IPv6 전이 환경에서 IP VPN 모델 분석과 평가에 대한 연구

임 형 진[†] · 양 진 석[††] · 이 은 선[††] · 김 희 승[††] · 김 태 경[††] · 정 태 명[†††]

요 약

현재 IPv4 네트워크 기반으로부터 IPv6 네트워크로의 자연스러운 전이를 위하여 다양한 상황에 따른 전환 메커니즘과 응용에 대한 연구가 진행되고 있다. 이에 본 논문에서는 VPN 적용 모델에 따른 처리 비용을 산정하고 시뮬레이션을 통해, VPN 터널링 종단점과 IP 앤캡슐레이션 터널링 종단점의 일치여부, 변환 메커니즘의 적용 위치, 적용 VPN 모델이 소요비용에 영향을 주는 요소임을 제시한다.

A Study on Evaluation and Analysis for IP VPN Model in IPv6 Transition Environment

Hyung J. Lim[†] · Jin S. Yang[††] · Eun S. Lee[††]
Hee S. Kim[††] · Tae K. Kim[††] · Tai M. Chung[†††]

ABSTRACT

For a smooth transition from IPv4 to IPv6 network, the research of transition mechanisms have been processing according to the various network situations. Therefore, we calculate the cost based on the VPN applicable model. Also, we present that conformance between the end point of VPN, the IP encapsulation tunneling, applying position of translation mechanism and VPN applicable model are the factors which affect costs.

키워드 : IPv6, 가상사설망(VPN), IPSec, 변환 메커니즘(Transition Mechanism)

1. 서 론

IPv6가 네트워크 전체에 전개되기까지 상당한 기간동안 현재의 IPv4 네트워크와 공존이 필요하게 될 것이다. 이러한 혼재된 환경에서 IPv6 네트워크로의 자연스러운 전환을 위해서 IETF NGTrans 워킹 그룹에서는 다양한 전환 메커니즘을 연구 개발하였다. 하지만 이러한 전환 메커니즘의 대부분은 연결성을 위한 기본 동작만을 정의한다. 현재, v6ops 워킹 그룹에서는 현존하는 망의 특성에 따른 IPv6 전개 시나리오를 제시하고 있다[1].

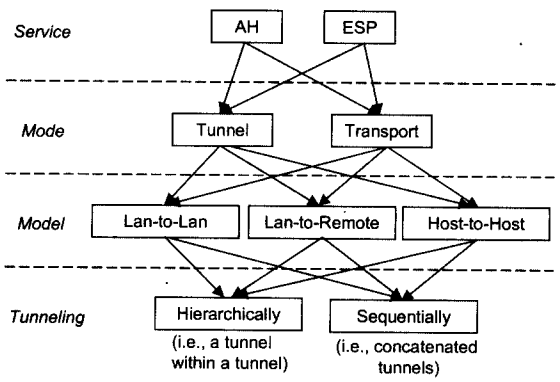
IPv6가 도입될 다양한 망의 특성과 IPv6의 점진적 전개 시나리오의 요구사항분석, 그리고 다양한 변/전환 메커니즘들의 적용은 IPv6망의 원활한 전개를 위한 필수 요구사항이다. 또한 안전한(Secure) 연결 구성을 위한 응용 분야로서 IPsec 적용 가능 여부는 전환 메커니즘 선택에 중요한 요소로 작용할 수 있다. IPv6 네트워크가 도입됨에 따라 IPv4에서 사용되던 VPN 응용구조가 IPv6환경에서도 동작 가능해야 한다. 그러나 서로 다른 두개의 IP버전이 혼재하는 환경에서는 종단간 VPN 연결시 변환과정을 요구하게 되고, 구성되는 메커니즘에 따라서 기밀성, 무결성을 만족해야 하는 IPSec의 특성으로 인해 종단간 VPN을 적용할 수 없는 경우가 발생한다. IPv6 전개과정 동안에 전환 메커니즘을 이용해 상호간에 통신을 가능하게 하는 연결성을 확보한다고 하더라도 VPN이 도입되어질 때 특정 변환 메커니즘에서는 구성이 불가능하거나 추가적인 구성방식을 요구할 수 있다. 따라서 IP버전의 혼재 환경에서 다양한 시나리오의 안전한(Secure) 연결 구성을 위한 응용 분야로서 IPsec 적용 가능 여부와 비용 분석은 전환 메커니즘 선택에 중요한 요소로 작용할 수 있다. 따라서, 본 논문에서는 2장에서 관련 연구로서 IP VPN과 IPv6 전환 메커니즘에 대해 설명하고, 3장에서는 각 전환 메커니즘에 따라 VPN 시나리오의 적용 가능성을 분석하였다. 4장에서는 모델별 VPN 적용 가능성에 따라 비용을 산정하였으며, 5장에서 각 비용 산정에 대한 시뮬레이션을 수행하였다.

※ 본 논문은 보건복지부 보건의료기술진흥사업회 지원에 의하여 이루어진 것임(과제번호 : 02-PJ3-PG6-EV08-0001).
† 정 회 원 : 성균관대학교 대학원 컴퓨터공학과
†† 준 회 원 : 성균관대학교 대학원 컴퓨터공학과
††† 종신회원 : 성균관대학교 정보통신공학부 교수
논문접수 : 2004년 2월 27일, 심사완료 : 2004년 5월 12일

2. 관련 연구

2.1 IP VPN 구성

VPN을 지원하는 기술들은 통신 계층별로 다양하게 지원되고 있으나, IPv4에서 뿐만아니라 IPv6에서는 전송패킷에 대하여 무결성과 기밀성을 지원해주는 IP 계층의 VPN 기술로서 IPSec을 사용하고 있다. (그림 1)에서는 VPN에서 제공하는 서비스와 모드, 구성 방식에 따른 분류를 나타내고 있다. IPSec의 AH와 ESP 헤더는 IP 계층에서 패킷에 대한 인증과 암호화를 수행하는 부분으로 IPv4에서는 AH와 ESP처리에 대한 추가모듈 구현을 통해 IPsec을 구현한다. 그러나 IPv6에서는 AH와 ESP의 확장헤더를 통하여 구현되어 지며, IPv4와 마찬가지로 전송 방식에 있어서 상위 계층 프로토콜에 대한 보호 서비스를 제공하는 트랜스포트(Transport)모드와 전송 데이터의 IP헤더를 포함한 IP 패킷 전체에 대한 보호 서비스를 제공하는 터널모드(Tunnel)로 구성될 수 있다. 또한 IPSec은 터널 종단점에 대한 구성 방식에 따라 Host-to-Host(H-t-H), Gateway-to-Gateway (G-t-G), Host-to-Gateway(H-t-G)으로 구분되어 질 수 있다[2, 3].



