논문 99-24-4B-10 한국통신학회논문지 '99-4 Vol.24 No.4B

이동 인터넷 프로토콜을 위한 질적으로 개선된 방화벽 횡단 해법

정회원 이 충 기*

An Enhanced Firewall Traversal Solution for the Mobile Internet Protocol

Chungki Lee* *Regular Member*

요 약

본 논문에서는 패킷 필터들과 방화벽들이 설치된 보안이 강화된 인터넷에서 이동 인터넷 프로토콜(Mobile IP)을 사용할 때 일어나는 문제들을 다룬다. 이동 노드의 소속 네트워크뿐만이 아니라 방문하고 있는 외국 네트워크도 방화벽에 의해 보호되고 있는 경우에 Mobile IP 프로토콜을 위한 질적으로 개선된 방화벽 횡단 해법을 제안한다. 기존의 방화벽 횡단 해법들은 소속 영역만이 방화벽에 의해 보호되는 비대칭적 해법인데 비해 본 해법은 대칭적 해법이다. 또한 본 해법은 이동 노드가 상대 노드에게 패킷을 보내는 경우에 소속 대리인을 거치지 않고 외국 영역 밖의 열린 노드를 통하여 직접 보내므로 거의 최적의 라우팅을 사용하는 해법이라고 볼 수 있다. 본 해법의 이러한 기능은 열린 노드를 사용하고 보내는 패킷에 필요한 헤더들을 추가하는 등의 최소한의 오버헤드를 사용함으로써 이루어진다.

ABSTRACT

This paper discusses problems arising out of the use of Mobile Internet Protocol (IP) in a security conscious Internet with packet filters and firewalls. An enhanced firewall traversal solution for Mobile IP is proposed in case there are firewalls protecting visited networks as well as home networks of mobile nodes. While previous solutions are asymmetric ones in the sense that only home networks are protected by firewalls, this solution is a symmetrical one. Also, packets from a mobile node can go directly to the correspondent node via a "Open Node" just outside of a foreign domain without going through the home agent of the mobile node. Therefore the solution uses an almost optimal routing. This is achieved with the minimal overhead such as using open nodes and adding necessary headers to packets directed from the mobile node to the correspondent node.

I. 서 론

최근에 랩탑 컴퓨터와 노트북 컴퓨터의 보급이 폭발적으로 증가하고 있고 이러한 휴대용 컴퓨터들이 인터넷과 웹(World Wide Web)에 접속하는 수 또한 빠르게 증가하고 있다. 인터넷의 향후 성장은 이러한 휴대용 컴퓨터들에 기인할 것으로 전망되고 있다. 왜냐하면 휴대용 컴퓨터들이 가장 빠르게 성장하고 있는 컴퓨터 시장중의 하나이기 때문이다. 이러한 추세와 아울러 무선 통신 장비 시장도 꾸준히 성장하고 있다. 그러한 장비들은 인터넷에 접속하는 선택의 폭을 늘리는 효과를 가질 수 있다. 이동하는 고객들은 인터넷 접속을 위해 다양한 무선 통신 장비들 중 선택할 수 있다. 다양한 라디오 부

* 명지대학교 전자정보통신공학부(cklee@wh.myongji.ac.kr)
논문번호 : 98260-0622, 접수일자 : 1998년 6월 22일
※ 이 연구는 일부 정보통신부의 정보통신 우수 시험학교 지원사업에 의해 수행되었음

착 장비들, 적외선 장비들, 이동 전화망을 통한 통신 장비 등이 이에 해당된다.

이러한 추세는 이동 컴퓨터들이 인터넷에 무선으로 접속할 수 있고 이동하면서 인터넷에 계속 연결할 수 있는 방법에 대한 많은 관심을 불러일으키고 있다. 이러한 문제가 대두되면서부터 IP 프로토콜을 확장하여 망 계층에서 이동성을 지원하는 방법이 적절한 것으로 받아들여지고 있다. 이러한 접근 방법은 응용 프로그램의 투명성과 빈틈없는 이동의 가능성과 같은 혜택을 제공할 것이다. 이동 컴퓨터 사용자들이 이동성을 지원하는 응용 프로그램들을 사야만 하는 것은 적절하지 않기 때문에 응용 프로그램의 투명성은 이동 지원 문제의 모든 해법에 대해 요구된다. 빈틈없는 이동은 아직 필수적이지는 않지만 연속적인 접속을 위한 무선 접속 수단이 널리 보급된다면 사용자 편의성 측면에서 필요할 것 같다. 이동 인터넷 프로토콜(Mobile Internet Protocol 혹은 Mobile IP)은 인터넷에서 이동 컴퓨터들에게 빈틈없는 이동성을 제공하는 유일한 수단이고 현재 인터넷의 표준으로 확정되었다[1].

Mobile IP는 이동 노드가 자신의 IP 주소를 사용하여 어느 곳에 있든지 IP 패킷들을 보내고 받을 수 있는 것을 가능하게 하는 프로토콜이다. 그러나 현재 Mobile IP 프로토콜 명세서는 패킷 필터들 혹은 방화벽들이 설치된 보안이 강화된 인터넷에서 어떻게 운용될 것인지에 대해 고려하지 않고 있다. 따라서 Mobile IP를 사용할 때 패킷 필터 통과 문제와 방화벽 횡단 문제가 가장 큰 문제중의 하나로 대두되고 있다[2,3,4,5]. Gupta등은 Mobile IP를 위한 방화벽 횡단 해법 요구 사항의 목록을 제시하고 있다[3]. 또한 그들은 이동 노드의 소속 네트워크가 방화벽에 의해 보호되고 있는 경우에 이동 노드가 보내거나 받는 패킷들이 방화벽을 통과할 수 있는 해법을 제안하고 있다[4]. Montenegro등은 이동 노드의 소속 네트워크가 SKIP[6] 방화벽에 의해 보호되고 있는 경우에 이동 노드가 보내거나 받는 패킷들이 방화벽을 통과하는 안전한 채널을 구성하는 해법을 제안하고 있다[5]. 그러나 이러한 해법들은 이동 노드가 방문하고 있는 네트워크에는 방화벽이 없다고 가정하고 있고 이동 노드가 보내고 받는 패킷의 경로가 최적이 아닌 라우팅을 사용한다.

본 논문에서는 Mobile IP 프로토콜의 개요를 살펴보고 Mobile IP 프로토콜을 사용할 때 패킷 필터와 방화벽 횡단 문제를 자세히 살펴본다. 그리고 이동 노드의 소속 네트워크뿐만이 아니라 방문하고 있는 네트워크도 방화벽에 의해 보호되고 있는 경우에 Mobile IP 프로토콜을 위한 질적으로 개선된 방화벽 횡단 해법을 제안한다. 이 해법은 기존의 해법들과는 달리 이동 노드가 상대 노드에게 보내는 패킷을 소속 네트워크를 거치지 않고 직접 보내는 최적의 라우팅을 사용한다. 이 논문의 구성은 다음과 같다. 2장에서는 이동 인터넷 프로토콜에 대해 간단히 살펴본다. 3장에서는 패킷 필터와 방화벽 통과 문제에 대해 자세히 다룬다. 4장에서는 새로운 방화벽 횡단 해법을 제안한다. 5장에서는 제안된 해법을 기존 해법들과 비교한다.

