안전한 방화벽 Traversal을 제공하는 Mobile IP의 보안 메커니즘

진 민 정[†] · 박 정 민[††] · 채 기 준[†††]

요 약

Mobile IP는 이동 노드가 이동하는 동안 통신의 단절없이 IP 서비스를 제공하기 위하여 고안된 프로토콜로 외부 네트워크로 이동한 이동 노드는 마치 내부망에 있는 것과 같이 서비스를 받을 수 있다. 기업망과 같은 대부분의 내부망은 방화벽에 의해서 보호되고 있으며 이동 노드들은 보통 무선 링크로 연결된다. 따라서 Mobile IP를 이와 같은 실제 네트워크 환경에서 성공적으로 사용하려면 이동노드가 내부망에 있는 것과 같은 보안 서비스를 받을 수 있어야 한다. 본 논문에서는 방화벽으로 보호되는 내부망의 이동 노드가 외부 네트워크로 이동한 경우에도 안전하게 통신할 수 있도록 하기 위하여 Mobile IP에 IPSec 터널을 통합한 보안 기법을 제안하였다. 시뮬레이션 결과를 통해서 제안한 보안 기법은 기존의 Mobile IP 터널링 기법에 비해 성능상의 차이를 보이지 않으면서 효율적으로 보안서비스를 제공함을 확인할 수 있었다.

Security Mechanism for Firewall Traversal in Mobile IP

Minjeong Jin[†] · Jung-Min Park[††] · Kijoon Chae[†††]

ABSTRACT

Mobile IP is designed to provide IP services to roaming nodes. Mobile users take advantage of this protocol to obtain the services as if they were connected to their home network. In many cases mobile users is connected through a wireless link and is protected by corporation's firewall in virtual private network. In order to have a successful deployment of Mobile IP as an extension of a private network, security services should be provided as if the mobile node were attached to its home network. In this paper, we propose the security mechanism of combining Mobile IP and IPSec tunnels, which can provide secure traversal of firewall in a home network. The simulation results show that the proposed mechanism provides the secure and efficient communication.

키워드 : Mobile IP, 보안, 방화벽 통과, IPSec, 터널링

1. 서 론

노트북, 휴대전화, PDA 등과 같은 이동 단말기를 통해 인터넷 서비스를 받고자 하는 요구가 늘어남에 따라 사용자의 이동성을 지원하기 위한 다양한 기술들이 개발되어 왔으며 이동 중의 서비스 제공을 위한 연구가 매우 활발히 이루어지고 있다. IETF(Internet Engineering Task Force)[1]에서는 LAN 환경의 무선 통신 환경을 이용하면서 통신망을 위한 데이터그램 교환은 기존의 유선 인터넷 망을 그대로 이용할 수 있도록 하기 위하여 Mobile IP[2, 3]를 제안하였다.

무선 인터넷 환경은 유선 네트워크 환경보다 안전한 통신을 위해서 더욱 더 높은 신뢰성과 보안성을 요구한다. 현재의 유선 인터넷 환경에서 개인의 사생활과 기업의 기밀, 금융 거래, 국방 외교 및 기타 공공 기관의 네트워크는 VPN (Virtual Private Network)으로 이루어지기도 하며 방화벽을 통해서 내부의 네트워크를 보호하고 있어서 인증된 사용자만이 접근할 수 있도록 한다. 그러나 Mobile IP는 방화벽이 있는 네트워크 구조에서 잘 동작하도록 고려하여 설계되지 않았으므로 이동 노드의 통신에 있어서 안전한 동작을 보장하지 못한다. 예를 들면 방화벽으로 보호된 내부 네트워크에 있던 이동 노드가 외부 네트워크로 이동하였을 경우 다음과 같은 문제들이 발생하게 된다. 첫째로 외부 네트워크로 이동한 이동 노드가 인터넷과 같은 공중망을 통하여 패킷을 전송할 때 이동노드의 트래픽은 공격당하기 쉽다. 둘째로 방화벽은 인증된 사용자만 접근을 허용하고 패킷 필터링 기능이 있으므로 외부 네트워크로 이동한 이동 노드가 내부망의 홈 에이전트에게 보내는 패킷을 중간에서 차단한다. 셋째, 이동 노드가 내부 망에서 사용하던

※ 본 논문은 정보통신부 정보통신연구진흥원에서 지원한 ITRC 프로그램 및 2002년도 정보통신기초연구지원사업의 연구결과입니다.
† 정 회 원 : 이화여자대학교 과학기술대학원 컴퓨터학과
†† 준 회 원 : 이화여자대학교 과학기술대학원 컴퓨터학과
††† 종신회원 : 이화여자대학교 컴퓨터학과 교수
논문접수 : 2003년 10월 13일, 심사완료 : 2004년 1월 19일

내부 주소는 외부 네트워크로 이동하였을 때 사용할 수 없게 되므로 이동 노드는 홈 네트워크와 통신이 단절된다. 따라서 방화벽으로 보호받고 있는 내부망의 이동노드가 외부 네트워크로 이동했을 때 이동 노드가 안전하게 내부망과 통신할 수 있도록 하는 안전한 방화벽 통과기법(traversal mechanism)이 필요하다.

본 논문에서는 내부망의 이동 사용자가 외부 네트워크로 이동하였을 경우 공중망을 경유하여 방화벽으로 보호되고 있는 내부망까지 기밀 데이터를 전송할 수 있도록 하기 위하여 Mobile IPv4 프로토콜의 터널링에 IPSec 기술을 적용한 안전한 터널링 기법을 제안하였다. 제안한 터널링 기법은 IPSec과 Mobile IP 터널링을 통합한 것으로서 제안한 방법의 적합성을 검증하기 위하여 터널링 적용 방법을 네 가지 경우로 모델링하고 각각에 대하여 성능을 측정·분석하였다.

본 논문의 구성은 다음과 같다. 1장의 서론에 이어 2장에서는 관련 연구들에 대해 살펴보고 3장에서는 본 논문에서 제안하는 안전한 터널링 기법에 대하여 상세히 설명한다. 4장에서는 제안한 터널링 기법의 성능을 분석하기 위하여 네 가지 터널링 기법에 대한 시나리오를 설명하고 네 가지 시나리오를 시뮬레이션하여 성능을 비교·분석한다. 마지막으로 5장에서는 본 논문의 결론을 맺는다.

