobile IPv6를 설명하며 접속을 위한 VPN에 관해 논의 된다 그리고 이 환경에서 보안성을 강화하기 위한 IPSec ,IKE를 다룬다. 3장에서는 Mobile IPv6 와 IPSec-VPN의 연동을 하기위한 방안과 그에 따른 사용시의 문제점을 살펴보고 4장에서는 문제점을 해결하기 위한 방법을 제안한다. 마지막으로 결론에 대해 기술한다.

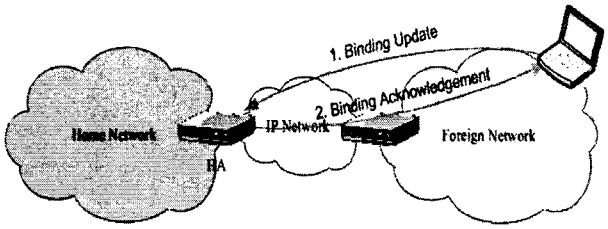
Ⅱ. Mobile IPv6 환경의 VPN

1. Mobile IPv6

Mobile IPv6 는 노드에 이동성을 보장해주어서 이동하는 노드에게 향하는 패킷을 전달하게 하는 것으로 MN이 상대노드인 CN과 지속적인 통신을 수 있도록 한다. MN은 자신의 home link나 foreign link중 어디에 접속되어 있든지 상관없이 기본적으로 고유한 글로벌 주소인 home address를 가지고 통신을 한다. home link상에 위치하고 있는 경우 MN는 자신의 home address를 사용하여 고정된 노드와 차이 없이 일반적인 방법으로 통신을 할 수 있다. 이것은 home link의 subnet prefix와 MN의 home address의 subnet prefix가 동일하므로 MN로 전달된 패킷이 home link로 라우팅 되기 때문에 가능한 것이다. MN가 home link에서 다른 link로 이동한 경우에는 기존에 가지고 있던 home address만을 가지고는 더 이상 다른 노드와 통신을 할 수 없고, 새로 접속된 foreign link상에서 자신의 위치를 나타낼 수 있는 임시 주소가 추가적으로 필요하게 된다. 이 주소를 CoA(Care of Address) 라고 하며 CoA는 foreign link의 subnet prefix를 포함하고 있기 때문에 현재 MN의 위치를 나타내게 된다.

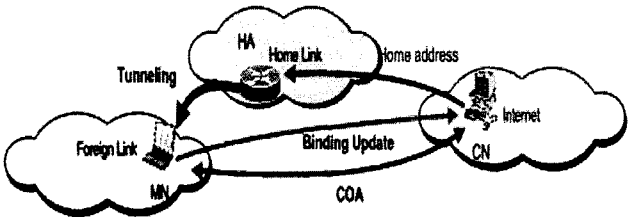
MN이 CoA를 얻는 방법으로는 DHCP(Dynamic Host Configuration Protocol) server를 통해서 동적으로 할당 받는 stateful address autoconfiguration과 IPv6의 stateless address autoconfiguration을 이용해서 구성하는 방법이 있다. 이러한 방법으로 구성된 CoA의 subnet prefix는 foreign link의 subnet prefix를 같게 되고, 인터넷의 다른 노드에서 CoA를 목적지로 전달한 패킷은 foreign link에 라우팅 되고 MN

는 CoA를 통해서 통신을 할 수 있게 되는 것이다. MN는 CoA와 자신의 home address를 결합시키는 작업을 하는데 이것을 binding 이라 한다. MN가 home link를 떠나서 외부 link로 이동하여 CoA를 얻고 binding을 구성한 후에는 자신의 home link에 있는 HA(Home Agent)에게 바인딩 정보를 등록하게 되고, HA는 MN의 home link 주소인 home address와 CoA에 관한 정보를 관리한다. 그림 1에서 보여주는 것과 같이 MN가 HA에게 바인딩 정보를 전송하는 것을 binding update라 한다.