Ⅱ. 이동 인터넷 프로토콜

Mobile IP 프로토콜은 인터넷 내에서 노드의 이동성을 지원하는 효율적이고 확장성이 있는 메커니즘을 제공한다. 이 프로토콜을 이용하여 노드들은 그들의 IP 주소들을 바꾸지 않고 인터넷에 접속점을 변경할 수 있다. Mobile IP 프로토콜은 이동하는 노드가 자신의 소속 네트워크에 더 이상 연결되어 있지 않을 때에도 자신의 IP 주소를 사용하여 IP 패킷들을 보내고 받는 것을 계속하게 한다.

1. 용어 정의

여러 용어들이 Mobile IP 프로토콜의 명세서에서 사용된다. 이 논문에 적절한 용어들에 대해 Mobile IP 명세서에 근거하여 이 절에서 기술한다[1].

Mobile IP는 다음과 같은 새로운 기능적 개체들을 소개한다.

이동 노드 (Mobile Node 혹은 MN) - IP 주소를 바꾸지 않고 한 네트워크나 부분망(subnet)으로부터 다른 네트워크나 부분망으로 접속점을 변경하는 호스트나 라우터. 이동 노드는 자신의 IP 주소를 사용하여 어느 곳에서든지 다른 인터넷 노드들과 통신을 계속할 수 있다.

소속 대리인 (Home Agent 혹은 HA) - 이동 노드들에게 패킷들을 배달하고 각 이동 노드의 현 위치에 대한 정보를 가지고 있는 이동 노드의 소속 네트워크(home network)에 있는 라우터.

외국 대리인 (Foreign Agent 혹은 FA) - 이동 노드가 소속 네트워크밖에 있는 동안 패킷들을 배달하기 위해 소속 대리인과 공조하고 이동 노드가 현재 연결되어 있는 네트워크에 있는 라우터.

다음 용어들은 Mobile IP 프로토콜과 연관되어 자주 사용된다.

대리인 선전 (Agent Advertisement) -외국 대리인들은 라우터 선전 메시지에 특별한 확장자를 첨부하여 생성되는 특별한 메시지를 사용함으로써 자신들의 존재를 알린다.

전교 주소 (Care-of Address 혹은 COA) - 이동 노드가 소속 네트워크밖에 있는 동안 전송되는 패킷들에 대한 이동 노드 방향으로의 터널의 종점. 두 가지 다른 유형의 전교 주소가 있다. 외국 대리인 전교 주소 (foreign agent care-of address)는 이동 노드가 현재 등록된 외국 대리인의 IP 주소이다. 반면에 배치된 전교 주소(co-located care-of address)는 이동 노드가 외부에서 얻은 자신의 네트워크 접속부들 중의 하나에 대응된 지역 IP 주소이다.

상대 노드 (Correspondent Node) - 이동 노드가 통신하고 있는 동료 노드. 상대 노드는 이동 노드이거나 고정 노드일 수 있다.

외국 네트워크 (Foreign Network) - 이동 노드의 소속 네트워크 외의 네트워크.

소속 주소 (Home Address) - 이동 노드에게 장기간 배정된 IP 주소. 이 주소는 이동 노드가 인터넷에 접속되어 있는 위치와 무관하게 변경되지 않는다.

소속 네트워크 (Home Network) - 이동 노드의 소속 주소의 네트워크 번호와 같은 네트워크 번호를 가지고 있는 네트워크. 가상 네트워크일 수 있다. 표준 IP 라우팅 메커니즘은 이동 노드의 소속 주소가 수신지인 패킷들을 소속 네트워크로 배달한다.

링크 (Link) - 노드들이 데이터 링크 계층에서 통신할 수 있는 시설 혹은 매체. 링크는 망 계층 아래에 있다.

이동 지원 대리인 (Mobility Agent) - 소속 대리인 혹은 외국 대리인

이동성 보안 결합 (Mobility Security Association) - 한 쌍의 노드들 사이의 보안 관계들의 모음. 이러한 보안 관계들은 두 노드들 사이에 교환되는 Mobile IP 프로토콜 메시지들에 적용될 수 있다. 각 보안 관계는 인증 알고리듬 및 모드, 공유키 혹은 적절한 공개 키/ 사설 키 쌍과 같은 비밀, 사용중인 재전송 보호 유형 등을 나타낸다.

보안 매개변수 색인 (Security Parameter Index 혹은 SPI) - 이동성 보안 결합에 사용될 수 있는 문맥들 중에서 한 쌍의 노드들사이의 보안 문맥을 식별하는 색인. 0에서 255까지의 SPI 값들은 예약되어 있고 어떠한 이동성 보안 결합에서도 사용되어서는 안된다.

터널(Tunnel) - 패킷이 캡슐화 되는 동안 패킷이 지나가는 경로. 패킷이 캡슐화 되어 있는 동안 패킷은 이 사실을 알고 있는 캡슐을 제거할 수 있는 이동 지원 대리인으로 보내진다. 그 대리인은 패킷의 캡슐을 제거하고 이를 최종 수신지로 배달한다.

방문 네트워크 (Visited Network) - 이동 노드가 현재 연결되어 있는 소속 네트워크가 아닌 네트워크

2. 프로토콜 개요

Mobile IP 프로토콜은 세 가지의 관련된 기능들을 수행하는 방법이다[1].

대리인 발견 (Agent Discovery) - 소속 대리인들과 외국 대리인들은 자신들의 존재를 서비스를 제공하는 각 링크를 통해 알린다. 새로 도착한 이동 노드는 Mobile IP 를 지원하는 대리인이 있는 지를 알기 위해 그 링크를 통해 대리인 요청 메시지를 보낼 수 있다.

등록 (Registration) - 이동 노드가 소속 네트워크 밖에 있을 때 자신의 전교 주소를 자신의 소속 대리인에게 등록시킨다. 이동 노드가 인터넷에 어떤 방식으로 연결되어 있느냐에 따라 자신의 소속 대리인에게 직접 등록할 수도 있고 등록 메시지를 소속 대리인에게 전송해 주는 외국 대리인을 통하여 등록할 수도 있다.

터널 만들어 보내기 (Tunneling) - 이동 노드가 소속 네트워크밖에 있을 때 패킷들을 전달하기 위하여 소속 대리인은 패킷들을 전교 주소로 터널을 만들어 보낸다.

다음은 Mobile IP 프로토콜의 운용에 대해 대략적인 개요를 제공한다.

◇ 이동 지원 대리인들은 대리인 선전 메시지들을 보냄으로써 자신들의 존재를 알린다. 이동 노드는 선택적으로 대리인 요청 메시지를 보냄으로써 현재 연결되어 있는 이동 지원 대리인들로부터 대리인 선전 메시지를 요청할 수도 있다.

◇ 이동 노드는 이러한 대리인 선전 메시지를 받자마자 자신이 소속 네트워크에 있는지 아니면 외국 네트워크에 있는 지를 확인한다.

◇ 이동 노드가 소속 네트워크에 있다는 것을 탐지할 때 이동 노드는 이동 서비스를 사용하지 않고 소속 네트워크에 있는 어떤 다른 노드들과 같이 행동한다. 이동 노드가 외국 네트워크에서 소속 네트워크로 돌아왔다는 것을 확인한다면 등록 요청 메시지와 등록 답장 메시지를 소속 대리인과 교환함

으로써 자신의 등록을 취소한다.