2. 관련 연구

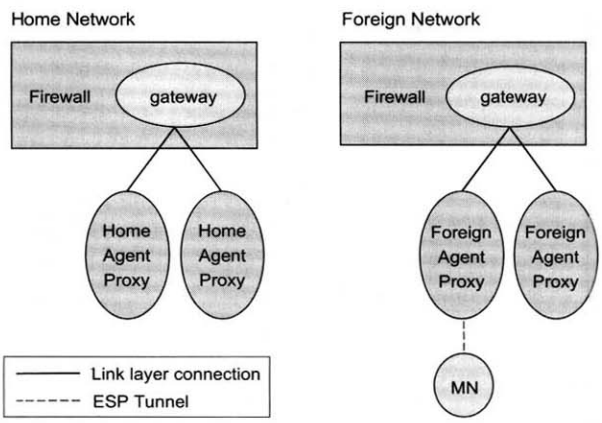
방화벽으로부터 보호받고 있는 내부망의 이동 노드가 외부 네트워크로 이동했을 경우 이동 노드는 내부망에 접속해 있을 때와 마찬가지로 외부 네트워크에서도 방화벽의 보호를 받을 수 있어야만 한다. 그리고 이동 노드가 외부 네트워크로 이동했을 때 자신의 홈 네트워크와 통신하고자 할 경우 방화벽이 그 패킷들을 내부망으로 전송해야만 한다. 1997년 IETF에서 논의되기 시작한 Mobile IP의 방화벽 통과에 대한 보안 관련 연구는 다음과 같은 세 가지 기법으로 분류된다.

2.1 어플리케이션 프록시 기법

SOCKS 프로토콜은 일반적으로 방화벽을 통과하기 위해서 제공되는 프로토콜이며 서버-클라이언트 방식으로 방화벽을 통과하도록 한다. 이 기법은 Mobile IP에서의 방화벽 통과 기법 중에서 제일 처음으로 제안된 방법으로 SOCKS 프로토콜을 사용한다. 즉, 방화벽을 SOCKS 서버로 간주하여 방화벽과 외부 망으로 이동한 이동노드 사이에는 TCP 세션을 설정하여 이동노드가 방화벽과 UDP 트래픽을 교환한다. 이 때 프로토콜로 SOCKS 프로토콜을 사용하며 클라이언트에 해당되는 이동노드가 이동하여 방화벽을 통해서 실제로 데이터를 보내기 전에 인증형태에 따라 차이는 있지만 최소한 4회의 라운드 트립 지연이 발생한다. 이 과정은 이동노드가 이동하여 새로운 의탁주소(Care-of-Address)를 등록할 때마다 수행되어야 하므로 매우 비효율적이다. 더불어 어떻게 인증된 연결을 설정하는지에 대하여 정의하고 있으나 트래픽 암호화에 대한 명확한 방법이 제시되지 않았다. 또한 이 방법은 SOCKS 서버인 최소한 하나의 상업용 네트워크가 필요하며, SOCKS 서버의 네트워크 관리자가 강력한 인증 기법을 구성하지 않는다면 네트워크의 보안에 문제가 생기게 되는 제한점이 있다.

2.2 구조적 접근 기법

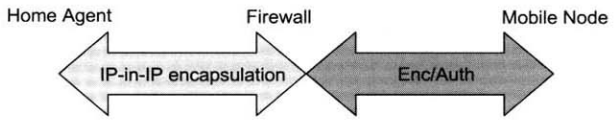
Mink 등이[5] 제안한 FATIMA(Firewall-Aware Transparent Internet Mobility Architecture)가 이 방법으로 분류된다. FATIMA는 계층적인 구조를 가진다는 점에서 기존 연구와 유사하지만 계층구조의 루트노드는 네트워크의 방화벽 기능이 통합된 게이트웨이로 홈 에이전트와 외부 에이전트 역할을 수행한다[5]. 따라서 보안의 중요한 기능은 FATIMA 게이트웨이에 집중된다. 또한 모든 구성요소간의 제어 및 트래픽은 ESP(Encapsulating Security Payload Header) 터널로 이동노드와 외부 네트워크 사이에 상호 인증이 제공된다. 이 기법은 보안 서비스를 통합할 뿐만 아니라 기존의 Mobile IP 구현에 있어서 투명성을 제공하며 다른 기법과 달리 미세 이동성을 지원하며 규모가 큰 네트워크에서 라우팅 에이전트를 계층적인 구조로 설계함으로써 확장성을 제공할 수 있는 장점이 있다. FATIMA 구조에 대한 개념을 그림으로 도시하면 (그림 1)과 같다. 그러나 기존 네트워크에 FATIMA 게이트웨이와 같은 새로운 구성요소들을 추가해야하므로 개발비용이 커지며 FATIMA 게이트웨이에 보안이 집중되므로 시스템 집중화에 따른 단일 노드 오류(single node failure)의 문제가 발생하는 단점이 있다.



(그림 1) FATIMA 구조도

2.3 IP 기반 기법

Mobile IP에서 이동 노드가 외부 네트워크로 이동하여 방화벽으로 트래픽을 전송할 때 세션리스(session-less) IP 보안 기법을 사용하여 암호화와 인증을 제공하는 방법으로 대표적인 연구 예로는 Montegro 등[6]의 방법이 있다. 이 방법을 개념적으로 나타내면 (그림 2)와 같다. 홈 네트워크와 방화벽사이는 Mobile IP 터널링의 대표적인 방법인 IP-in-IP로 터널링하고 방화벽과 이동노드 사이는 SKIP(Simple Key-Management for Internet Protocol) 터널링한다[7, 8].



(그림 2) SKIP 터널링

이 방법에서는 키 관리, 인증, 암호화를 위하여 공개키 기반 구조인 SKIP을 사용한다. SKIP은 송신자의 공개키 기반 이름을 이용하여 인증 기능을 제공한다. 홈 네트워크의 통신노드와 이동 노드사이에 데이터를 교환하는 경우 먼저 통신노드가 이동 노드로 보낸 패킷을 홈 에이전트가 가로채어 방화벽으로 전달하고 방화벽은 이동 노드와의 보안 연계(security association)를 통하여 패킷을 SKIP으로 보호하여 전송한다. 이동 노드에서 통신노드로 데이터를 전송하는 경우 SKIP으로 보호하여 방화벽으로 전달한 후 인증과정을 거쳐 통신노드로 전송한다. 이 기법은 이동 노드들이 SKIP을 구현하고 있다는 것을 가정한다. 따라서 이러한 가정은 다음과 같은 몇 가지의 다른 가정을 전제로 하며 제한점을 가진다. 방화벽과 이동노드가 Diffie-Hellman 공개키로 서로 인증되어있어야만 하는데 어떻게 구성하는지에 대하여 명시하지 않았다. 이것은 이동 노드의 수가 작은 경우에는 손쉽게 가능하지만 이동노드의 수가 많아질 때는 융통성(scalability)을 위해서 공개키 기반구조(Public Key Infrastructure)가 필요하게 된다. 이동 노드가 방화벽을 통하여 등록 요청을 보낼 때 이동노드의 주소와 의탁주소의 이전 바인딩을 대치시킨다. 이것은 동시 바인딩(simultaneous binding)이 불가능함을 의미한다. 방화벽이 동시 바인딩을 제공하도록 수정할 수는 있지만 그와 같은 경우는 방화벽에 Mobile IP를 구현해야만 하는 단점이 생긴다. 각 SKIP 패킷은 SKIP 헤더를 포함하므로 이것 또한 심각한 부담이 된다. 또한 사용되는 인증과 암호화 알고리즘이 패킷 자체에 명시되므로 공격자의 이용을 쉽게 만든다.