(그림 1) VPN 구성 분류

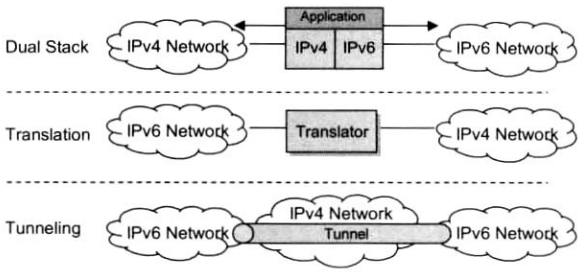
마지막으로 IPSec은 네트워크의 보안 요구사항에 따라 이상의 각 구성 방식들의 조합에 의해 계층적(Hierarchically), 순차적(Sequentially) 터널링을 구성할 수 있다. 전자는 기존의 VPN 터널에 QoS나 보안을 강화하기 위한 방식으로 사용될 수 있는 방식으로 MPLS나 L2TPv3와 같은 다른 터널링 프로토콜과 함께 사용되어지는 방식이고, 후자는 VPN 게이트웨이 전후에서 새로운 터널을 형성하는 방식이다. 이는 종단간 터널링을 구성하기 위해 일련의 터널을 연결하는 방식으로, 망 사업자에서 제공하는 네트워크 기반 VPN 구성시에 라우터에서 액세스 네트워크와 코어 네트워크간의 터널링 연결을 구성하는데 사용되어 질 수 있는 방식이다. 또한 IPSec은 AH와 ESP, 전송모드 그리고 터널의 종단점의 적용 위치에 따라 다양한 모델로 사용가능하다. IPSec은 이외에도 보안 항목에 대한 구성, 키관리, 암호/인증에 대한 알고리즘을 정의한다.

2.2 IPv6 전환 메커니즘

IETF에서 제시되고 있는 다양한 전환(Transition) 메커니즘들은 망의 특성에 따라 개별적으로 적용되어질 수 있으며, 그 내부에서 듀얼 스택(Dual stack), only-IPv6 혹은 only-IPv4 특성을 갖는 노드들 간의 연결성을 구성할 수 있다. 이러한 전환 메커니즘은 (그림 2)에서 나타내는 것과 같이 크게 듀얼 스택(dual stack), 변환(Translation), 터널링(Tunneling) 메커니즘으로 분류되어질 수 있다[3, 4].

- 듀얼스택(Dual Stack)

호스트 혹은 라우터와 같은 노드에 구성 될 수 있으며, 기존의 IPv4 운영체제에 다중 프로토콜 스택을 추가로 로드(Load)하는 형태로 사용될 수 있다. 즉 같은 네트워크 노드나 호스트에 IPv4와 IPv6가 공존하는 시스템이다. 듀얼 스택을 사용하는 응용프로그램은 통신 초기에 IPv4 혹은 IPv6에 대한 DNS로부터의 선택이 요구되어지며, IPv4-IPv4 혹은 IPv6-IPv6 통신에 사용되어질 수 있는 방식이다[3].



(그림 2) IPv6 전환 메커니즘

- 변환 메커니즘(Translator)

IPv4 전용 노드와 IPv6 전용 노드 사이에 직접적인 통신을 가능하게 하는 것이 변환 메커니즘의 주 목적이다. 기본적으로 Only-IPv4 혹은 IPv6 노드들 간의 통신을 지원하는 메커니즘으로 IP와 ICMP 패킷의 변환을 요구하는 메커니즘이다. 구현방식에 따라 통신 스택의 계층별로 지원되는 메커니즘들이 존재한다. 네트워크 계층에서는 NAT-PT[5], SIIT[6] 가 있으며 하위 계층에서 동작하기 때문에 상위 계층보다 상대적으로 빠른 속도를 가질 수 있지만 주소 체계뿐만 아니라 패킷 구조자체가 변경되어야 하기 때문에 Path MTU, 프레그먼테이션 유무에 따른 헤더 변환, ICMPv6, TCP, UDP의 가상 헤더(Pseudo Header) 재계산 등 고려되어야 할 사항들이 있다. 전송 계층에서는 SOCKS[7], TRT[8] 메커니즘이 존재하나 네트워크 계층보다 상대적으로 느리며 헤더 포맷에 대한 매핑 과정이 필요하지 않다. 또한, BIA[9]와 BIS[10]는 종단 호스트에서 동작하는 변환 메커니즘으로

서 IPv4 응용프로그램들을 IPv6 환경에서 사용 가능토록 변환하여 준다. 변환메커니즘은 처리의 복잡성으로 인해 기본적으로 코어(core) 네트워크보다는 네트워크의 에지(edge)에서 적용되어지는 메커니즘이다.

• 터널링(Tunneling)

터널링은 IPv6 전개과정에 있어서 초기에 존재하는 IPv4 네트워크에 대한 변화 없이 연결성을 구성하기 위해 제안된 방법이다. 따라서 IPv6 네트워크 경계라우터(border router)는 IPv6패킷을 IPv4 패킷으로 엔캡슐레이션(encapsulation)하여 IPv4 네트워크로 전송하게된다. 터널링을 구성하는 방법에는 두 노드간의 IPv4 주소를 통해 매뉴얼하게 터널을 설정하는 방식과 IPv4 주소와 매뉴얼(manual)한 설정 없이 IPv6 주소 체계 중 IPv4 주소를 포함하고 있는 IPv6 주소를 이용하여 자동으로 터널링을 하는 방식으로 나누어 질 수 있다. 따라서 터널링은 IPv6 패킷을 IPv4로 IP 엔캡슐레이션 하거나 그 반대의 형태로 전송하는 메커니즘이다. 터널링은 연결성 구성에 따라서 6-to-6 over 4, 4-to-4 over 6 형태로 분류할 수 있고, 적용 위치에 따라서 네트워크 노드간 혹은 네트워크 노드와 호스트간 적용 위치에 따라서 분류되어 질 수 있다. <표 1>는 터널링 메커니즘에 대한 분류를 나타내고 있다[11-13].