◇ 이동 노드가 외국 네트워크로 옮겼다는 것을 탐지할 때 외국 네트워크에서 전교 주소를 얻는다. 이 전교 주소는 외국 대리인의 선전 메시지로부터 결정된 외국 대리인 전교주소일 수도 있고 Dynamic Host Configuration Protocol (DHCP)와 같은 외부 배정 메커니즘에 의해 얻어진 배치된 전교 주소일 수도 있다.

◇ 외국 네트워크에 있는 이동 노드는 외국 대리인을 통하여 소속 대리인과 등록 요청 메시지와 등록 답장 메시지를 교환하므로써 자신의 새 전교 주소를 소속 대리인에게 등록시킨다.

◇ 이동 노드의 소속 주소로 보내진 패킷들은 소속 대리인이 중간에서 차단한 후 이를 캡슐화 하여 이동 노드의 전교 주소로 터널을 만들어 보낸다. 이 패킷들은 터널의 종점에서 외국 대리인 혹은 이동 노드 자신에 의해 캡슐이 제거된후 최종적으로 이동 노드에게 전달 된다.

◇ 이동 노드가 상대 노드로 보내는 패킷들은 표준 IP 라우팅 메커니즘들을 사용하여 그들의 수신지로 보내진다. 이러한 패킷들은 반드시 소속 대리인을 경유하지는 않는다.

소속 대리인이 이동 노드의 소속 주소로 보내진 패킷을 이동 노드의 전교 주소로 터널을 만들어 보낼 때 캡슐내의 내부 IP 헤더의 수신지 (이동 노드의 소속 주소)는 소속 네트워크와 이동 노드의 현 위치 사이에 있는 모든 라우터로부터 효율적으로 감춰진다. 본래의 패킷은 이동 노드의 전교 주소에서 캡슐이 제거된 후 이동 노드로 보내진다.

이동 노드가 소속 대리인과 등록을 한 후에 이동 노드로 보내진 패킷들이나 이동 노드로부터 보내진 패킷들의 라우팅은 그림 1에 설명되어 진다. 이동 노드는 외국 대리인이 제공한 전교 주소를 사용하고 있다고 가정된다.

(1) 이동 노드의 소속 주소로 보내진 패킷은 표준 IP 라우팅을 통하여 소속 네트워크에 도착된다.

(2) 그 패킷은 소속 대리인에 의해 차단되어 캡슐화되어 이동 노드의 전교 주소로 터널을 만들어 보내진다. 그림에서 관을 관통하는 화살표에 의해 기술된다.

(3) 그 패킷은 터널의 종점인 외국 대리인에 도착된 후 캡슐이 제거된 후 이동 노드에게 전달된다.

(4) 이동 노드가 보낸 패킷들에 대해서는 표준 IP 라우팅이 각 패킷을 그것의 수신지로 배달한다. 이 그림에서 외국 대리인이 이동 노드의 기본 라우터 (default router)이다.

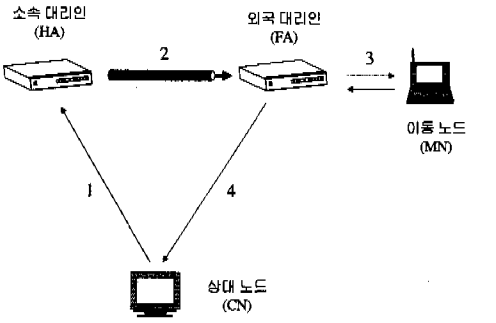


그림 1. Mobile IP 패킷 흐름

Ⅲ. 패킷 필터링과 방화벽 횡단 문제

현재 인터넷에서 Mobile IP 프로토콜의 보급에 걸림돌이 되는 가장 큰 문제점들 중의 하나는 외부 기업들의 네트워크에 연결되어 있는 이동 노드들이 침입자들처럼 보인다는 사실이다. 이러한 노드들로 가거나 오는 트래픽을 차단하기 위하여 외부 영역들에서 방화벽들과 패킷 필터링 기능을 가지고 있는 라우터들이 설치되어 운영되고 있다. 이는 해커들에 의한 프로토콜 공격의 위험을 줄이기 위한 대응책이고 해커들이 선호하는 숨기 위한 장소들을 최대한 줄이고자 하는 노력이라고 볼 수 있다. 이 장에서는 보안이 강화된 인터넷에서 Mobile IP 프로토콜을 사용함에 따라 발생하는 패킷 필터 통과 문제와 방화벽 횡단 문제들에 대해 보다 자세히 기술한다.

1. 패킷 필터 통과 문제

Mobile IP 프로토콜에서 점대점 통신의 라우팅은 전적으로 수신지 주소에 기초한다고 가정한다. 그러나 현재 인터넷에서 사용되고 있는 많은 라우터들은 받은 패킷들을 전송할 때 여러 가지 다른 사항들을 고려한다. 예를 들면 원시 필터링 라우터 (source-filtering router)들은 원시 IP 주소와 일치하지 않는 인터페이스에 도착하는 패킷들을 버린다. 그러한 라우터는 이동 노드가 외국 네트워크를 방문하고 있다면 그 노드가 보내는 원시 주소가 그 노드의 소속 주소로 되어 있는 모든 패킷들을 버릴 것이다.

이것은 Mobile IP 프로토콜에 대한 최대의 장애물이다. 외국 네트워크에 있는 이동 노드는 보내는 패킷의 원시 주소를 자신의 소속 주소로 만들 것이다. 이동 노드가 보내는 패킷은 원시 필터링 라우터에게 원시 주소가 의심이 가는 패킷으로 보여 버려질 것이다. 이에 대한 해법은 역 터널(reverse tunnel)을 사용하는 것이다[7]. 즉 이동 노드가 상대 노드에게 보내는 패킷을 캡슐화 하여 소속 대리인으로 보내는 것이다. 물론 가장 밖에 있는 IP 헤더의 원시 주소를 이동 노드의 전교 주소로 한다. 그러면 캡슐화된 패킷은 원시 필터링 라우터를 무사히 통과하여 소속 대리인에 도착될 것이다. 소속 대리인은 캡슐을 제거하여 본래의 패킷을 추출한 후 이를 상대 노드에게 전송한다.

그러나 패킷의 원시 주소로서 전교 주소를 사용하는 역 터널을 사용하는 것은 다음과 같은 이유로 인하여 바람직하지 않은 해법이다. 이동 노드가 상대 노드에게 보내는 패킷은 직접 배달되지 않고 소속 대리인을 거쳐 배달되므로 비효율적이다. 이러한 비효율성을 제거하기 위하여 이동 노드가 상대 노드에게 캡슐화된 패킷을 직접 보내는 것은 IPv4를 지원하는 상대 노드가 캡슐을 제거하는 기능을 대부분 가지고 있지 않기 때문에 적절치 못하다. 따라서 이 패킷 필터 통과 문제를 해결하고자 하는 많은 연구가 현재 진행되고 있다.

2. 방화벽 횡단 문제

대부분의 기관들은 자신들의 네트워크를 인터넷으로부터 보호하기 위해 방화벽을 사용한다. 이러한 방화벽은 추가적인 제약 사항을 가지고 있다. 예를 들면 신뢰하지 않는 외부 호스트들로부터의 요청되지 않은 패킷을 버릴 수 있다[2]. 그러한 버리는 정책은 모든 수송 계층 패킷들을 전송할 때 원시 주소, 수신지 주소, 원시 포트 및 수신지 포트를 주의 깊게 조사하여 전송 여부를 결정한다. 보다 구체적으로 방화벽은 TCP 패킷들에 대해 ACK bit를 감시할 지도 모른다. 이러한 상황에서 이동 노드의 등록 요청 패킷들은 ACK bit가 0이므로 소속 네트워크를 보호하는 방화벽에 의해 버려질 것이다. 이러한 문제를 해결하기 위해 방화벽은 적어도 패킷들이 소속 대리인의 UDP 프로토콜 포트 434로 보내진다면 그 패킷들을 받도록 구성되어야 할 것이다.