<그림 1> Binding update 과정

HA가 바인딩 정보를 유지하는 이유는 MN의 home address로 전달되는 패킷을 정확하게 MN에게 터널링 해주기 위해서이다. MN는 글로벌한 주소인 home address를 가지고 있으므로 인터넷상의 다른 노드가 보내는 패킷은 home address를 목적지로 하여 home link로 라우팅 되고 MN가 home link에 접속되어 있을 때는 고정노드와 다름없이 자신의 home address로 패킷을 받고 다른 노드와 통신을 한다. 하지만 MN가 home link를 떠나서 foreign link로 이동하였을 경우에도 인터넷상의 다른 노드들은 여전히 MN의 글로벌한 주소인 home address로 패킷을 전송하게 된다. HA가 MN로 전송되는 패킷을 중간에서 intercept하여 foreign link 상에 있는 MN의 CoA로 터널링하여 패킷을 전달하는 proxy neighbor discovery 역할을 한다. 정확하게 MN로 터널링을 수행하기 위해서 HA는 MN의 현재 주소인 CoA를 알고 있어야 하고, 현재 MN가 속해있는 foreign link의 CoA는 MN의 BU(binding update) 메시지를 통해서 HA에게 전달된다. MN는 하나 이상의 CoA를 가지고 있을 수 있고 여러 개의 CoA를 가지고 있을 경우에 그 중에서 BU에 의해서 HA에 등록하게 되는데 이때의 CoA를 primary CoA라 한다.



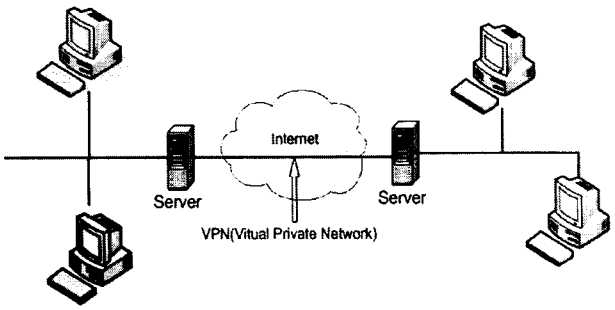
<그림 2> Mobile IIPv6 의 기본 동작

그림 2에서 MN는 자신의 CoA를 CN에 등록하기 위해서 binding update 메시지를 CN에 전달하고, CN는 바인딩 정보를 바인딩 캐쉬 목록에 등록한 뒤 그 다음번에 MN에게 보내는 패킷은 바인딩 캐쉬 목록을 검색하여 MN의 CoA로 패킷을 전송한다. 이에 따라 handoff가 발생할 때 마다 CoA를 획득하여 이 주소를 CN에 전달하게 된다. 이와 같이 이동 노드가 외부 link에 있을 때 HA를 거치는 일 없이 CoA를 가지고 직접 CN과 통신을 할 수 있게 한다. 이때의 CoA는 Foreign Agent CoA와 Co-located CoA 2가지가 있다.[5][6]

2. VPN

VPN(Virtual private network)[9]는 기존의 전용선이나 VAN(value added network)을 이용하여 기업 간 정보제공을 위한 통신망을 구축하는 것이 아니라 인터넷과 같은 공중망을 이용하여 기업외부에 있는 직원이 해당지역 ISP를 통해 기업의 네트워크에 접속하는 방법으로서, 공중망을 사용하여 지사와 본사 사이의 가상의 통신망을 구축하는 기술이라 할 수 있다. VPN은 통신의 시작점과 끝점 즉, 본사와 지사 또는 본사와 직원의 PC에 터널링 프로토콜을 설치하여, 터널링이라는 가상의 통신 선로를 구축하는 방법이 많이 사용되고 있다. 결국 VPN은 인터넷과 같이 누구에게나 개방되어 있는 공중망에서 터널링을 통한 논리적인 회선을 설정하여 가상 사설 통신망을 구축하는 기술이라고 할 수 있다.