〈표 1〉 터널링 메커니즘의 분류

터널링 메커니즘	연 결 성	적 용 위 치
6over4	6-to-6 over 4	종단 호스트와 네트워크 노드간
ISATAP	6-to-6 over 4	〃
DSTM	4-to-4 over 6	〃
Configured IP-in-IP	6-to-6 over 4, 4-to-4 over 6	종단 호스트간, 네트워크 노드간, 종단 호스트와 네트워크 노드 간
6-to-4	6-to-6 over4	네트워크 노드간

3. IPv6 전이 환경에서 IPsec 적용 가능성 분석

이 절에서는 현재 제안된 변환 메커니즘에 IPsec이 도입되어질 때, IPv4 환경에서 구축되던 VPN 모델 중심으로 적용 적합성 여부에 대한 분석을 하고자 한다. IPv6 전개과정 동안에 전환 메커니즘을 이용해 상호간에 통신을 가능하게 하는 연결성을 확보한다고 하더라도 VPN이 도입되어질 때 특정 변환 메커니즘에서는 구성이 불가능하거나 추가적인 구성방식을 요구할 수 있다. 앞서 2.1절에서 살펴본 바와 같이 IPv6 전개과정 하에서도 IPv4환경에서 구성되던 VPN 모델들은 그대로 적용되어야한다. 따라서 기존에 적용되던 VPN 모델에 따라 전환 메커니즘이 도입된 혼재 환경 하에서 적용가능성 여부를 분석하였다. <표 2>은 IETF에서 제시하였었던 전환 메커니즘들에 대하여 VPN 모델별 분류에 따라서 IPsec 적용 가능성 여부를 분석한 것이다.

3.1 듀얼 스택 메커니즘

듀얼 스택에서는 통신에 대한 연결성 자체를 버전별로 구성하기 때문에, IPsec 적용 또한 IPv4 프로토콜과 IPv6 프로토콜에 개별적으로 적용되므로 IPsec 적용에 제한이 없다. 그렇지만, IPv6 IPsec 설정과 IPv4 IPsec 설정을 모두 가져야 하기 때문에 보안 연계(Security Association)나 키에 대한 관리가 기존의 단일 스택 구현에 비해 복잡하고 어려워 질 것이다. <표 2>에서와 같이 듀얼 스택에서는 VPN 설정시 구성 방식에 따라 터널의 종단점 혹은 통신의 시작점으로 사용가능할 것이다. H-t-H VPN 구성시 듀얼스택은 터널의 종단점으로 기능해야한다. G-t-G VPN 구성시 듀얼스택은 터널링 메커니즘이 사용되어지는 사이트의 내부 노드나 게이트웨이로 구성될 수 있으며, 게이트웨이에서 VPN 구성을 처리하기 때문에 내부 노드로서 듀얼 스택은 단지 통신의 시작점으로 동작하고 특별한 요구사항은 없다. 그러나 듀얼 스택라우터로서 게이트웨이 역할을 할 경우 호스트에서와 같이 두 버전에 대한 IPSec 처리 능력에 대한 요구사항을 갖게 된다.

3.2 변환 메커니즘(Translator)

변환 메커니즘의 경우에는 호스트 기반의 변환 메커니즘인 BIA/BIS와 네트워크 노드 기반의 변환 메커니즘인 TRT, NAT-PT등으로 분류하여 IPsec 적용 가능성을 고려해 볼 수 있다.

• 호스트 기반 메커니즘(BIA, BIS)

BIA는 네트워크 계층보다 상위 계층에서 변환 과정이 이루어지므로 상위 어플리케이션에 독립적으로 보안성을 제공하는 IPsec의 적용은 문제가 없다. BIS의 경우 IPv6 VPN을 구성하기 위해서는 모듈의 상위에 변환기(translator)가 위치하기 때문에 적용에는 문제가 없다. 그러나 BIA나 BIS 모두 IPv4 VPN 연결성을 위해서는 IPSec처리 모듈이 추가되어야한다. 종단 호스트에서 변환을 제공하는 메커니즘들은 듀얼 스택과 마찬가지로 버전에 따른 보안 연계에 대한 관리와 IPSec 처리능력을 보유하여야 한다.

• 네트워크 노드 기반 메커니즘(L4 : SOCKS, TRT, L3 : NAT-PT, SIIT)

IPsec의 경우 양 종단 간의 네트워크 계층 기반의 보안 설정을 통해 이루어지게 되고, TCP와 UDP 헤더 역시 IPsec에 의해 암호화되거나 인증을 위해 사용되므로 게이트웨이의 전송 계층에서 변환을 수행할 경우, IP 헤더와 함께 TCP 헤더의 구성이 변경된다. 따라서 VPN 터널링 중간에 트랜스포트 변환이 수행될 경우, IPSec에서 제공하는 종단간 무결성을 보장할 수 없기때문에 종단간 VPN 구성을 위해서는 새로운 VPN 터널을 구성하여야 한다. 따라서 SOCKS나 TRT와 같은 전송 계층(Layer 4 : L4)에서 제공하는 변환 메커니

즘은 적용되는 노드가 VPN 터널의 종단점으로 구성되어야 IPSec적용이 가능할 수 있다. 따라서 종단 호스트간에 하나의 IPsec 구간으로는 VPN 구성에 제약이 따르게 된다.

〈표 2〉 전환메커니즘에서의 IPsec 적용 가능성

변환메커니즘		H-to-H		G-to-G		H-to-G	
		AH	ESP	AH	ESP	AH	ESP
Dual Stack		○	○	○	○	○	○
Trans-lator	SIIT	X	X	△	△	X	X
	SOCKS	X	X	△	△	X	X
	NAT-PT	X	X	△	△	X	X
	BIS	△	△	○	○	△	△
	BIA	○	○	○	○	○	○
	TRT	X	X	△	△	X	X
Tunnel	Configured Tunnel	○	○	○	○	○	○
	6to4	○	○	○	○	○	○
	6vоer4	○	○	-	-	-	-
	ISATAP	○	○	○	○	○	○
	DSTM	△	△	○	○	△	△

○ : 이 경우는 IPv4/IPv6가 혼재된 상황 속에서 IPSec이 추가적인 요구사항 없이 구성 가능한 경우이다.
△ : 이 경우는 IPsec 적용이 가능하기는 하나, 기존의 IPv4에서의 처리 과정을 변경하거나, IPv6에서도 또 다른 처리 과정을 거친 후에 IPsec 적용이 가능해야할 때를 나타낸다. 또한 전송 모드나 터널 모드 중 한 가지만 가능할 때를 의미한다. ex) 무결성 위배 경우, IPSec 처리위한 별도의 추가 모듈 요구 경우 등
X : 이 경우는 이론상으로 가능하지만 실제로 이 방법으로 구축할 가능성이 없음을 의미한다. ex) 중첩 터널링 요구 경우, 무결성 위배 경우, 동적 키 협상 불가능(IKE) 경우 등
- : 한 홉을 기준으로 정의되는 메커니즘으로 다른 VPN 모델에는 적용되어지지 않음.