Mobile IP 프로토콜을 사용하는 이동 노드와 상대 노드사이의 통신을 고려할 때 그림 2는 방화벽이 설치될 수 있는 세 곳을 보여주고 있다[8].

- 방화벽 1 (Firewall 1 혹은 FW1)은 소속 대리인이 속한 소속 영역을 보호한다.
- 방화벽 2 (Firewall 2 혹은 FW2)는 이동 노드가 현재 인터넷에 연결되어 있는 외국 영역을 보호한다.
- 방화벽 3 (Firewall 3 혹은 FW3)은 상대 노드가 속한 영역을 보호한다.

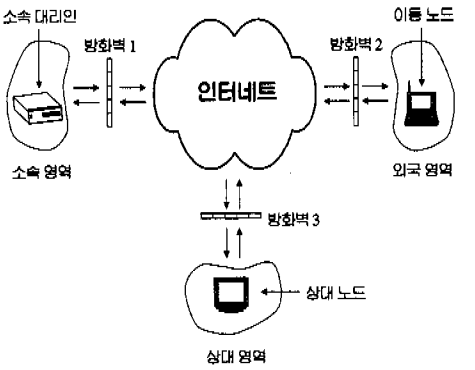


그림 2. 가능한 세 곳의 방화벽 설치 장소

방화벽 1과 방화벽 2를 횡단하는 구성 문제가 이동 노드들에 더 관심이 있다. 방화벽 3은 Mobile IP가 운용되는 방법에 영향을 끼치지 않는다. 왜냐하면 이동 노드가 소속 네트워크에 있으나 나가 있으나 상대 노드와 통신하는 똑같이 어려운 문제에 부닥칠 것이기 때문이다.

방화벽 1을 횡단하는 문제는 소속 영역을 보호하는 방화벽을 통과하는 것을 포함한다. 이는 이동 노드가 원시 IP 주소로서 자신의 소속 주소를 가진 패킷을 소속 대리인으로 보내기 때문에 해법이 필요하다. 보통 소속 영역을 보호하는 방화벽들은 소속 영역에 있는 호스트들을 보호하기 위해 소속 영역밖에 있는 컴퓨터들이 소속 영역 내에 있는 것처럼 가장하고 보내는 패킷들을 버린다. 방화벽 1을 통과하는 것을 지원할 수 있는 두 가지 기술들은 응용 중개(application relaying)과 IP 보안이다[5]. 응용 중개를 위한 공통의 인터페이스를 마련하기 위한 노력은 IETF내의 인증된 방화벽 횡단(authenticated firewall traversal) 작업반에 의해 이루어지고 있다. 그 작업반에 의해 제안된 해법은 SOCKS version 5이다[9]. 그 해법은 이동 노드나 외국 대리인이 방화벽과 UDP 트래픽을 교환하기 위해 TCP 세션을 설정하고 방화벽으로 보내는 트

래픽을 캡슐화하기 위해 SOCKS 라이브러리를 사용할 것을 요구한다. 이러한 세션은 이동 노드가 새로운 전교 주소를 등록할 때마다 필요하다. 이러한 비효율성외에도 이 해법은 IP 패킷들을 캡슐화하기 위해 UDP를 사용할 것을 요구한다. 이러한 이유로 이 해법을 사용하는 상용 네트워크는 드물다.

이에 대한 대안으로 이동 노드가 방화벽으로 보내는 트래픽은 세션에 상관없이 SKIP과 같은 IP 보안 메커니즘을 사용하여 인증되고 암호화될 수 있다. 이는 단지 UDP 트래픽을 방화벽과 교환하기 위해 한 세션을 설정해야 하는 요구 사항을 제거한다. SKIP에 기초한 해법은 이러한 경우에 적절하다. 이는 SKIP에 인증 정보가 패킷마다 포함되도록 AH[10]와 같이 사용되고 ESP[11]를 사용한 암호화가 이루어진다는 것을 의미한다. IP 계층에서 보안을 이루는 SKIP외에 다른 해법들이 있다[12].

방화벽 1를 횡단하는 문제에 대한 최신의 대표적인 해법은 Montenegro등이 제안한 해법이다[5]. 그 해법에서는 이동 노드의 소속 네트워크가 SKIP 방화벽에 의해 보호되고 있는 경우에 이동 노드가 보내거나 받는 패킷들이 방화벽을 통과하는 안전한 채널을 구성하는 것을 가능하게 한다. 그들은 방화벽내의 네트워크는 사설 네트워크(private network)으로서 사설 (IP) 주소 (private address)를 사용한다고 가정한다. 또한 상대 노드가 이동 노드와 같은 소속 네트워크에 있는 경우만을 고려한다. 그 밖에 패킷을 암호화하기 위해 ESP 프로토콜과 AH 프로토콜과 같이 SKIP 프로토콜을 사용하고 이동 노드가 배치된 전교 주소를 사용한다고 가정하고 있다. 따라서 이 해법은 이러한 가정들로 인해 제한된 경우에만 적용할 수 있다.

방화벽 2를 횡단하는 문제는 이동 노드가 외국 영역 내에서 보내는 패킷들이 그 외국 영역을 보호하는 방화벽들 혹은 패킷 필터들을 통과하는 것을 포함한다. ingress filtering 과 같은 간단한 방법을 사용하는 것은 여기서는 적절치 못하다. 왜냐하면 이동 노드는 소속 영역에서 보다 방문하고 있는 외국 영역에서 신뢰를 얻기가 훨씬 힘들다고 가정할 수 있기 때문이다. 설정할 수 있는 신뢰의 수준은 방화벽과 패킷 라우터와 같은 보안 개체들과 보안 결합을 만들고 사용하기 위해 이동성을 결정하는 기본적인 요소이다.

방화벽 2를 횡단하는 문제에 대한 만족스럽지는 않으나 간단한 해법들은 아래와 같이 제안되었다 [8].

- 수동적 구성 (manual configuration)
- 이동 노드들을 외국 영역들과 고립된 영역에 포함시킴

첫 번째 해법은 수동적으로 방화벽과 보안 결합을 구성하여 방화벽을 횡단하는 해법이다. 이동 노드가 방화벽 2와 접촉하기 위한 필요한 정보를 가진다면 이동 노드는 정의된 프로토콜은 현재 없지만 아마도 그 방화벽과 필요한 보안 결합들을 설정하기 위해 나아갈 수 있다. 따라서 많은 이동 노드들은 당분간 수동적으로 구성된 보안 결합들에 의존해야만 할 것 같다. 실제로 이는 이동 노드가 방문하는 영역에 있는 방화벽들을 횡단할 수 있기 전에 시스템 관리자를 접촉해야만 할 지 모른다는 것을 의미한다. 필요한 보안 결합들이 주어진다면 이동 노드는 방화벽 2를 횡단하는 역터널(reverse tunnel)을 사용한 패킷들의 적어도 일부를 인증하고 암호화하는 것이 요구될 것이다. Mobile IP 프로토콜에서 방화벽 횡단을 지원하는 방법이 제안되어 표준화된 후 설치될 때까지 방화벽 횡단을 위한 최선의 해법은 이동 노드가 방화벽의 횡단을 위해 방화벽과 특별한 계약을 할 수 있는 능력에 달려 있다. 이는 이동 노드가 소속 영역에 있는 망 관리자와 방문하는 망의 관리자와 접촉하여 방화벽을 횡단하는 특별 허가를 얻는 것을 의미한다.