지금까지 Mobile IP 네트워크 환경에서 방화벽 통과에 관한 연구들의 특징에 대해서 살펴보았다. 어플리케이션 프록시 기반 방법은 라운드 트립 지연과 상용 네트워크 구조가 필요하다는 점에서, 구조 기반 기법은 각각에 맞는 구조를 설계하고 구현해야 하는 비용측면에서 문제가 있다. IP 기반 구조의 SKIP 프로토콜을 이용한 방법은 이동노드와 방화벽사이에 상호 신뢰 관계를 설정하기 위해 발생하는 라운드 트립 지연시간이 없으며 방화벽은 첫 번째 패킷을 받자마자 이동노드에 대한 패킷을 전송(relay)하기 시작하므로 프록시 기반 방법보다 좋지만 IKE(Internet Key Exchange)에 비해 키 관리와 보안 연계에 있어서 오버헤드가 크며 ISAKMP/Oakley(Internet Security Association and Key Management Protocol/Oakley Key Determination Protocol) 대신에 공개키 기반의 SKIP을 사용함으로써 Mobile IP의 보안문제를 쉽고 효율적으로 해결하고자 하였으나 모든 이동 노드들이 새로운 프로토콜인 SKIP을 필요로 하게 되므로 단점이 있었다. 따라서 Mobile IP에서 이동노드와 방화벽간에 안전한 통신을 위하여 적합한 키 관리 기술을 선택하고 터널링으로 교환되는 패킷의 오버헤드를 줄이는 것이 중요하다.

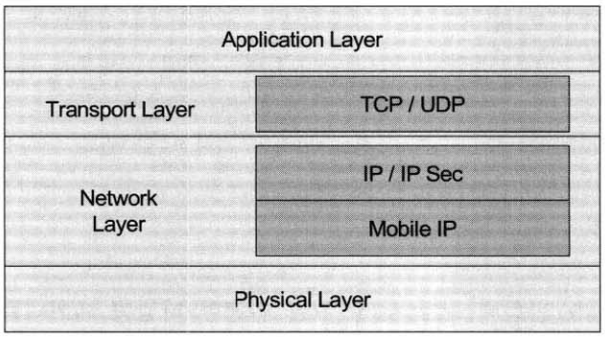
3. 방화벽 Traversal을 위한 안전한 터널링 메커니즘

3.1 제안한 안전한 터널링 기법

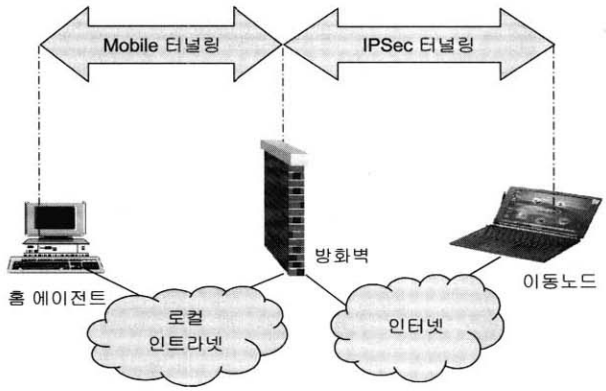
본 논문에서는 외부 네트워크로 이동한 이동노드가 내부망을 보호하고 있는 방화벽을 안전하게 통과하기 위한 방법으로서 Mobile IP 터널링과 IPSec 터널링을 통합한 방법을 제안하고자 한다. 외부 네트워크로 이동한 이동노드가 자신이 소속된 내부망에 접근하기 위해서 내부망을 보호하고 있는 방화벽을 통과하기 위한 방법으로 IPSec을 통한 인증과정을 거치게 된다. 터널링을 생성하기 전에 방화벽과 이동노드는 미리 비밀키를 생성하여 공유해야 한다. 이때 비밀키는 이동노드가 내부망에 있을 때 미리 교환되므로 쉽게 비밀키를 생성할 수 있다. 이동 노드와 방화벽간에 보안을 제공하는 IPSec 터널이 설립되면, 그들간에 교환되는 모든 패킷에 인증과 암호화 기법이 적용되므로 강력한 보안을 제공하며 동시에 경량의 Mobile IP를 실행할 수 있다. 본 논문에서는 Mobile IP 패킷이 인터넷을 통하여 내부망의 방화벽까지 전송될 때 Mobile IP 패킷을 보호하기 위하여 IPSec의 터널모드를 사용한다. 이를 위해서 AH(Authentication Header) 또는 ESP(Encapsulating Security Payload Header)필드가 IP에 덧붙여진 후에 전체 패킷과 보안 필드는 새로운 바깥 IP 헤더를 가진 새로운 바깥 IP 패킷의 페이로드로 다루어진다. 이 패킷은 IP 네트워크의 한 장

소로부터 다른 곳으로 터널을 통하여 이동한다. 데이터가 이동하는 도중 내부에 있는 IP 헤더를 점검할 수 있는 라우터는 없다. 원래의 패킷은 캡슐화되어 있기 때문에 AH와 ESP가 적용된 새롭고 더 커진 패킷은 보안이 이루어진 상태에서 완전히 다른 발신지와 목적지 주소를 가질 수 있다. 이러한 터널 모드는 보안 연계의 종단 중 한쪽이 IPSec이 실행되는 방화벽이나 라우터 같은 보안 게이트웨이일 경우에 사용된다. 방화벽을 통과한 후 내부 망에서는 IPSec 을 실행하지 않고 Mobile IP 터널링 만으로도 충분히 보안을 유지할 수 있다.

(그림 3)과 (그림 4)는 안전한 터널링 형태를 나타내며 본 논문에서는 이와 같은 터널링 기법으로 보안을 제공한다.



(그림 3) IPSec과 Mobile IP의 통합 구조



(그림 4) 안전한 터널링 기법

홈 에이전트와 이동 노드간에 통신 경로는 중간에 위치한 방화벽으로 분리된다. 방화벽과 이동 노드간에 터널링은 암호화 및 인증 기법이 사용되고, 홈 에이전트와 방화벽간에는 Mobile IP 터널링 기법인 IP-in-IP 터널링만 적용된다. 방화벽으로 보호되고 있는 네트워크에서는 각자가 신뢰성을 가지기 때문에 방화벽과 홈 에이전트간에 인증은 불필요하다. 이 구조에서 한 가지 중요한 특징은 방화벽이 이동 노드와 홈 에이전트의 인증 책임을 가진다는 것이다. 외부 네트워크에 있는 이동노드가 내부망에 있는 홈 에이전트를 목적지로 하는 IP 패킷을 생성한다. 이때 이동 노드는 IPSec 절차를 수행하고 외부 IP 헤더 안에 패킷을 캡슐화한다. 이 외부 IP 패킷의 발신지 주소는 이동노드의 의탁주소(CoA)가 되고 목적지 주소는 방화벽이 된다. 이제 이 패킷은 방화벽으로 전송되는데 중간 라우터의 점검은 오로지 외부 IP 헤더에 의해서만 이루어진다. 내부망의 방화벽에서 외부 IP 헤더는 벗겨지고 내부 패킷이 홈 에이전트에게 전달된다. 터널 모드에서 ESP는 암호화하고 선택적으로 내부 IP 헤더를 포함하는 전체 내부의 IP 패킷을 인증한다. 터널 모드에서 AH는 전체 내부의 IP 패킷과 바깥 IP 헤더의 선택적인 부분을 인증한다.