그 외 메커니즘인 SIIT와 NAT-PT 메커니즘은 네트워크 계층(Layer 3 : L3)에서 변환이 이루어지게 된다. 기본적으로 IPv4와 IPv6는 주소 체계, 헤더 형식과 구성이 다르며 그 크기도 다르기 때문에, 종단 간의 VPN 구성시 L4, L3에서 SIIT와 같은 변환 메커니즘이 적용되어 IP헤더의 패킷 구성 정보가 변경될 경우 IPsec에서의 보안 연계, 인증, 암호화가 패킷의 헤더의 내용, 크기에 영향을 받기 때문에 관련된 계산이 다시 이루어져야 한다. 하지만 이러한 변환메커니즘 역시 변환 메커니즘이 적용되어지는 게이트웨이에서 VPN터널의 종단점을 구성하여 순차적 VPN 터널링을 구성할 경우 이론적으로는 종단간 VPN적용 구성가능하다.

3.3 터널링 메커니즘(Tunnel)

터널링 메커니즘은 호스트에서 생성된 패킷이 엔캡슐레이션 터널 종단점에서 새로운 헤더와 함께 캡슐화되고 터널의 반대편 종단점에서 디캡슐레이션(decapsulation)되므로 호스트에서 생성된 원본 패킷에는 변화가 없다. 따라서 종단간 VPN을 구성할 경우 전송데이타에 대한 무결성, 기밀성을 유지할 수 있으므로 IPSec구성에는 문제가 없다.

터널링 메커니즘은 2.2절에서 언급한 바와 같이 연결성 구성 형태에 따라 두 가지 형태로 구분되어질 수 있다. 다른 터널링 메커니즘의 연결성과 다르게 DSTM의 경우에는 IPv4 패킷이 IPv6로 터널링 된다. 따라서 DSTM 호스트로부터의 VPN 터널링을 구성하고자 할 경우는, IPv4 스택에 IPsec이 포함되어 있지 않기 때문에 구성되어지는 토폴로지에 따라 별도의 IPsec 전용 장비나 호스트에 IPsec 클라이언트를 설치가 요구된다.

터널링 메커니즘에 VPN이 요구되어 계층적 터널을 형성할 경우, 중첩된 IP헤더를 통해 터널이 형성되며, 따라서 이에 대한 처리비용이 요구된다. 터널링 변환메커니즘에 VPN 터널링을 적용할 경우, IP 엔캡슐레이션을 VPN터널로서 교체할 수 있으나, 터널링 메커니즘의 종단점에 일치하는 IPSec외부 헤더를 처리해 주는 절차가 라우터나 호스트에 추가로 구현되어야 한다.

위와 같이 전환 메커니즘에 VPN 구성시 적용 가능성의 차이가 발생하는 이유는 변환 메커니즘의 경우, 서로 다른 IP버전간의 연결성 확보와 패킷 헤더에 포함되는 부가적인 정보 전달을 위해, IP주소와 헤더의 해당 필드 내용을 수정 가능 토록 하는 메커니즘인 반면, IPSec의 경우 보안을 강화하기 위하여 전송 과정상의 데이터의 변경, 조작을 제한하기 위한 목적이기 때문에 근본 메커니즘에서 충돌이 발생하기 때문이다.

4. IPv6 전이환경에서 VPN 모델 평가

4.1 IPv6 NGtrans VPN 모델 구성

NGtrans 환경에서 안전한 채널 구성과 연결성 확보를 위해 제시하고 있는 듀얼 스택, 변환, 터널링의 세 가지 범주의 전환 메커니즘과 VPN의 기본 시나리오로서 제시되어지는 H-t-H, G-t-G, H-t-G 모델을 구성함으로서 요구되는 데이터 전송과 처리에 대한 비용을 산정하고자 한다.

RFC2893에서는 터널링 메커니즘의 구성 방식을 host-to-host(HtH), router-to-router(RtR), router-to-host(RtH) 로 분류하고 있다. VPN구성의 모델이 H-t-H, G-t-G, H-t-G 형태로 분류되는 것과 비교하여, 터널링 메커니즘의 구성분류는 네트워크를 구성하는 자원 간의 연결성 확립에 목적을 두어 광의의 의미를 갖지만, VPN모델의 경우 터널링 메커니즘의 구성에 비해 한정적 분류범주를 갖는다. 따라서 본 논문에서는 router-to-host, host-to-router 터널링 메커니즘 모델을 VPN 모델과 비용을 비교하기 위해서 router에 대하여 인터넷과의 접촉 경계에 위치하는 게이트웨이로서 한정하고, host-to-router 모델의 경우 host는 리모트 접속을 수행하는 호스트에 한정한다. 즉 연결 구성에 있어서, 공중 인터넷망을 경유하여 사설망을 구성하기 때문에 VPN의 터널 종단점으로 사용되어지는 라우터는 일반적으로 인터넷과의 접촉 경계에 위치하는 게이트웨이를 의미하게 된다. 즉 다양한 변환 메커니즘을 통하여 연결성이 구성되어

진 후에, 각 VPN모델을 적용하였을 때의 비용을 산정하여 적합한 모델을 네트워크에서의 처리비용 관점에서 분석하여 보고자 한다.