방화벽 2를 횡단하는 두 번째 해법은 이동 노드들을 외국 영역과 고립된 영역에 포함시키는 것이다. 이 해법에서는 이동 노드가 외국 영역에 들어갈 때 제한된 부분망 내에서만 Mobile IP를 사용하도록 제한한다고 가정한다. 또한 그러한 부분망들은 방문 영역내의 다른 네트워크와의 접촉이 완전히 차단되나 부분망내에서는 자유로운 통신이 허락된다고 가정한다. 그러면 방문 영역을 보호하는 방화벽을 통과하는 어려움은 거의 없을 것이다. 그러나 방문 영역 내에 있는 노드들과의 통신은 이러한 구성에서는 매우 어려울 것이다. 이 해법은 외국 영역에서 이동 노드에게 인터넷에 연결하는 기능만을 제공하므로 지나치게 통신 기능을 제한하는 면이 있다. 이러한 제한을 완화하기 위해 방화벽 내에 보호되는 특정 호스트들과 통신할 수 있도록 할 수 있으나 이 또한 만족스럽지는 않은 방법이다. 따라서 일반적인 방화벽 횡단 문제는 쉬운 해법을 구할 수 없다. 그러므로 이 문제를 여러 단계로 풀려고 노력하는 것이 적절해 보인다.

Ⅳ. 이동 인터넷 프로토콜을 위한 질적으로 개선된 방화벽 횡단 해법

3장 2절에서 언급된 모든 영역을 보호하는 방화벽이 있는 일반적인 형태의 방화벽 횡단 문제는 쉬운 해법을 찾기가 매우 어렵다. 그러므로 이 문제를 간단한 문제부터 시작하여 여러 단계로 풀려고 하는 것은 합리적이다. 가장 간단한 문제인 소속 영역(home domain)만이 방화벽에 의해 보호되고 있는 경우에 이동 노드가 소속 영역 밖의 인터넷으로 나와 있을 때의 Mobile IP의 운용을 가능하게 하는 방화벽 횡단 해법들은 이미 제안되었다[4,5]. 이 장에서는 소속 영역과 외국 영역이 방화벽에 의해 보호되고 있는 경우에 이동 노드가 소속 영역 밖의 인터넷으로 나와 있을 때 Mobile IP 프로토콜을 사용하여 상대 노드와 인터넷 통신을 할 수 있는 해법을 제시한다. 즉, 이동 노드가 소속 영역과 외국 영역이 방화벽에 의해 보호되고 있는 경우에 소속 네트워크에 있을 때와 같은 연결성을 외부 네트워크에 있을 때 제공하는 것이다. 모든 영역이 방화벽에 의해 보호되고 있는 경우에는 이동 노드가 외국 네트워크에 있을 때나 소속 네트워크에 있을 때나 상대 노드와 Mobile IP를 사용하여 통신하는 것이 똑같이 어려우므로 이 논문에서는 고려하지 않는다.

소속 영역과 외국 영역이 방화벽에 의해 보호되고 있는 경우에 외국 영역에 있는 이동 노드에게 가는 혹은 이동 노드로부터 오는 Mobile IP 프로토콜의 패킷들은 다음과 같이 네 가지 종류로 나눌 수 있다.

(1) 이동 노드로부터 소속 대리인으로 가는 등록 요청(Registration Request) 패킷

(2) 이동 노드가 상대 노드로 보내는 패킷

(3) 소속 대리인으로부터 이동 노드로 가는 등록 답장(Registration Reply) 패킷

(4) 상대 노드가 이동 노드로 보내는 패킷

1. 가정

여기서 제시되는 방화벽 횡단 해법은 다음과 같은 가정들에 기초한다.

(1) 이동 노드는 자신의 현 위치와 소속 대리인에 도달하기 위해 횡단해야 하는 방화벽들의 존재를 알 수 있다.

(2) 해법을 단순화하기 위해 이동 노드의 소속 네트워크를 외부 인터넷으로부터 보호하기 위해 외부 인터넷과의 경계에 하나의 방화벽만이 있다.

(3) 이동 노드가 외국 영역에 있을 때 이동 노드와 소속 네트워크의 방화벽사이에 외국 영역을 외부의 인터넷으로부터 보호하는 하나의 방화벽이 있다.

(4) 모든 방화벽들은 IETF의 IP Security 작업반에 의해 제안된 인증과 암호화를 위한 표준 메커니즘들을 구현하고 있고 방화벽들 사이에 서로 보안 결합을 설정할 수 있다[10,11,13,14]. 방화벽들은 이러한 보안 결합으로 인증된 패킷들이 통과되는 것을 허용한다.

(5) 소속 영역밖에 있는 이동 노드와 소속 영역 내에 있는 소속 대리인 사이에는 임의의 수의 라우터들이 존재할 수 있다. 이러한 라우터들은 원시 주소 필터링을 구현한다. 즉, 이 라우터들은 원시 주소가 불명이거나 패킷이 도착하는 인터페이스와 일치하지 않는 패킷들을 버린다. 또한 모든 라우터들은 모르는 수신지를 가진 패킷들을 버린다.

(6) 방화벽에 의해 보호받는 영역 내에 있는 노드들은 서로 신뢰한다. 따라서 보호받는 영역 내에서 네트워크 링크 위에서 이동 노드의 트래픽을 암호화할 필요는 없다.

위의 가정 중 가정 (3)은 이미 제안된 방화벽 횡단 해법에는 없는 것이고 이 장에서 새로 제시되는 방화벽 횡단 해법을 기존의 해법과는 달리 대칭적인(symmetric) 해법으로 만들어 준다. 가정 (5)은 방화벽 횡단 해법 요구 사항들에 있는 것들보다 추가적인 제약 사항을 나타내고 있다[3].

2. 이동 노드로부터 나가는 패킷 처리 방법

이동 노드가 소속 영역밖에 있다는 사실을 알 때 이동 노드는 우선 외국 영역에 있는 방화벽과 보안 결합을 설정한다. 그런 다음에 이동 노드는 소속 영역에 있는 방화벽과 보안 결합을 설정한다. 이동 노드가 소속 대리인이나 상대 노드에게 패킷을 보내기 위해서는 이동 노드는 각 방화벽과 터널형 인증 헤더를 패킷 앞에 첨가한다. 또한 수송 계층 암호화 헤더가 인증 헤더를 첨가하기 전에 선택적으로 첨가될 수 있다.

각 방화벽에서 보안 정책은 패킷들을 처리하기 위하여 다음과 같이 구성되어질 수 있다.

(1) 패킷에 있는 인증 헤더를 확인하고 그 헤더에 포함된 보안 매개 변수 색인에 의해 참조된 보안 결합을 찾는다. 만약에 인증 헤더가 없다면 패킷을 버린다.

(2) 인증자 (authenticator)를 확인한다. 인증이 실패하면 패킷을 버린다.

(3) 암호화가 사용되어 ESP헤더가 있다면 새로운 패킷을 추출하기 위해 역암호화를 수행한다.