VPN은 크게 IPSec을 이용한 IPSec VPN과 MPLS (MultiProtocol Label Switching)를 이용하는 MPLS VPN으로 나누어진다. IPSec은 IP 패킷자체를 암호화 하여 전송하는 것으로 보안에 강하고 MPLS는 traffic separation으로 다양한 QoS 를 제공한다. 또한, VPN 구조는 도입 범위에 따라 크게 4가지로 나누어 볼 수 있다. Intranet VPN은 가장 단순한 형태의 VPN으로서 기업내부의 부서를 LAN을 통해 연결, 각지사의 가까운 ISP 까지만 접속하여 인터넷 망을 이용해 각 지사를 연결하는 개념이다. Extranet VPN은 Intranet VPN의 확장형으로 자사뿐 만 아니라 고객과 업체까지도 하나의 망으로 연결한 것이다. Site to site VPN은 모바일 환경에서 개인과 개인의 네트워크사이에 VPN을 구성하는 형태이다. 그리고 마지막 Remote access VPN은 원격지원으로 회사내에서 원격으로 연결을 지원하는 형태이다. 본 논문에서는 IPSec VPN바탕의 Remote access VPN에 이동성을 보장하는 MIPV6 를 연동하는 개념을 다루며 그림 3은 VPN의 기본적인 VPN의 모습을 나타내고 있다.



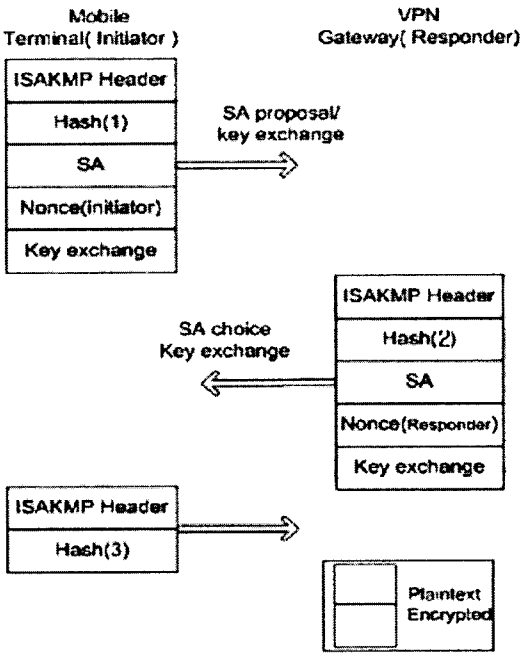
<그림 3> VPN의 사용 예

3. IKE protocol

IPSec 은 IPSec-SA들 간의 공유를 위한 기능을 가지고 있지 않지만 파라미터와 관계된 SA를 언급하는 SPI를 정의한다. IPSec은 사용자들 간의 통신에 어떻게 SA를 공유할 것인지에 관여하지 않는다. 따라서 IPSec은 이러한 목적을 위해 IKE(Internet Key Exchange) protocol[7]을 사용한다. IKE 는 IPSec과 IKE 사이의 암호화된 키를 사용하기 위해 Diffie Hellman key exchange 기법을 사용한다. IP패킷이 IPSec에 의해 보호되기 전에 먼저 SA가 있어야 한다. IKE는 RFC2409에 정의되어 있으며 SA를 동적으로 생성하는데 이용되어 IPSec에서 SA를 협상하고 SADB에 위치한다. IKE는 Internet Security Association and Key Management Protocol (ISAKMP), oakley, SKEME, 이 세 개의 프로토콜에 근거해서 만든 혼합형으로 ISAKMP에 기초해서 Oakley의 모드를 이용하고 SKEME의 rekeying 기술을 적용한다. ISAKMP에서는 key교환에 대해서 정의하지 않는다. IKE는 ISAKMP의 절차를 이용해서 이런 key교환에 대한 사항들을 정의하고 IKE 교환이 끝나고 나면 authenticated key와 SA가 설정되게 된다. 여기서 두 단계의 phase를 이용하게 되는데, IPSec-SA IKE 프로토콜을 사용하는 IKE-SA negotiation 과 IPSec-SA negotiation 이다. IKE negotiation 의 phase 1은 ISAKMP-SA negotiation, key exchange, mutual authentication 이고 phase 2는 IPSec-SA와 관련된 것으로. IPSec-SA negotiation, key exchange가 있다.