4.2 성능 인자 추출에 대한 고려사항

IPv6 전이 환경에서 VPN구성을 구성할 때, 데이터 전송시 처리비용은 IP 버전간의 변환 비용이외에도 엔캡슐레이션 터널링 구성비용, 암호/인증에 관련된 VPN터널링 구성비용으로 나누어 고려할 수 있다. IP 버전간의 변환 비용은 변환방식 중 전환 메커니즘에 의한 처리 비용을 말할 수 있고, 엔캡슐레이션 터널링 구성 비용은 듀얼 스택을 포함한 다양한 모드와 버전을 가지는 호스트가 구성할 수 있는 터널링메커니즘 연결 방식으로서 처리 비용을 의미한다. 또한 VPN 터널링을 구성할 때에는, IPSec 전송 모드에 따른 처리와 암/복호화에 관련된 알고리즘 수행에 대한 처리비용이 포함된다. 본 논문에서는 헤더 구조의 변경에 의한 버전간의 전송 효율과 암/복호화 처리 비용은 기존의 개별적인실험결과를 통해서[14-20] 나타난 인자들을 추출하여 NGtrans환경에서의 VPN모델별 구성비용을 평가한다. 그러나 실제 적용수치는 실험환경과 구현 방식에 따라 상이할 수 있으며, 상대적인 효율을 정량화하기 위한 기준 실험데이터 인자로서 활용한다. VPN을 구성하는 전송 모드에 있어서는 기본적으로 트랜스포트 모드만을 고려하였으며, 터널 모드를 사용할 경우는 트랜스포트 모드에 비해 외부 헤더 추가로 인한 전송 패킷량의 증가와 프레그멘테이션 그리고 추가적인 암/복호화량에 대한 비용을 산정하여 고려할 수 있다.

NGtrans 환경에서 완전한 VPN 연결성을 구성하기 위해서는 주소 리졸루션 방식과 응용프로그램의 버전 차이에 따른 변환 메커니즘 구성은 구현방식에 따라 상이한 방식이 사용가능하므로 따로 고려하지 않고, 기본적인 변환 메커니즘들의 기능을 통한 연결성의 확보와 VPN구성에 있어서의 비용을 중심으로 산정하였다. 또한 터널링 비용을 산정하기 위해서 종단간 통신을 위한 터널 종단점에 대한 설정과 VPN 터널링을 위한 보안 연계 협상이 사전에 이루어진 상태를 가정하였다.

VPN 구성 비용 산정은 통신을 구성하는 종단간 호스트에 데이터 전송시 패킷당 암/복호화에 소용되는 비용을 산정하도록 하였으며, 기본적으로 종단간(end-to-end) VPN을 구성함에 있어서의 모델간 구성비용을 분석하고자 하였다. 적용 모델 별로 노드에서 요구되는 처리 비용(Chost)과 라우터에서 요구되는 처리비용(Crouter)을 산정하였고, 각 VPN 모델 H-t-H, G-t-G, H-t-G에 대한 VPN 구성에서 데이터 전송시 네트워크에서 소요되는 총 처리 비용으로 나타내었다.

4.3 NGtrans VPN 성능 인자 및 비용

버전별 헤더 구성에 따라 전송 성능 비용에 영향을 주는 인자로서 IPv4 checksum 계산 비용, 버전별 변환시 파라메타 변환비용, IPv6 TCP, UDP 슈도헤더 재계산 이 있다. 따라서 버전별 전송 성능 비용은 IPv6 전송 데이터 증가량으로 인한 전송 지연 비용(v6*Irate (byte/pkt))과 IPv4 전송 데이터 증가량으로 인한 전송지연(Irate(byte/pkt))로 다른 가중치를 두었다. v6 상수는 앞서 언급한 기존의 실험 결과들로부터 도출되어지는 전송 지연에 대한 가중치를 의미하며, IPv6의 구현 방식에 따라 다른 값을 가질 수 있다[14, 15]. <표 3>에서는 전환메커니즘환경에서 VPN구성시 소요비용에 대한 평가에 사용되어지는 인자들을 나타내고 있다.

〈표 3〉 NGtrans 환경에서 VPN 성능 인자

성능인자	설 명
Vhth	host-to-host VPN 구성 비용
Vgtg	gateway-to-gateway VPN 구성 비용
Vrtg	remote-to-gateway VPN 구성 비용
Chost	터널 종단호스트에서 VPN 구성비용
Crouter	터널 종단 라우터에서 VPN 구성비용
Irate	IP 버전별 패킷 구조 변경에 의한 전송량의 증감율에 따른 전송지연
v6	IPv6 전송지연 가중치 상수(v6 > 0)
Sh	보안 헤더 처리비용
Cip	엔캡슐레이션 헤더 처리 비용
fc	MTU에 따른 패킷당 프레크멘테이션 상수(fc > 0)
Fd	프레그먼테이션 처리비용
Pkt	호스트당 전송 패킷 수(Pkt = fc × Fd)
M	송/수신 패킷당 터널링/전환시 재계산에 소비되는 임시버퍼 비용
Csiit	변환 메커니즘에서 SIIT알고리즘 재계산과 lookup 처리비용
N	Public Net. 도메인 경로상의 홉 수
n	로컬 사이트의 홉 수(default = 1)
Nn	VPN적용되어지는 종단 호스트 수

변환 메커니즘과 VPN을 구성함에 있어서 터널링은 IP 엔캡슐레이션[21] 터널링과 VPN 구성을 위한 터널링으로 구분되어 질 수 있다. 기본적으로 전환 메커니즘에서 사용하는 터널은 다른 IP 인프라로 데이터를 전송하기 위해 자동 터널, configured 터널로 설정되는 IP 엔캡슐레이션 방식을 사용하고, VPN 터널링은 IKE나 인증서를 통한 보안 연계(SA : security association)협상이나 메뉴얼한 방식으로 설정된 구성을 기반으로 터널 모드에 따라 안전한 채널을 구성하기 위해 사용된다. 터널링 구성 비용은 AH, ESP 프로토콜에 따라, 사용되어지는 암호알고리즘을 처리하기 위해 소비되는 CPU 계산 처리 비용이 발생하게 되지만, IPv6 전이 환경에서의 IPSec에 적용되어지는 암호/인증 알고리즘에 따른 영향은 IP 버전별 구성시 동일하게 사용되기 때문에 따로 고려하지는 않고 단지 보안 처리비용(Sh)으로 산정한다. 전환 메커니즘에서 터널링 구성시 엔캡슐레이션으로 사용되어지는 비용(Pip)은 추가적인 헤더의 확장과 이에

따른 프레그멘테이션과 패킷처리를 위해 소비되어지는 CPU 처리 비용이다. 또한 IP 엔캡슐레이션 터널링과 VPN 터널링 구성시 외부에 IP헤더 추가에 따르는 프레그먼트 처리에 관한 비용은 터널링 구성시 동일하게 각기 적용하였다[17].