3.2 터널링에 적용된 보안 메커니즘

본 논문에서는 안전한 키 관리를 위하여 ISAKMP/Oakley를 선택하였다. ISAKMP/Oakely는 SKIP[6]과 유사하지만 보안 연계 협상 후에 모든 패킷들이 교환되므로 키에 대한 오버헤드가 낮으며 키 관련 헤더를 포함하지 않으므로 SKIP보다 단순하다. 또한 이 기법은 공격자가 암호화와 인증을 위해서 어떤 알고리즘이 사용되었는지 알 수 없게 하므로 강력한 보안을 제공한다는 장점을 가진다.

제안한 안전한 터널링에서 데이터의 무결성을 제공하기 위한 인증 알고리즘은 HMAC-MD5[9]가 선택되었다. 해쉬 알고리즘은 해쉬값을 계산하는 시간이 암호화·복호화 수행 시간에 비해 매우 작기 때문에 터널링의 성능에 많이 영향을 미치지는 않지만 전반적인 네트워크의 성능을 고려하였을 때 중요한 문제가 아닐 수 없다. 따라서 본 논문에서는 AH 프로토콜에 적합한 인증 알고리즘을 HMAC-MD5로 결정하였다. 또한 ESP를 위한 암호화 알고리즘은 DES-CBC로 선택하였다. 4장에서 입증된 사실이지만 MD5와 마찬가지로 IPSec에서 사용되는 암호화 알고리즘 중 수행속도가 가장 빠르다는 장점을 가진다.

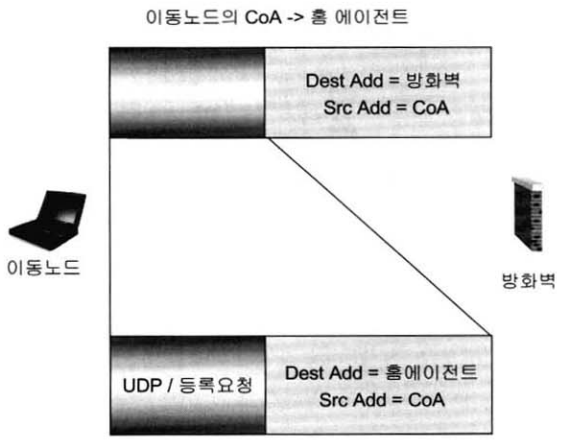
3.3 패킷 설계

소스 필터링(source filtering)과 내부 주소(private address)를 사용하는 방화벽을 통과하기 위해서 요구사항에 맞는 패킷의 타입을 고려해야 한다. 소스 필터링과 내부주소의 문제는 역 터널링(reverse tunneling) 기법[10]을 이용하여 해결할 수 있다. 이동 노드가 홈 에이전트와 통신하기 위하여 자신이 생성한 패킷의 소스 주소를 내부 주소를 사용하지 않고 역 터널링 기법을 이용하여 새로 부여받은 CoA로 지정하여 홈 에이전트에게 전송하게 된다. 그러나 역 터널링 기법을 이용하기 위해서는 새로운 형태의 패킷을 필요

로 한다. 본 논문에서는 역 터널링을 위해 사용하는 패킷을 진입 패킷과 진출 패킷이라 부른다.

3.3.1 진입 패킷

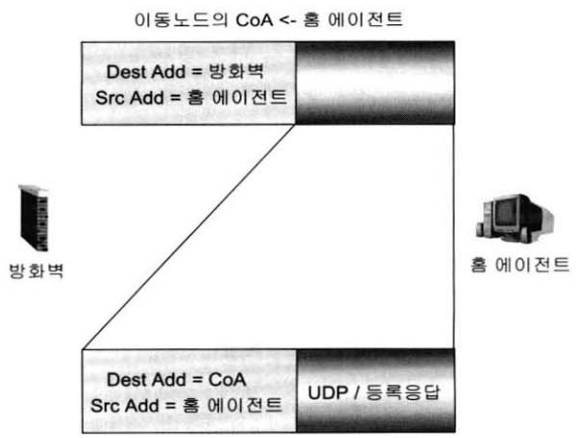
이동 노드가 홈 에이전트에게 등록 요청 패킷과 데이터그램을 전송하고자 할 때 이 트래픽은 역 터널링되며 이를 내부망으로 들어가는 진입패킷이라 한다. 이 경우 가장 바깥의 IP 헤더의 발신지 주소는 이동노드의 의탁주소가 되고 목적지 주소는 내부망에 있는 방화벽 주소가 된다. (그림 5)는 진입패킷을 나타낸다.



(그림 5) 진입 패킷 형태

3.3.2 진출 패킷

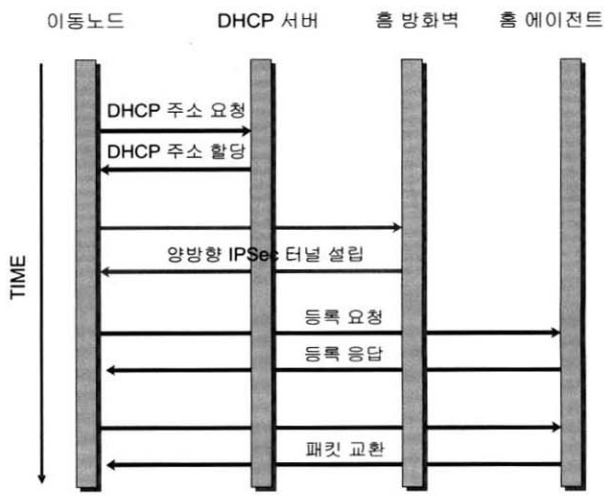
이 패킷은 진입 패킷과 반대 방향으로 등록 응답 패킷과 데이터그램을 터널링한다. 원래 IP 헤더의 발신지 주소는 홈 에이전트이고 목적지 주소는 의탁주소(CoA)이다. 그러나 진출 패킷은 방화벽을 통과하기 위하여 홈 에이전트에서부터 방화벽까지는 가장 바깥 헤더의 발신지 주소는 홈 에이전트, 목적지 주소는 방화벽 주소로 설정된다.