IKE 메시지는 사용자의 IP주소를 가지고 있지 않다. 또한 IP 주소가 변화되는 호스트를 발견할 수 없지만 새로운 IPSec-SA를 공유하려 시도한다. 여기서 중요한 것은 mobile IPv6 상에서 handoff 뒤 새로운 IP 주소를 가지는 사용자 터미널에게 SA 정보를 어떻게 전송 할 수 있느냐는 것이다.

그래서 본 논문에서는 IKE가 가지고 있는 key updating 과정을 이용하고자 한다. 이 key updating의 순서는 시첨 연결의 phase 2 negotiation 부분과 동일하다. 따라서 VPN gateway에 변경된 IP주소를 알리기 위해 key updating 과정 순서를 사용한다. 이 경우 handoff 될 때 사용자는 터미널은 노드가 이동 되어 IP주소가 변경된다는 것을 알 수 있다. 그렇게 되면 VPN gateway는 session key update 를 알게 되고 원래 IP 주소를 검사하고 IPSec-SA를 업데이트 시킨다. 여기서 VPN gateway 는 예전 SA를 새로운 SA 를 대처하기 위해 Initiator Cookie를 사용한다. 다음 그림 4은 IKE phase 2로 알려진 key updating이다[8][9].

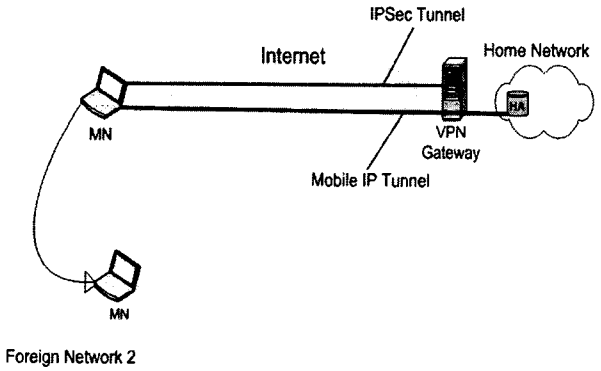


<그림 4> The key update in IKE

III. Mobile IPv6 와 IPSec-VPN의 연동과 문제점

Mobile IPv6 환경은 앞으로 IP 바탕의 이동 통신 네트워크에서 사용되어 질것이다. 그리고 그 환경에 기업체와 같이 사설망을 구성해야 하는 경우 외부에서 그 보호된 망을 접속하여야 할 필요성이 생기게 된다. 특히 사용자가 이동하면서 회사 네트워크에 접속하게 되면 기본적인 VPN 으로는 사용이 힘들뿐 아니라 정보 보안에도 큰 문제점이 발생한다. 그래서 여기서 Mobile IPv6 와 IPSec-VPN 의 연동이 필요하게 된다.

IPSec-VPN은 일반적으로 remote access 환경에서 사용된다. 그리고 모바일 터미널를 위해 고정된 주소를 제공한다. 만약 사용자터미널이 IPsec-VPN의 gateway에 연결한다면 VPN gateway는 서비스제공자와 터미널 사이의 통신을 위한 NAT(Network Address Translator)처럼 동작한다. 서비스 사용자가 사용하는 가상 IP 주소는 각 터미널에 연결될 수 있게 VPN gateway에 의해 제공된다. 그러므로 사용자 터미널은 이와 동시에 가상 주소와 강력한 보안성을 제공 받을 수 있다. Mobile IPv6 환경에서 IPSec-VPN을 연동하는 데에는 다음 그림 5와 같이 이루어진다.