노드에서 엔캡슐레이션 혹은 암/복호화 터널링을 처리하거나 전환 메커니즘 처리과정에 전송헤더의 정보를 수정할 때, 해당 패킷을 처리하기 위한 임시 버퍼를 사용하게 된다. 시스템 내에서의 데이터의 복사나 프로토콜의 재계산에 사용되어지는 임시버퍼에 대한 비용(M)을 산정하였다. 또한 변환 메커니즘 사용시 SIIT 알고리즘의 적용시 처리 되어야 하는 주소 체계, Path MTU, 프레그먼테이션 유무에 따른 헤더 변환, ICMPv6, TCP, UDP의 가상 헤더(Pseudo Header) 재계산 등의 비용(Csiit)을 추가로 산정하였다[16-20].

인터넷을 경유하게 되는 NGtrans환경에서 종단간 VPN 구성시 버전에 따른 전송 데이터 량의 차이에 따른 전송지연(Irate)을 고려하기 위하여 로컬 사이트(n)과 공공망(N)에서의 전송 홉 수를 고려하였다. 전송 홉 수가 증가함에 따라 버전에 따른 전송지연의 차를 고려하기 위함이며, VPN에 참여하는 호스트수가 증가할 경우 호스트간 VPN의 경우보다 게이트웨이 VPN노드에서는 암/복호화 처리에 비용이 가중될 수 있기 때문에 네트워크 전체에서 호스트수(Nn)에 따른 VPN 구성 비용이 반영되도록 추가로 고려하였으며, 각 호스트는 하나의 VPN 세션을 가진다고 가정하였다.

4.3.1 듀얼 스택

듀얼 스택 환경에서 같은 IP버전 간에 3가지 VPN 모델의 구성 비용을 고려하였다. VPN 터널의 종단점이 호스트일 때 소요되는 비용(Chost)으로서 (Sh + M) * Pkt를 산정하였다. 여기에는 패킷 당 암/복호화에 처리되는 비용과 이에 따르는 메모리 비용을 산정하였고 해당 호스트가 포함된 네트워크의 로컬 홉 수 n을 고려하였다. 터널의 종단 점으로 라우터가 사용될 때 비용(Crouter)으로서 (Sh + M + Fd) * Pkt * Nn을 산정하였다. 라우터에서 소요되는 비용은 다중의 호스트들에 대한 VPN 플로우들을 처리할 수 있기 때문에 호스트에서 처리되어지는 비용이외에 호스트 수를 고려하였다. 듀얼 스택 환경 하에서 각 VPN 모델별 비용을 산정하면 아래와 같다.

$$Vhth = 2 * Chost + [N * v6 * Irate + 2 * v6 * n * Irate] * Pkt \quad (1)$$

$$Vrtr = 2 * Crouter + [N * v6 * Irate + 2 * v6 * n * Irate] * Pkt * Nn \quad (2)$$

$$Vhtr = Chost + Crouter + [2 * v6 * n * Irate + N * v6 * Irate] * Pkt * Nn \quad (3)$$

Vhth는 듀얼 스택 노드 간의 종단간 VPN 구성시 비용을 나타낸다. Vrtr과 Vhtr 경우 증가되는 종단 호스트수에 따라 게이트웨이 역할을 하는 라우터에서의 비용과 전체 전송 데이터의 량은 차이를 나타낼 수 있음을 나타내고 있다. Vhtr과 Vrtr에서 호스트수(Nn)은 기본적으로 1로 가정하였으나, 1이상일 경우는 다중의 리모트 액세스 노드를 포함하는 경우이거나 VPN게이트웨이 내부에 다중호스트가 VPN 플로우를 형성하는 경우를 나타낼 수 있다. 위 각 VPN 모델 비용은 듀얼 스택간의 IPv6 연결 구성을 나타내고 있고, IPv4의 경우 전송 지연에 따른 Irate 값이 변경되어지며 | Irate * (N + 2 * n) * (v6 * -1) | 만큼의 전송 지연차를 갖게 된다.

4.3.2 터널링

터널링 메커니즘들을 6-to-6 over 4 와 4-to-4 over 6 의 연결성에 따라 분류가능하고 이에 따라 VPN의 3가지 모델 구성 비용을 고려하였다. 또한 각 터널링 연결성은 토폴로지에 따라, RFC2893[3]에서와 같이 Router-to-Router(RtR), Router-to-Host(RtH), Host-to-Host(HtH)의 3가지 변형으로 구성되어질 수 있다. 각 해당 토폴로지는 다양한 환경에서 요구사항에 따라 채용되어질 수 있으며, 6 over 4 형태의 RtH의 터널링의 경우 한 홉을 기준으로 정의하고 있으나 리모트 VPN을 구성하기 위해여 홉 수의 제한은 별도로 고려하지 않는다.

<표 4>에서는 터널링 메커니즘 토폴로지에 따라 VPN 모델을 각기 적용하여 소요비용을 산정하였다. 그림에서 게이트웨이사이 인터넷 구간은 IPv4 네트워크를 사용하게 되고, 종단 호스트가 위치하는 게이트웨이 내부 구간은 IPv6 구간을 나타낸다. 또한 e는 엔캡슐레이션 터널링 종단점으로서 엔캡슐레이션이 적용되어지는 노드를 의미하고, v는 VPN 터널링의 종단점으로서 암/복호화가 이루어지는 노드를 의미한다.

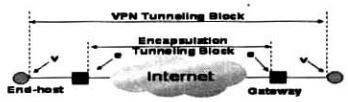
- 터널링 메커니즘 RtR모델과 VPN 구성 비용

IPv6 island[22] 도메인은 IPv4 ocean[22] 도메인을 가로지르는 연결성을 보장하여주는 방식으로서 island 내부의 호스트들은 연결성을 위한 메커니즘을 제공할 필요없이 도메인간의 경계 라우터에서 그 메커니즘을 제공한다. RtR에 적용되어지는 전환 메커니즘으로는 Configured 터널, 6to4 터널 방식이 있다. 기본적으로 RtR 방식에서 라우터 간에는 IP 엔캡슐레이션 방식을 적용하며, 호스트와 라우터간에는 해당 island 도메인의 IP버전을 통한 연결성을 구성한다. RtR을 구성할 때 라우터는 IP엔 캡슐레이션 처리(Cip)와 함께 VPN 터널링을 처리하는 능력을 가진다. 따라서 VPN 터널링에 소요되는 암/복호화와 메모리 비용 이외에 프레그멘테이션 비용, 호스트증가에 따른 비용을 함께 산정하였다.