(그림 6) 진출 패킷 형태

3.4 안전한 방화벽 Traversal을 위한 터널링 기법

새로운 네트워크로 이동한 후, 이동 노드는 무선 네트워크의 액세스 포인터를 통해 연결하게 된다. 이때 외부 에이전트는 이동노드의 이동성 여부를 확인하기 위하여 에이전트 광고 메시지를 정기적으로 방송한다. ICMP(Internet Control Message Protocol) 메시지를 받은 이동 노드는 자신이 새로운 네트워크로 이동했음을 알게 되고 이전에 부여받은 co-located CoA를 통한 IPSec 터널의 사용을 멈춘다. 본 연구에서는 DHCP(Dynamic Host Configuration Protocol) 서버를 통하여 CoA를 부여받는다고 가정하였다. 이동 노드는 이전에 사용하던 CoA를 현재 이동한 네트워크의 DHCP 서버로부터 할당받은 co-located COA로 갱신한다. Mobile IP에서 안전한 데이터 전송을 위하여 내부망의 방화벽과 이동 노드의 새로운 CoA사이에 IPSec 터널을 설립한다. IPSec 터널은 Mobile IP의 등록 과정을 포함한 IP 패킷 전송을 위하여 보안서비스를 제공한다. IPSec을 통하여 내부망의 방화벽을 통과한 이동 노드와 홈 에이전트 사이에서 모든 Mobile IP 협상이 이루어진 후에는 다른 Mobile IP 등록 메시지의 인증이나 암호화 기법을 요구하지 않는데 그 이유는 방화벽으로 보호되는 내부망은 안전하다고 가정하고 있기 때문이다. (그림 7)은 Mobile IP의 안전한 방화벽 통과를 위한 터널링 기법의 동작과정을 순차적으로 나타낸 것이다.



(그림 7) 메시지 교환 단계

4. 성능 평가

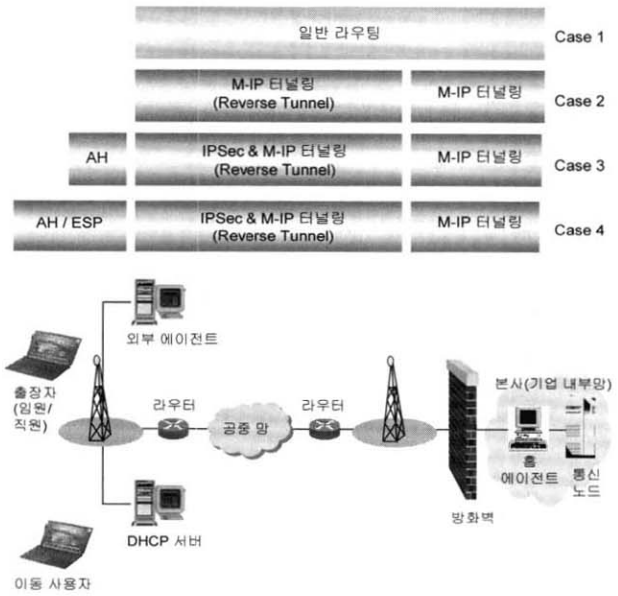
4.1 시뮬레이션 환경

본 절에서는 시뮬레이션 시나리오를 설명하고 시뮬레이션 결과를 분석한다. 시뮬레이션도구로는 ITU-T에서 개발

되었으며 ITU-T Recommendation Z.100으로 표준화된 통신 시스템 개발용 명세 언어인 SDL(Specification and Description Language)[11, 12]을 사용하였다. 본 모델링은 SUN Solaris 7.0 OS를 사용하는 서버와 CPU 1.5GHz RAM 256 MB인 Window 2000를 사용하는 클라이언트에서 실행하였다. 본 시뮬레이션에서 유선 링크의 대역폭은 10 Mbps이며 지연시간은 5ms/km이다. 무선 링크는 대역폭이 2Mbps이고 지연시간은 7ms/km이다.

4.2 시뮬레이션 시나리오

본 논문의 시뮬레이션은 (그림 8)과 같이 네 가지 경우로 나누어 수행되었다. 첫 번째는 Mobile IP 터널링이나 IPSec 터널링이 적용되지 않은 일반적인 라우팅으로 데이터를 전송하는 것이고, 두 번째는 이동노드와 홈 에이전트간에 Mobile IP 터널링이 이루어지는 경우이며 세 번째와 네 번째는 Mobile IP 터널링에 보안을 제공하기 위하여 IPSec 프로토콜을 적용한 경우이다. 모델링의 결과를 분석하기 전에 일반 패킷 라우팅만 하는 경우를 Case 1이라 하고 Mobile IP 터널링만 적용되는 경우를 Case 2라고 하며 IPSec 프로토콜 중 AH 프로토콜만 적용된 경우를 Case 3하고, 완전한 IPSec 프로토콜이 적용된 경우를 Case 4라고 한다.

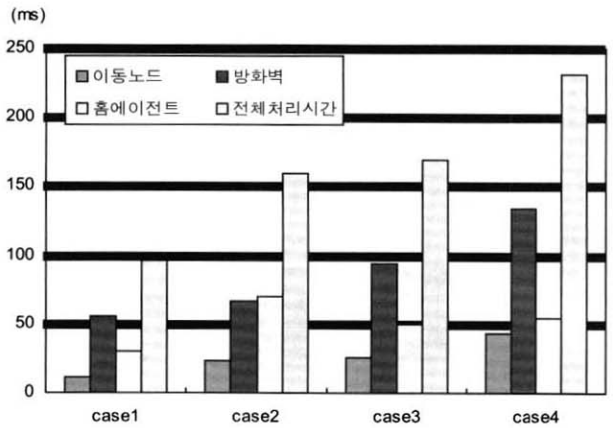


(그림 8) 시뮬레이션 시나리오 및 망 구성

4.3 시뮬레이션 결과 및 분석

4.3.1 노드별 평균 데이터 처리시간과 등록 지연시간

(그림 9)는 각 시나리오에서 등록 요청 패킷을 처리하는 노드별 평균 데이터 처리 시간을 나타낸다. 각 시나리오마다 노드별 처리방법과 인증 및 암호화 역할이 달라지므로 등록 요청을 위한 노드별 프로세스 시간을 통해서 노드별 역할에 따라 터널링 기법을 적용하였을 때 받게 되는 영향을 분석할 수 있다.