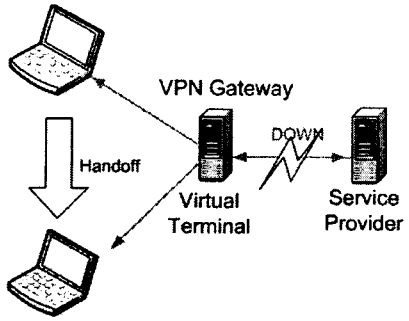


<그림 5> Mobile IPV6의 IPSec-VPN 사용

사설망인 Home network 안에 HA 가 있고 Mobile IPv6의 MN가 사용자 터미널 역할을 한다. 여기 IPSec-VPN 망에서 MN와 VPN gateway 사이에는 real IP 주소를 사용하여 Security를 위한 IPSec 터널을 형성하고, VPN gateway와 서비스제공자라 할 수 있는 HA사이는 vitual IP 주소를 사용해 Mobile IP 터널을 만들게 된다. 따라서 VPN 의 사용자 터미널이 다른 네트워크로 이동하여도 패킷은 Mobile IP의 라우팅을 통해 handoff되어 사용자 터미널은 노드 이동시에도 계속 서비스를 제공받을 수 있다.

사용자가 PDA와 같이 이동성을 지원해야하는 경우에서는 사용자가 다른 장소로 위치를 옮기더라도 연결은 계속 되어야 한다. 하지만 모바일 환경에서 사용자가 이동하는 경우에는 IP 주소는 새로운 주소로 변경되고 이 과정에서 IPsec-SA(Security Assocation)가 새로운 IP 주소를 공유할 때 까지 IPsec-VPN 의 연결은 끊어진다. 이와 같이 handoff 할 때 문제점을 발생하고 있는데 이는 IPsec가 다른 사용자 host의 IP 주소에 의존성을 가지고 있기 때문이다.

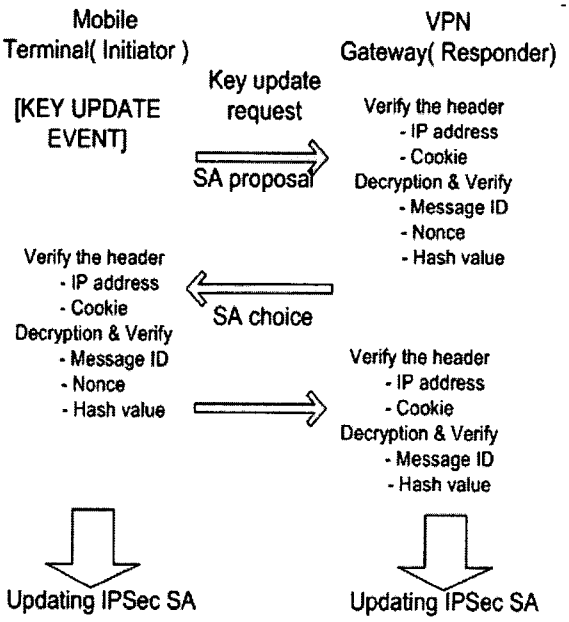
SA는 IPsec에서 보호를 위한 규약으로 단방향이기 때문에 2개의 SA를 형성하여 쌍방향을 지원한다. IPsec- SA는 3가지 파라미터 값들에 의해 정의 된다. 이 파라미터는 SPI (Security Parameter Index), an IP destination address, and a security protocol (AH or ESP) 으로 그림 6는 모바일 터미널에서 handoff 시에 VPN gateway는 SA 관리가 이루어지지 않음을 보여준다.