<표 4>에서 RtR경우를 살펴보면, IPv4와 IPv6네트워크에서 전송지연으로 2 * v6 * n * Irate + N * Irate를 나타내고, 터널링의 종단점과 VPN 종단점의 위치에 따라 Chost 와 Crouter 가 산정되었다. 두 터널링 방식이 각기 다른 종단

점을 갖을 때 프레그먼테이션 비용(Fd)는 각기 산정되나, 같은 지점에서 적용되어질때는 1회만 산정하였다. 이는 통신 스택에서 엔캡슐레이션과 암/복호화 처리 이후에 프레그멘테이션이 수행되기 때문이다. 또한, 네트워크 경계가 아닌 종단에서는 Fd가 터널링 유무에 상관없이 발생할 수 있기 때문에 따로 산정하지 않았다.

〈표 4〉 터널링 메커니즘 VPN 구성 비용

	터널링 메커니즘 VPN 적용지점	개별 구성 비용	
RtR		Vhth = 2 * Chost + [2 * v6 * n * Irate + N * Irate + 2 * (Cip + Fd)] * Pkt	(4)
		Vrtr = 2 * Crouter + [2 * v6 * n * Irate + N * Irate + 2 * Cip] * Pkt * Nn	(5)
		Vrth = Chost + Crouter + [2 * v6 * n * Irate + N * Irate + Fd + 2 * Cip] * Pkt * Nn	(6)
RtH		Vhth = 2 * Chost + [v6 * Irate * (n + N) + n * Irate + 2 * Cip + Fd] * Pkt	(7)
		Vrtr = 2 * Crouter + [v6 * Irate * (n + N) + n * Irate + 2 * Cip] * Pkt * Nn	(8)
		Vrth = Chost + Crouter + [v6 * Irate * (n + N) + n * Irate + 2 * Cip] * Pkt * Nn	(9)
HtH		Vhth = 2 * Chost + [Irate * (2n + N) + 2 * Cip] * Pkt	(10)
		Vrtr = 2 * Crouter + [Irate * (2n + N) + 2 * Cip] * Pkt * Nn	(11)
		Vrth = Chost + Crouter + [Irate * (2n + N) + 2 * Cip] * Pkt * Nn	(12)

VPN 모델중 Vhth 경우는 전송 패킷당 비용을 산정하였고, Vrtr, Vrth경우는 VPN 터널링을 형성하는 세션수(Nn)에 따라 게이트웨이에서의 처리비용이 증가할 수 있기 때문에 VPN 터널을 형성하는 호스트수를 고려하였다.

• 터널링 메커니즘 HtR모델과 VPN 구성 비용

HtR은 ocean 도메인으로서 IPv4 도메인에 위치한 리모트 호스트가 IPv6 island 도메인으로 연결성을 구성하기 위해 사용되어지 방식이다. HtR에 적용되어지는 전환 메커니즘으로는 6over4, DSTM, ISATAP, 6to4 터널링 방식이 있다. 터널링이 적용되는 노드는 각 해당 메커니즘을 지원하며, 또한 개별 메커니즘 동작은 틀리지만, 다른 IP버전간 연결성을 확보하기 위한 패킷 구성방식이 전송 패킷에 외부 IP를 추가하는 엔캡슐레이션 방식을 사용한다. HtR에서는 island 도메인 구간의 연결은 해당 도메인의 IP체계를 따르는 연결성을 구성하며, 변환 메커니즘이 적용되어지는 구간의 호스트와 라우터 구간에서는 IP 엔캡슐레이션 터널링이 사용되어진다. 전환 메커니즘 특성에 따라 DSTM은 IPv6 터널링(4 to 4 over 6)을 6over4와 ISATAP는 IPv4터널링(6 to 6 over 4)을 구성한다.

<표 4>에서 인터넷은 IPv4 네트워크를 구성하고 있으나, 리모트 호스트가 위치한 로컬 사이트는 터널링 메커니즘에 따라 IPv4혹은 IPv6 네트워크를 구성할 수 있다. 비용 산정은 IPv6 네트워크일 때로서 v6 * Irate * (n + N) + n * Irate로 산정하였으나, IPv4 네트워크일 때는 | v6 * N - n | * Irate 만큼의 비용차를 갖게 된다. VPN 호스트와 전송 패킷이 증가할 때 해당 로컬 사이트에서의 IP버전에 따른 전송지연은 v6 만큼의 차이를 나타낼 수 있다. RtR에서와 같이 터널링 적용 지점에 따라 Crouter, Chost, Cip에 대한 비용을 산정하였다.

• 터널링 토폴로지 HtH VPN 구성 비용

HtH 터널링 토폴로지가 사용될 수 있는 전이환경에서의 네트워크 조건은 네트워크가 IPv4로 구성 되었을 때 IPv6 호스트간의 터널링을 구성하는 방식이다. NGtrans 에서는 ocean을 경유하는 환경보다는 island를 형성하는 로컬 도메인 내에서의 연결성을 위해 사용할 수 있는 방식이지만, VPN 구성 비용을 분석하기 위해 island 도메인으로 한정하지 않았으며, Fd에 대한 비용은 통신 시작시 터널링 적용여부에 상관없이 모든 호스트에서 동일하게 산정되므로 비용에 포함하지 않았다.

4.3.3 전 환

라우터에서 동작하는 전환 메커니즘과 종단 호스트에서 동작하는 전환 메커니즘으로 분류하여 3가지 VPN모델 구성비용을 산정하였다. 전환 메커니즘은 전송 스택의 계층별로 정의하나 계층별 가중치를 따로 고려하지 않았다.

<표 5>에서는 변환 메커니즘의 적용지점에 따라 분류하였다. 표에서 ①은 통신의 종단 호스트에서 BIS와 같은 변환 메커니즘이 적용되어질 때를 의미한다. ②의 경우는 리모트 노드가 포함된 사이트의 Gateway에서 NAT-PT와 같은 변환 메커니즘이 동작하는 경우로서, 두 경우 모두 변환 메커니즘이 적용되는 호스트와 게이트웨이 외부는 IPv4 네트워크로 구성된 환경을 고려하였다. 해당 네트워크의 IP버전 구성에 따라 전송지연(Irate)에 대한 차는 |v6 - 1| * N * Irate만큼 발생할 수 있다. ②에서, Vhth와 Vhtr의 경우, 종단간 VPN을 구성하기 위해서는 변환 메커니즘의 전후에 순차터널링을 구성하여야 한다. 따라서 이에 대한 비용이 부과되었다.