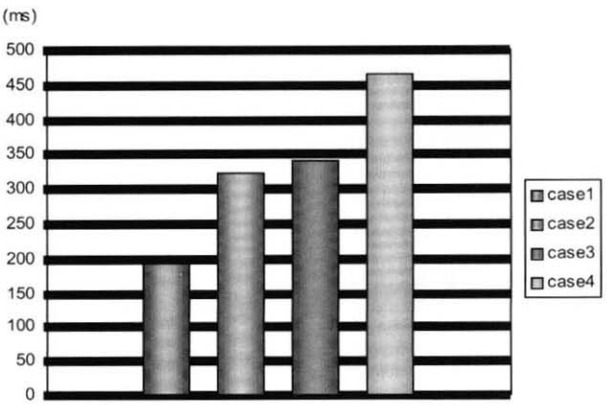
(그림 9) 노드별 평균 처리시간

이동 노드에서의 등록시간은 전체 등록시간 중에서 이동 노드에서 수행된 시간만을 계산한 것이다. 이동 노드는 일반적으로 전력의 사용이 제한되므로 최소로 유지할 필요가 있다. 따라서 각 Case들에서 이동 노드에서의 처리시간을 살펴보면 방화벽과 홈 에이전트에 비해서 처리 시간이 적게 걸렸다. 이동 노드에서 수행되는 계산이 방화벽과 홈 에이전트로 넘어갈 경우 방화벽과 홈 에이전트는 자원이 풍부하므로 더 빠르고 효율적인 계산을 할 수 있고 상대적으로 자원이 부족한 이동 노드에게 전력 부담을 줄일 수 있으므로 중요한 측면이다. Case1과 Case4를 비교해 보면 보안이 적용되지 않은 터널링보다 IPSec 터널링을 적용하였을 때 이동노드에서의 처리부담이 3배 이상 증가함을 볼 수 있다. 그러나 Mobile IP 터널링만 적용된 Case2와 AH 프로토콜이 적용된 Case3을 보면 처리 시간에 있어서 차이가 거의 없음을 알 수 있다. 이 때의 차이점은 Case2의 경우 방화벽의 역할은 단지 패킷 필터링만 수행하며 외부로 이동한 이동노드와 홈 에이전트 간에만 기본적인 MD5[9] 인증이 이루어지므로 방화벽보다 홈 에이전트에서의 처리시간이 약간 더 걸린다. 반면에 Case3의 경우는 방화벽과 이동노드 간에 IPSec 터널링이 형성되므로 방화벽이 이동노드가 보낸 패킷을 복호화, 디캡슐화하여 내부망의 홈 에이전트에게 전송하므로 Case2보다 이동노드의 AH를 위한 처리시간이 약간 증가하며, 홈 에이전트에서의 인증이 방화벽으로 옮겨감으로써 방화벽에서 처리하는 시간이 증가하게 된

다. AH만 적용된 Case3와 AH와 ESP가 모두 적용된 Case 4를 비교해보면 Case4에서 이동노드는 1.7배, 방화벽은 1.4배 증가함을 보아 큰 증가율은 아니지만 성능의 차이를 알 수 있었다.

(그림 10)는 이동노드에서 등록요청패킷을 생성하여 홈 에이전트까지 보내고 홈 에이전트에게서 등록 응답을 받을 때까지 걸리는 평균 등록 지연시간(latency)을 측정한 그래프이다. 이 전체 데이터 전송 지연시간은 이동 노드와 에이전트간에 메시지를 주고받는 시간과 등록 요청, 등록 응답을 생성하는 시간, 이동 노드나 에이전트가 가진 정보테이블을 갱신하는 시간, 넌스(nonce)나 타임스탬프를 검사하는 시간, 아이디를 검사하는 시간 등을 포함하여 암·복호화에 들어가는 계산시간도 모두 포함된 시간을 의미한다. Case2와 Case3은 거의 성능의 차이가 나타나지 않지만 Case3와 Case4는 성능의 차이가 크게 나타난다.

(그림 9)과 (그림 10)를 분석한 결과 IPSec 터널링을 적용하면 접근제어, 기밀성, 무결성, 데이터 발신처 인증 등의 완전한 데이터 보호를 제공하지만 암·복호화 과정으로 인한 노드별 계산 비용과 데이터 전송시간이 전반적으로 커짐을 알 수 있었다. 따라서 사용자가 빠른 IPSec의 실행을 원할 경우에는 기밀성은 제공하지 않지만 AH 프로토콜만 적용된 IPSec을 사용함으로서 성능을 향상시킬 수 있다.



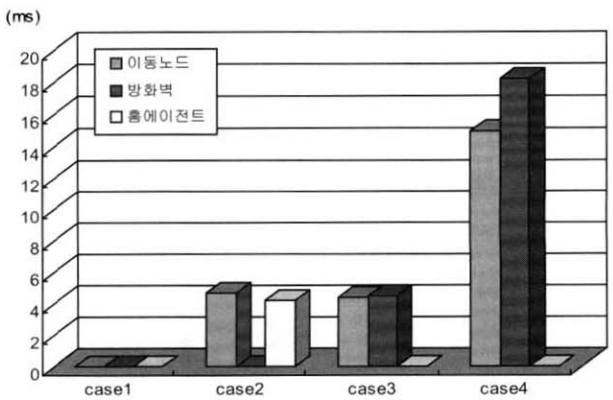
(그림 10) 등록 지연시간

4.3.2 IPSec 터널링의 보안 강도에 따른 지연시간

계산 비용이 높은 암·복호화 과정은 노드의 자원을 사용하게 되며 이동 노드의 전력 소모를 가속화시킨다. 제안한 터널링은 암·복호화하는 계산 비용이 높은 작업을 수행하므로 성능을 좌우하며 많은 동작은 전력 소모를 일으킬 것으로 예상하고 실제 암호화시간을 측정해 보았다. 본 시뮬레이션에서는 각 Case에서 노드별 평균 데이터 암호화 시간을 측정하였으며 IPSec에서 지원하는 인증 및 암호화 알고리즘 중 대표적인 것을 선택하여 성능을 분석하였다.

(그림 11)은 각 Case에 대한 노드별 암호화 처리시간을 나타낸다. 보호되는 패킷은 이동노드가 생성한 등록요청 패킷이며 앞서 설명한 인증 및 암호화 알고리즘이 적용되었다. 이 알고리즘들은 각각 C로 구현하여 SDL 언어와 연동하여 사용되었다. 시간측정은 C의 시간함수로 SDL 내부 프로세스에서 시간함수를 호출하여 밀리 세컨드(milliseconds) 시간 단위로 하나의 메시지를 암호화하는데 걸리는 시간을 측정하였으며 이를 이용하여 인증 및 암호 알고리즘의 성능을 평가하였다. Case 3에서는 최소한의 IPSec 적용을 위하여 AH 프로토콜만 사용한다. AH 프로토콜은 해쉬 알고리즘을 적용하여 메시지의 해쉬 값을 생성하고 메시지와 같이 전송함으로써 데이터가 중간에서 위·변조되지 않음을 증명하여 수신자가 데이터의 무결성을 입증하도록 한다. 해쉬 값을 계산하는 시간은 암호화·복호화 수행시간에 비해 매우 작기 때문에 Case2의 Mobile IP 터널링과 별 차이가 없이 나타났다. 즉, IPSec에서 무결성 서비스는 큰 오버헤드 없이 제공할 수 있다.