(4) 추출된 패킷이 수신지에 도착하기 전에 필터링 라우터에 의해 버려질 것 같다면 그 패킷을 다음 수신지까지 터널을 만들어 전송한다.

이동 노드가 Mobile IP 프로토콜을 사용하여 보내는 패킷은 두 가지가 있다. 즉, 이동 노드가 소속 대리인에게 보내는 등록 요청 패킷과 이동 노드가 상대 노드에게 보내는 패킷이다. 먼저 이동 노드가 소속 대리인에게 보내는 등록 요청 패킷은 두 개의 방화벽을 횡단하기 위하여 패킷에 두 개의 인증 헤더를 첨가하여 소속 대리인으로 보낸다. 이는 그림 3에 나타나 있다. 그림에서 실선은 이동 노드가 외국 대리인 전교 주소를 사용하여 외국 대리인을 통하여 보내는 경우이고 점선은 이동 노드가 배치된 전교 주소를 사용하여 직접 보내는 경우이다.

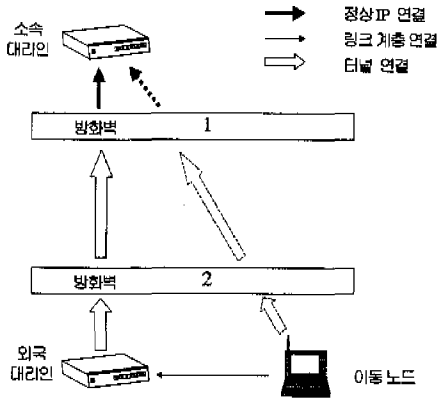


그림 3. 이동 노드가 소속 대리인에게 보내는 등록 요청 패킷의 경로

어느 경우에나 이동 노드가 보내는 등록 요청 패킷은 다음과 같다.

s=COA d=FW2	AH2	s=COA d=FW1	AH1	ESP	s=COA d=HA	Reg. Request

방화벽 2가 위의 패킷을 받을 때에 인증 헤더(AH2)을 검사한 후 적절하다고 판명되면 이 헤더를 제거하고 다음과 같은 등록 요청 패킷을 방화벽 1로 보낸다.

s=FW2 d=FW1	AH′	s=COA d=FW1	AH1	ESP	s=COA d=HA	Reg. Request

방화벽 1이 위의 패킷을 받은 후 인증 헤더(AH′)을 검사한 후 적절하다고 판명되면 그 안에 있는 인증 헤더(AH1)과 암호화 헤더(ESP)를 검사한다. 이러한 헤더들이 적절하다고 판명되면 이러한 헤더들을 제거하고 소속 대리인에게 다음과 같은 등록 요청 패킷을 보낸다.

s=FW1 d=HA	AH	s=COA d=HA	Reg. Request

소속 대리인은 위의 패킷을 받은 후 인증 헤더(AH)를 검사한 후 적절하다고 판단되면 이러한 헤더를 제거하여 이동 노드가 보낸 등록 요청 패킷을 추출한 후 이 패킷을 Mobile IP 프로토콜에 따라서 처리한다.

이동 노드가 상대 노드에게 보내는 패킷의 경우 Gupta등이 제안한 방화벽 횡단 해법에서는 이 패킷을 소속 대리인을 거쳐 상대 노드에게 보내는 최적이 아닌 라우팅을 사용하였다. 이를 개선하여 최적의 라우팅을 사용하기 위해 본 해법에서는 외국 영역에 있는 방화벽밖에 열린 노드 (Open Host 혹은 OH)를 두어 이동 노드가 상대 노드로 보내는 패킷을 외국 대리인 (혹은 이동 노드)가 캡슐화하여 열린 노드로 보낸다. 즉, 이동 노드가 외국 대리인 전교 주소를 사용하는 경우에는 이동 노드가 보낸 패킷을 외국 대리인이 받은 후 이를 캡슐화하여 열린 노드로 보낸다. 이동 노드가 배치된 전교 주소를 사용하는 경우에는 자신이 보내는 패킷을 캡슐화하여 열린 노드로 보낸다. 이 경우에는 이동 노드가 터널 만들어 보내기를 수행할 수 있는 기능을 가져야 한다. 열린 노드가 이 패킷을 받은 후 캡슐을 제거한 패킷을 상대 노드에게 보낸다. 열린 노드를 사용하는 것은 방화벽에 의해 보호되는 네트워크에 대해 부적절한 것은 아니다. 이미 방화벽을 가진 많은 조직들은 HTTP 프로토콜과 같은 열린 서비스를 제공하기 위해 그러한 노드들을 사용하고 있기 때문이다. 그러한 노드에 캡슐을 제거하는 기능을 추가하는 것은 상대적으로 비용이 적게 들것이다. 이러한 해법은 이동 노드로부터 상대 노드로 가는 경로의 길이를 거의 늘리지 않는다. 이러한 패킷들은 어떤 경우든지 방화벽을 통과해야만 할 것이고 열린 노드가 방화벽밖에 바로 있다면 오버헤드는 최소한으로 줄일 수 있을 것이다.

그림 4는 이동 노드가 상대 노드에게 보내는 패킷의 경로를 나타내고 있다. 그림에서 실선은 이동

노드가 외국 대리인 전교 주소를 사용하는 경우이고 점선은 이동 노드가 배치된 전교 주소를 사용하는 경우이다.

어느 경우에나 이동 노드가 보내는 패킷은 다음과 같다.

s=COA d=FW2	AH2	ESP	s=COA d=OH	s=MN home addr d=CN	Upper layer Payload

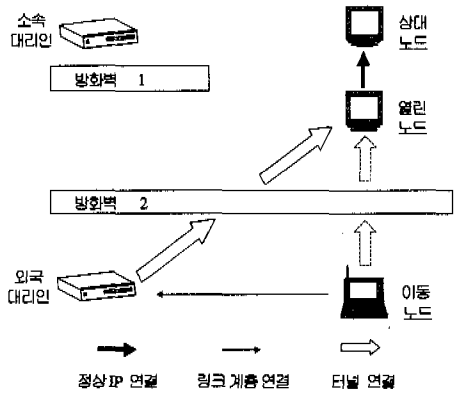


그림 4. 이동 노드가 상대 노드에게 보내는 패킷의 경로

방화벽 2가 위 패킷을 받을 때 인증 헤더(AH2)와 암호화 헤더(ESP)를 검사한 후 적절하다고 판명되면 이러한 헤더들을 제거한 후 다음과 같은 패킷을 열린 노드로 보낸다.

s=COA d=OH	s=MN home addr d=CN	Upper layer Payload

열린 노드는 위의 패킷을 받은 후 캡슐을 제거한 본래의 패킷을 상대 노드에게 표준 IP 라우팅을 사용하여 직접 보낸다.

3. 이동 노드로 들어오는 패킷 처리 방법

이동 노드가 Mobile IP 프로토콜을 이용하여 받는 패킷은 두 가지가 있다. 즉, 소속 대리인이 이동 노드로 보내는 등록 요청 패킷에 대한 등록 답장 패킷과 상대 노드가 이동 노드의 소속 주소를 수신지로 하여 보내는 패킷이다. 후자의 패킷은 상대 노드가 이동 노드의 새로운 전교 주소를 알기 전까지는 소속 네트워크로 보내질 것이다. 상대 노드가 그 패킷을 이동 노드의 소속 네트워크를 보호하는 방화벽 1을 횡단하기 위하여 필요한 방법을 알고 있고 그 방법을 사용하여 이동 노드에게 패킷을 보낸다고 가정한다.