<그림 6> VPN에서 Handoff시 IPSec-SA의 다운

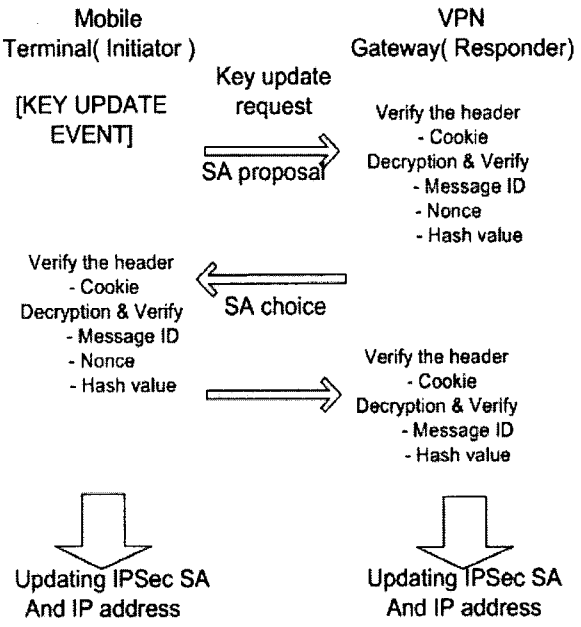
IV. 제안하는 기법

Key updating 과정은 IKE protocol에 의해 정의 된다. 그리고 이 과정은 handoff 되어 주소가 변경되어야 할 때 불러진다. Key updating 요구가 받아들여지면 응답자인 VPN gateway가 cookie 값과 source IP 주소로 사용자 터미널을 인식할 수 있다. 그리고 VPN gateway는 요구를 확인하고 IKE-SA 정보를 검사한다. 이 과정을 마친 후 요구에 따라 IPSec-SA를 업데이트한다. 그림 7은 IKE phase 2라고 알려진 key updating 과정을 보여준다.



<그림 7> IKE phase 2를 사용한 IPSec-SA updating 과정

이 방법의 사용자 터미널은 MN 가 다른 노드로 이동하여 handoff가 발생하여 IP 주소가 변경 되어질 경우에 key updating 요구를 보낸다. VPN gateway는 그것의 cookie 정보를 가지고 있는 IKE-SA를 결정하고 만약 이전에 사용하던 IP 주소와 차이가 있을시에 VPN gateway는 새로운 주소로 업데이트한다. 그 후에는 일반적인 IPSec-SA 과정을 진행한다. 이처럼 새로운 사용자의 IP주소를 가진 IPSec-SA가 만들어질 때 사용자 터미널과 VPN gateway 간에 정보는 보호될 것이다. 그림 8은 본 논문에서 제안한 handoff 방식에 의한 과정을 보여준다.



<그림 8> IKE phase 2를 사용한 제안된 handoff 과정

V. 결론

지금까지 Mobile IPv6에서 이동성을 지원하는 IPSec-VPN의 연동과 그에 따른 문제점을 지적하고 해결 방안을 살펴보았다. VPN의 사용자 터미널이 다른 장소로 이동하는 경우 handoff 가 발생하고 이 때문에 HA 와 VPN gateway의 SA를 다룰 수 없게 된다. 그래서 IKE를 도입하여 key updating과 cookie 값을 이용, 사용자의 요구에 따라 VPN gateway가 응답하여 IPSec-SA를 업데이트를 하게 된다.이 제안은 IKE 기능에 약간의 수정을 더한 것으로 handoff 시 HA와 VPN gateway간에 문제를 해결할 수 있다.

참고문헌

1. C. Perkins, drft-ietf-mobileip-ipv6-13.txt, Internet draft, November 2000.
2. Hesham Soliman, " Mobile IPv6", Addison Wesley, 2004.
3. N. Doraswamy and D. Harkins, *IPSec* , Prentice Hall, 1999.
4. Naganand doraswamy, DAN Harkins " IPSec 2nd" Prentice hall, 2003.
5. W. Fritsche, F. Heissenhuber, "Mobility support for the Next Generation Internet," April 2000.
6. C. Perkins, "IP mobility support," RFC2002, October 1996.
7. D. Harkins and D. Carrel, "The Internet Key Exchange (IKE)," RFC 2409, November 1998.
8. S. Kent and R. Atkinson, "IP Encapsulating Security Payload(ESP)", RFC2406, IETF, November 1998.
9. S. Kent and R. Atkinson, "IP Authentication Header," RFC 2402, November 1998.