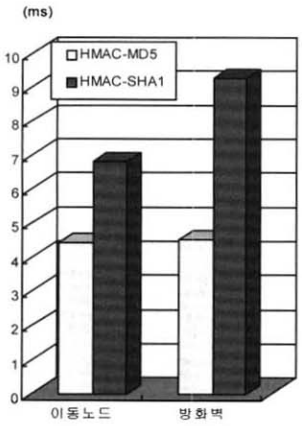
그러나 기밀성을 함께 제공하는 ESP 프로토콜은 암호화·복호화 처리로 인해 평균 데이터 전송시간이 지연된다. 즉, 무결성과 기밀성, 데이터 발신처 인증, 접근제어, 재사용 공격 방지를 모두 제공하는 강력해진 보안 기능이 제공되면 IPSec 터널링을 위한 보안 기법 처리로 인해 데이터 처리시간이 오래 걸린다.



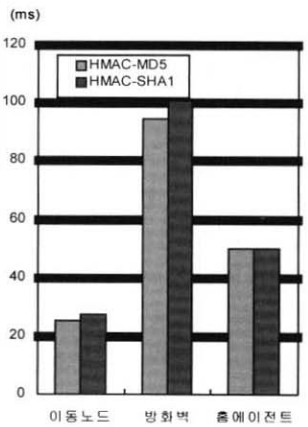
(그림 11) 노드 암호화 시간(등록요청) HMAC-MD5, DES-CBC

(그림 12), (그림 13)는 Case3에서 IPSec을 위해 사용하는 대표적인 두 가지 HMAC 해쉬 알고리즘을 적용하여 두 알고리즘의 성능을 분석한 결과이다. (그림 12)는 각 노드에 적용된 암호화 시간만을 측정한 값을 나타내며 (그림 13)는

등록 요청을 위해 소요되는 노드별 처리시간을 나타낸다. 실험의 결과는 SHA-1 알고리즘이 MD5 보다 다소 느리게 나왔지만 대규모 메시지 요약들이 폭력적 충돌 및 도치 공격을 받을 때 좀 더 안전하게 지켜준다는 강점을 가진다.

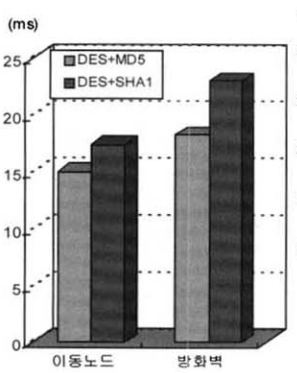


(그림 12) 해쉬 알고리즘 수행시간 비교 (Case 3)

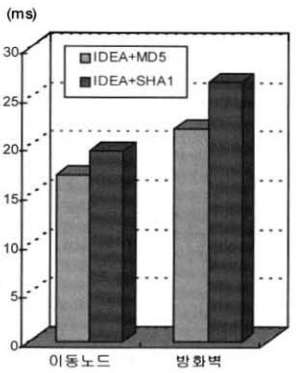


(그림 13) AH를 지원하기 위한 노드별 처리시간 (Case 3)

Case4에서는 AH와 ESP를 모두 적용한 IPSec 터널링을 구현하였다. AH와 같이 ESP도 96 비트 기본 길이의 MAC를 사용하고, AH는 앞서 실험한 HMAC-MD5와 HMAC-SHA1을 적용하여 수행하였으며 ESP는 CBC-DES와 IDEA 블록 암호 알고리즘을 적용하여 측정하였다. (그림 14)는 ESP의 암호 알고리즘은 DES를 사용하고 AH는 MD5, SHA-1을 각각 적용했을 때 결과이다. Case3에서 알 수 있듯이 SHA-1을 적용했을 때 ESP와 함께 사용하면 MD5를 적용했을 때보다 성능이 떨어진다. (그림 15)는 IDEA를 사용하는 것을 제외하고는 (그림 14)의 결과와 동일하다.

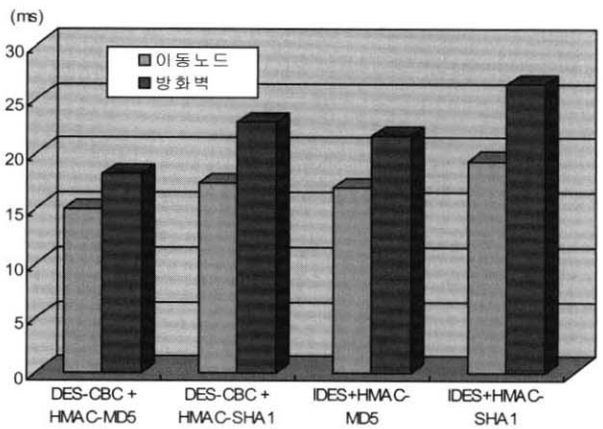


(그림 14) DES 암호 알고리즘과 MD5, SHA-1 해쉬 알고리즘 적용 (Case 4)



(그림 15) IDEA 암호 알고리즘과 MD5, SHA-1 해쉬 알고리즘 적용 (Case 4)

(그림 16)은 앞서 실험을 하나로 나타낸 결과이다. Case4에서 기밀성과 무결성, 데이터 인증 서비스를 제공하는 조건에서 그 성능을 살펴보면 IDEA와 DES의 성능은 약간의 차이가 나지만 IDEA보다 DES 암호 알고리즘을 적용한 성능이 더 좋다는 것을 알 수 있다. 또한 두 가지 암호 알고리즘과 해쉬 알고리즘을 적용해 본 결과 ESP 암호 알고리즘으로는 DES를 사용하고 AH 인증 알고리즘으로는 MD5를 함께 사용할 경우 성능이 가장 좋으며 ESP 알고리즘으로 IDEA와 AH 인증 알고리즘으로 SHA-1을 사용할 경우 성능이 저하된다는 사실을 알았다. 따라서 안전한 Mobile IP 터널링에서 인증 및 암호 알고리즘은 HMAC-MD5와 CBC-DES를 사용하는 것이 바람직하다.