먼저 소속 대리인이 이동 노드로 보내는 등록 답장 패킷은 방화벽을 통과하기 위하여 패킷에 인증 헤더를 첨가한 후 캡슐화하여 이동 노드로 보낸다. 이는 그림 5에 나타나 있다. 그림에서 실선은 이동 노드가 외국 대리인 전교 주소를 사용하는 경우이고 점선은 이동 노드가 배치된 전교 주소를 사용하는 경우이다.

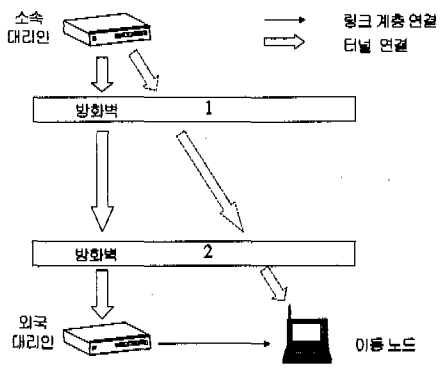


그림 5. 소속 대리인이 이동 노드로 보내는 등록 답장 패킷의 경로

어느 경우에나 소속 대리인이 이동 노드에게 보내는 패킷은 다음과 같다.

s=HA d=FW1	AH	s=HA d=COA	Reg. Reply

방화벽 1이 위 패킷을 받은 후 인증 헤더(AH)을 검사한 후 적절하다면 헤더를 제거한 후 본래의 패킷을 추출한다. 방화벽 1의 보안 정책은 다음과 같이 정해져야 한다. 한 패킷이 보안 결합이 존재하는 수신지로 전송되어진다면 적절한 IP 보안 프로토콜의 헤더들이 전송하기 전에 패킷 앞에 첨가되어져야만 한다. 이러한 정책의 결과로 방화벽 1은 본래의 패킷을 다음과 같이 캡슐화한 패킷을 만들어 방화벽 2로 보낸다.

s=FW1 d=FW2	AH	s=FW1 d=COA	AH"	ESP	s=HA d=COA	Reg. Reply

방화벽 2가 위의 패킷을 받은 후 인증 헤더(A

H′)을 검사한 후 적절하다면 이 헤더를 제거하고 외국 대리인 (혹은 이동 노드)에게 다음과 같은 패킷을 보낸다.

s=FW1 d=COA	AH″	ESP	s=HA d=COA	Reg. Reply

외국 대리인은 위 패킷을 받은 후 인증 헤더(AH″)과 암호화 헤더(ESP)를 검사한 후 적절하다면 캡슐을 제거하여 본래의 등록 답장 패킷을 추출하여 이동 노드에게 보낸다. 이동 노드가 위 패킷을 받는다면 캡슐을 제거하는 일을 하고 본래의 등록 답장 패킷을 추출하여 Mobile IP 프로토콜에 따라 처리한다.

상대 노드가 이동 노드에게 보내는 패킷은 소속 대리인을 거쳐 이동 노드에게 보내지는 최적이 아닌 라우팅을 사용한다. 이는 상대 노드가 이동 노드의 현재 전교 주소를 모르는 한 피할 수 없다. 그림 6에 상대 노드가 이동 노드에게 보내는 패킷의 경로가 나타나 있다. 그림에서 실선은 이동 노드가 외국 대리인 전교 주소를 가진 경우이고 점선은 배치된 전교 주소를 가진 경우이다.

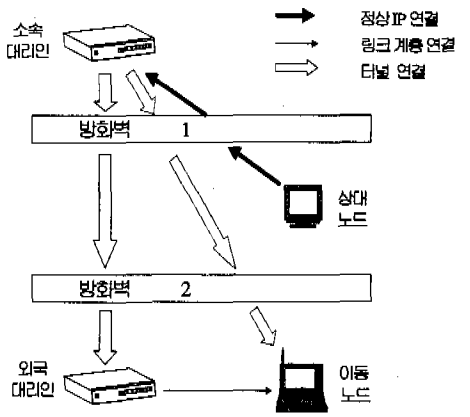


그림 6. 상대 노드가 이동 노드로 보내는 패킷의 경로

상대 노드가 보내는 패킷은 소속 대리인이 중간에서 받은 후 다음과 같이 캡슐화하여 보낸다.

s=HA d=FW1	AH	s=HA d=COA	s=CN d=MN home addr	Upper layer Payload

이후의 경로에서 방화벽 1, 방화벽 2와 외국 대리인이 위의 패킷에 대응하여 처리하는 과정은 소속 대리인이 이동 노드에게 등록 답장 패킷을 보내는 경우와 대동소이하다.

V. 기존 해법들과 비교

오늘날 거의 모든 기관/회사의 LAN들은 학교의 LAN을 제외하고는 대부분 방화벽에 의해 보호되고 있다. 따라서 이동 노드가 외국 영역에서 인터넷에 접속할 때 그 영역은 방화벽에 의해 보호되고 있을 가능성이 보호되고 있지 않을 가능성보다 훨씬 더 높다고 할 수 있다. 현재 방화벽에 의해 보호되고 있는 외국 영역에 있는 망에 이동 노드가 접속하여 통신하는 경우의 (3장의 마지막 부분에 기술된 Idea 수준의) 해법들은 간단하나 수동적 절차(이러한 절차에 대해 정의된 프로토콜이 아직 없음)를 거치거나 통신 기능을 제한한다는 등의 문제를 가지고 있는 만족스럽지 않은 해법들이다. 본 해법은 이러한 문제를 해결한 첫 번째 해법이다. 또한 이동 노드가 외국 영역에 있을 때에도 소속 네트워크에 있을 때와 거의 같은 연결성을 제공한다. 더욱이 이동 노드가 상대 노드에게 패킷을 보낼 때 본 해법에서는 소속 네트워크를 거치지 않고 열린 노드를 거쳐 상대 노드에게 직접 보내므로 거의 최적화된 라우팅을 사용하는 해법이다.

현재 발표된 가장 대표적인 이동 인터넷 프로토콜을 위한 방화벽 횡단 해법인 Montenegro 해법[5]은 소속 영역만이 방화벽에 의해 보호되는 경우의 해법이다. 따라서 본 해법과 기본적인 가정이 다르기 때문에 직접 비교하는 것은 적절하지 않다. Montenegro 해법과 본 해법과의 주요 차이점과 질적인 개선점은 다음과 같고 이는 표 1에 요약되어 있다.

(1) Montenegro 해법에서는 소속 네트워크가 방화벽에 의해 보호되고 방화벽내의 네트워크는 사설 네트워크로서 사설 (IP) 주소를 사용한다고 가정한다. 또한 상대 노드가 소속 네트워크와 다른 사설 네트워크에 있는 경우는 고려하지 않는다. 반면에 본 해법에서는 소속 네트워크뿐만이 아니라 이동 노드가 방문하고 있는 네트워크도 방화벽에 의해 보호되고 있는 경우를 고려하고 표준 라우팅 메커니즘을 사용하여 패킷을 전달할 수 있는 공중 (IP) 주소 (public address)를 사용한다. 따라서 본 해법은 더 일반적이고 대칭적이다.

(2) Montenegro 해법에서는 ESP 프로토콜과 AH

프로토콜과 같이 SKIP 프로토콜을 사용하여 패킷을 암호화한다. 반면에 본 해법에서는 ESP 프로토콜과 AH 프로토콜만을 사용하여 패킷을 암호화한다. 따라서 SKIP이라는 특정 프로토콜을 사용하지 않고 인증 및 암호화 프로토콜을 사용한다는 점에서 본 해법이 더 일반적인 해법이다.

(3) Montenegro 해법에서는 이동 노드가 배치된 전교 주소를 사용한다고 가정하고 있으나 본 해법에서는 배치된 전교 주소뿐만이 아니라 외국 대리인 전교 주소를 사용하는 경우도 고려한다. 따라서 본 해법이 더 일반적이다.

표 1. Montenegro 해법과의 비교

	Montenegro 해법	본 해법
방화벽이 있는 네트워크	소속 네트워크	소속 네트워크, 외국 네트워크
상대 노드의 위치	소속 네트워크	어느 네트워크 (Any Network)
인증 및 암호화 프로토콜	AH, ESP, SKIP	AH, ESP
소속 네트워크의 유형	사설 네트워크	공중 네트워크
이동 노드의 전교주소	배치된 전교주소	배치된 전교주소, 외국 대리인 전교주소
라우팅	최적이 아님	최적
연결성	제한적	일반적
적용성	제한적	일반적

본 해법을 실제로 적용할 경우의 오버헤드는 이동 노드가 이동 지원 대리인들 및 방화벽들과 인증 절차를 거치는 것과 이동 노드가 주고 받는 패킷을 암호화하는 것과 열린 노드를 사용함에 따른 오버헤드 등을 들 수 있다. 인증 절차는 이동 노드가 이동 지원 대리인과 통신하기 위해서 또한 방화벽들을 통과하기 위해서 거쳐야 하고 이중 일부는 Mobile IP 프로토콜에서도 명시되어 있다. 암호화는 안전한 보안 채널을 구성하는 경우에 필요하므로 이동 노드가 주고 받는 패킷들을 적대적인 사용자들로부터 보호하기 위해서는 필요하고 보호할 필요가 없다면 암호화 기능을 제거하면 된다. 열린 노드를 사용하는 경우의 오버헤드는 열린 노드를 방화벽밖에 바로 위치하게 함으로써 최소한으로 줄일 수 있다.

VI. 결 론

본 논문은 Mobile IP 프로토콜을 위한 질적으로 개선된 방화벽 횡단 해법을 제안한다. 본 논문에서 제안된 방화벽 횡단 해법은 소속 영역뿐만이 아니라 방문하고 있는 외국 영역도 방화벽에 의해 보호되고 있는 경우에 이동 노드가 Mobile IP 프로토콜을 사용하는 것을 가능하게 한다. Montenegro 등이 제안한 해법은 소속 영역만이 방화벽에 의해 보호되는 비대칭적 해법인데 비해 본 해법은 대칭적 해법이다. 따라서 본 해법은 이동 노드가 보편화되고 있는 방화벽에 의해 보호되고 있는 외국 영역에 있을 때에도 소속 네트워크에 있을 때와 거의 같은 수준의 연결성을 제공한다. 또한 본 해법은 Montenegro 등의 해법보다 일반적인 가정을 사용하므로 보다 더 일반적인 경우에 적용할 수 있다. 그 밖에 본 해법은 이동 노드가 상대 노드에게 패킷을 보내는 경우에 소속 대리인을 거치지 않고 외국 영역 밖의 열린 노드를 통하여 직접 보내므로 최적의 라우팅을 사용하는 해법이라고 볼 수 있다. 본 해법의 이러한 기능은 열린 노드를 사용하고 보내는 패킷에 필요한 헤더들을 추가하는 등의 최소한의 오버헤드를 사용함으로써 이루어진다.

본 해법에서는 Mobile IP 프로토콜을 사용할 때 이동 노드로부터 나가는 패킷과 이동 노드로 들어오는 패킷을 나누어 처리하고 소속 대리인, 외국 대리인 및 열린 노드 등과 같은 신뢰성이 있는 노드들이 개입하기 때문에 Mobile IP 프로토콜은 충분한 인증을 사용한다면 어떤 형태의 방화벽이나 패킷 필터를 통하여서도 안전하게 사용될 수 있음을 보여 준다. 이동 노드는 자신의 소속 영역을 둘러싸고 있는 보안 경계를 확장하는 역할을 해야 한다. 그러므로 소속 영역을 외부인들로부터 보호하는 책임을 공유해야 한다. 특히 사용자 고유의 인증을 위한 정보가 없는 경우에는 이동 노드인 척 하는 노드는 또한 소속 네트워크에 접속할 수 있다는 사실을 유의해야 한다.

참 고 문 헌

[1] C. E. Perkins, "IP Mobility Support", *RFC 2002*, October 1996.

[2] C. E. Perkins, "Mobile IP", *IEEE Communications Magazine*, Vol. 35, No. 5, pp. 84-99, May 1997.

[3] V. Gupta and S. Glass, "Firewall Traversal for Mobile IP: Goals and Reguirements", *Draft <draft-ietf-mobileip-ft-reg-00.txt>*-work in progress, January 1997.

[4] V. Gupta and S. Glass, "Firewall Traversal for Mobile IP: Guidelines for Firewalls and Mobile IP entities", *Draft <draft-ietf-mobileip-firewall-trav-00.txt>* -- work in progress, March 1997.

[5] G. Montenegro and V. Gupta, "Sun's SKIP Firewall Traversal for Mobile IP", *RFC 2356*, June 1988.

[6] A. Aziz and M. patterson, "Simple Key - Management for Internet Protocols (SKIP)", *Proc. INET'95*

[7] G. Montenegro, "Reverse Tunneling for Mobile IP", *Draft <draft-ietf-mobileip- tunnel-reverse-04.txt>* -- work in progress, August 1997.

[8] C. E. Perkins, *Mobile IP: Design Principles and Practices*, Addison-Wesley, pp. 275, 1998.

[9] M. Leech, M. Ganis, Y. Lee, R. Kuris, D. Koblas, and L. Jones, "SOCKS Protocol Version 5", *RFC 1928*, March 1996.

[10] R. Atkinson, "IP Authentication Header", *RFC 1826*, August 1995.

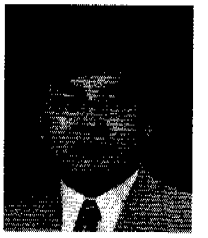
[11] R. Atkinson, "IP Encapsulating Security Payload(ESP)", *RFC 1827*, August 1995.

[12] J. Zao et al., "Public-Key Based Secure Mobile IP", *Proc. ACM Mobicom 97*, ACM, New York, pp. 173-184, October 1997.

[13] R. Oppliger, "Internet Security: Firewalls and Beyond", *Communications of the ACM*, Vol. 40, No. 5, pp. 92-102, May 1997.

[14] R. Atkinson, "Security Architecture for the Internet Protocol", *RFC 1825*, August 1995.

이 충 기(Chungki Lee) 정회원



1979년 : 서울대학교 계산통계학과(이학사)

1981년 : 서울대학교 계산통계학과(이학석사)

1993년 : Georgia Institute of Technology(전산학박사)

1994년 5월~1996년 2월 : 한국전산원 표준본부 선임연구원

1996년 3월~현재 : 명지대학교 전자정보통신공학부 조교수

<주관심 분야> 차세대 인터넷 기술, 이동 컴퓨팅, 분산 시스템, 네트워크 보안