(그림 16) AH, ESP를 지원하기 위한 알고리즘의 수행시간 비교(Case 4)

시뮬레이션 결과를 종합해보면 앞에서 분석한 것과 같이 Mobile IP 터널링만 수행한 Case2와 IPSec 터널링과 통합된 Case3와 Case4는 인증의 역할이 홈 에이전트에서 방화벽으로 이동한 것을 알 수 있다. 이것은 방화벽에게 좀 더 많은 수행시간을 요구하지만 몇 가지 장점을 지닌다. 내부 네트워크 전체를 보호하고 있는 방화벽으로 보안 기능을 집중시킴으로써 방화벽으로 보호되고 있는 내부의 모든 시스템들은 공격자의 위협에서 벗어나게 되어 자유롭게 상호 인증이 가능해진다. 따라서 기업의 네트워크가 성능이 좋은 방화벽 시스템을 가지고 있다면 네트워크의 변형이나 새로운 보안 장치의 추가 없이 IPSec 터널링을 통하여 강력한 보안을 수행할 수 있게 된다. Case2와 Case3의 평균 데이터 처리 지연 결과를 통해서 일반적인 Mobile IP 터널링과 AH 프로토콜만 적용된 IPSec 터널링이 처리 시간에 있어서 차이가 크지 않음을 알 수 있다. 반면에 Case2와 Case4

의 평균 데이터 처리 지연 결과를 보면 Case4의 IPSec 터널링은 수행에 있어서 시간이 훨씬 오래 걸리는 것을 확인할 수 있었다. 이것으로부터 이동 사용자가 강도 높은 기밀성을 필요로 하는 데이터를 전송하지 않을 경우 최소한의 IPSec 만을 실행하여 IPSec 터널링의 성능을 향상시킬 수 있다는 결론을 얻었다.

또한 Case 3의 경우에 두 가지 해쉬 알고리즘을 적용해 보면 HMAC-SHA1을 적용한 경우에 IPSec 터널링의 처리 속도가 HMAC-MD5 알고리즘에 비해 성능이 떨어진다. 마지막으로 Case 4에서는 AH와 ESP를 모두 적용한 IPSec 터널링을 구현에서 AH 프로토콜을 위해서는 HMAC-MD5와 HMAC-SHA1의 두 가지 알고리즘을 측정하였고 ESP 알고리즘으로는 DES-CBC와 IDEA 블록 암호 알고리즘을 적용하여 측정하였다. 그 결과 HMAC-MD5 해쉬 알고리즘과 DES-CBC 암호화 알고리즘을 함께 적용한 IPSec 터널링의 성능이 가장 좋았으며 HMAC-SHA1 해쉬 알고리즘과 IDEA 암호화 알고리즘을 적용했을 경우 성능이 떨어지므로 IPSec 터널링의 성능을 향상시키기 위하여 HMAC-MD5와 CBC-DES를 사용하는 것이 바람직하다.

5. 결 론

본 논문에서는 방화벽으로 보호된 내부망의 이동노드가 보안상의 제약을 받지 않으면서 외부 네트워크로 이동할 수 있도록 하기 위하여 Mobile IP 터널링과 IPSec 터널링을 통합하는 보안 기법을 제안하였다. 제안한 방법은 SDL을 이용하여 시뮬레이션 하였고 인증 및 암호화 알고리즘은 C로 구현하여 SDL과 함께 연동하여 성능을 측정하였다.

시뮬레이션을 통한 성능분석 결과 제안한 Mobile IP 터널링과 IPSec 터널링을 통합한 방화벽 통과기법은 기본적인 Mobile IP 터널링에 비해 처리 시간에 있어서 별다른 차이를 보이지 않으면서 내부망의 방화벽을 안전하게 통과하며 보안을 제공함을 보였다. 또한 제안한 방법은 보안 기능이 내부망의 방화벽에 치중됨으로써 기업망 등의 기존 네트워크에 변형을 요구하거나 새로운 보안 장치를 추가하지 않고 IPSec 터널링을 통하여 보안을 수행할 수 있어서 네트워크에 융통성을 줄 수 있고 이동 노드로 하여금 보안 기능을 수행하기 위한 처리 부담을 줄이는 장점이 있다.

본 연구는 방화벽으로 보호되는 내부망의 이동노드가 외부 네트워크로 이동한 경우에 대한 방화벽 통과 기법에 대한 연구로 외부 네트워크에 방화벽이 있는 경우 또는 다중 방화벽이 있는 경우에 대한 연구가 계속 진행되어야 할 것이다. 또한 이동노드가 방화벽을 벗어나 빈번하게 움직이는 경우 빈번한 이동에 따른 IPSec 터널링 설정 비용을 줄이기 위한 연구 등 성능 향상에 대한 연구가 계속 진행되어야 할 것이다.

참 고 문 헌

[1] Internet Engineering Task Force, http://www.ietf.org.

[2] C. Perkins, "IP Mobility Support for IPv4," RFC 3344, Aug., 2002.

[3] C. Perkins, "Mobile Networking Through Mobile IP," http://www.computer.org/internet/v2n1/perkins.htm, 1997.

[4] M. Leech, M. Ganis, Y. Lee, R. Kuris, D. Kobas, L. Jones, "SOCKS Protocol Version 5," RFC 1928, March, 1996.

[5] S. Mink, J. Schiller, "FATIMA : A Firewall-Aware Transparent Internet Mobility Architecture," Proc. of ISCC 2000, pp.172-179, Jul., 2000.

[6] G. Montenegro, V. Gupta, "Sun's SKIP Firewall Traversal for Mobile IP," RFC 2356, Jun., 1998.

[7] A. Aziz, M. Patterson, "Design and implementation of SKIP," available on-line at http://skip.incog.com/inet-95.ps, 1995.

[8] James R. Binkley, John McHugh, "Secure Mobile Networking Final Report," Portland State University, Jun., 1999.

[9] R. Rivest, "The MD5 Message-Digest Algorithm," RFC 1321, 1992.

[10] G. Montenegro, "Reverse Tunneling for Mobile IP," RFC 3024, Jan., 2001.

[11] R. Break, "SDL Basic," Computer Networks and ISDN System 28, 1996.

[12] SDT Getting Started, "Chapter 1. Introduction to Languages and Notations," SDL Manual.

진 민 정

e-mail : red9677@hanmail.net

2000년 부산여자대학교 전자계산학과 (이학사)

2003년 이화여자대학교 과학기술대학원 컴퓨터학과(공학석사)

2003년~현재 현대중공업 기계전기연구소 시스템제어연구실 근무

관심분야 : 정보통신, 보안, 통합항해시스템

박 정 민

e-mail : pjm@kist.re.kr

1989년 이화여자대학교 전자계산학과 (이학사)

1991년 이화여자대학교 대학원 전자계산학과(이학석사)

1999년~현재 이화여자대학교 과학기술대학원 컴퓨터학과 박사과정

1991년~현재 한국과학기술연구원 연구원

관심분야 : 네트워크 보안, Mobile IP, Active Network Security, Ad-hoc Network

채 기 준

e-mail : kjchae@ewha.ac.kr

1982년 연세대학교 수학과(이학사)

1984년 미국 Syracuse University 컴퓨터학과(이학석사)

1990년 미국 North Carolina State University 컴퓨터공학과(공학박사)

1990년~1992년 미국 해군사관학교 컴퓨터학과 조교수

1992년~현재 이화여자대학교 컴퓨터학과 교수

관심분야 : 네트워크 보안, 인터넷/무선통신망/고속통신망 프로토콜 설계 및 성능분석