〈표 5〉 전환 메커니즘의 VPN 구성 비용

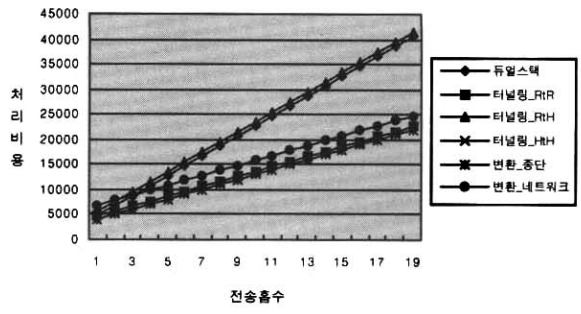
	전환 메커니즘과 VPN 구성	개별 구성 비용	
①		Vhth = [2 * n * Irate + N * Irate + Csiit + 2 * Chost] * Pkt	(13)
		Vrtr = Crouter + Chost + [2 * n * Irate + N * Irate + Csiit] * Pkt * Nn	(14)
		Vrth = 2 * Crouter + [2 * n * Irate + N * Irate + Csiit] * Pkt * Nn	(15)
②		Vhth = 2 * Chost + 2 * Crouter + [n * v6 * Irate + Irate * (N + n) + Csiit] * Pkt	(16)
		Vrtr = 2 * Crouter + [n * v6 * Irate + Irate * (N + n) + Csiit] * Pkt * Nn	(17)
		Vrth = 3 * Crouter + Chost + [n * v6 * Irate + Irate * (N + n) + Csiit] * Pkt * Nn	(18)

5. 시뮬레이션 결과

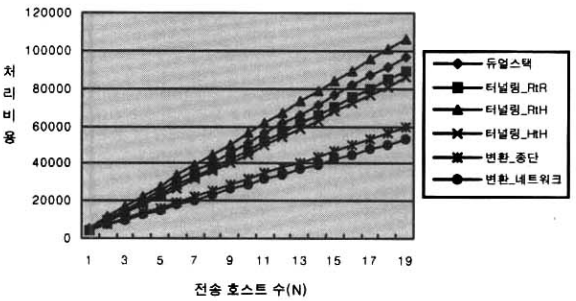
앞 장에서는 VPN 모델과 전환 메커니즘에 따른 구성에서 소요되는 비용을 산정하여 보았으며, 본 장에서는 VPN 연결 구성에 소요되는 개별 인자들의 변화에 따른 상관 관계를 통하여 성능에 미치는 영향을 시뮬레이션을 통해 분석하고자 한다. 시뮬레이션을 위한 망 구성 모델은 4.3절에서 기술된 형태를 따랐다. 개별 인자들 중 터널링 비용으로서 사용되어지는 Sh, Cip간의 관계는 Sh의 비용이 Cip와 같이 외부헤더에 대한 생성과정에서의 처리 비용 이외에 암, 복호화에 대한 처리비용이 요구되기 때문에 Sh > Cip의 관계를 갖도록 설정하였다. 또한 터널링 구성에 대한 Fd, M 에 대한 비용은 일반 패킷 처리시에도 발생하는 비용으로서 네트워크 임의에 노드에서 VPN 터널링 처리시 부수적으로 발생하는 인자이기 때문에 Sh와 Cip 처리비용 보다는 적은 임의 값으로 산정하였다.

(그림 3)와 같이 전송홉수(N), 전송지연(Irate)은 노드에서의 데이터 처리 비용에 영향을 주는 인자는 아니다. 하지만 전체 데이터 전송 비용에 영향을 주는 인자로서, 버전간 헤더 변화에 따른 증가된 데이터 전송량으로 인해 발생하는 전송지연에 영향을 주는 인자가 된다. 전환 메커니즘들 중에서 듀얼 스택의 경우 많은 증가량을 나타내고 있으나, 식 (1)~식 (3)의 비용 산정에 따라 전체 네트워크가 IPv6인 경우, IPv4에 비해 비용이 |Irate * (N + 2 * n) * (v6 * -1)|이기 때문에 IPv6의 경우 전송 홉 수(N)와 Irate증가로 인한 직접적인 영향 보다는 버전 차이에 따른 전송 데이터량 증가에 의해 더 많은 증가량을 보여주고 있다. 즉 |v6 - 1| > 0일수록 전송홉수, Irate 증가에 따라 전송지연에 대한 차가 크게 발생할 수 있음을 보여주고 있다. 또한 Vhth 구성에 있어서 다른 버전간 통신을 위해 터널링을 구성하는 외부헤더로 인한 전송 패킷 크기 증가로 인해 터널링_RtH가 많은 증가량을 보이고 있다.

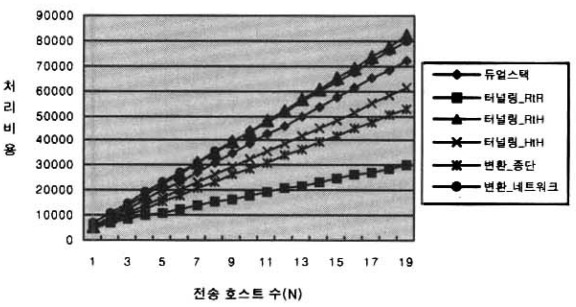
(그림 4), (그림 5)는 호스트수(Nn) 증가시 VPN 비용의 관계를 나타내고 있다. 본 논문의 지면 제한상 실험결과가 제시되지는 않으나, Vhth 경우 종단간 구성이기 때문에, 경로상의 라우터에서 처리 지연이 따로 고려되어지지 않았으며, 버전에 따른 전송량 증가 이외에는 모델간 비용 증가량에 있어서 호스트수 증가에 따른 영향을 받지 않았다. 그러나 Vrtr, Vrth 경우 VPN 호스트수가 증가할 때, 적용 모델에 따라 라우터에서는 다중 VPN 플로우를 수용하여 처리해야하기 때문에 더 많은 비용이 소모되어짐을 나타내고 있다.



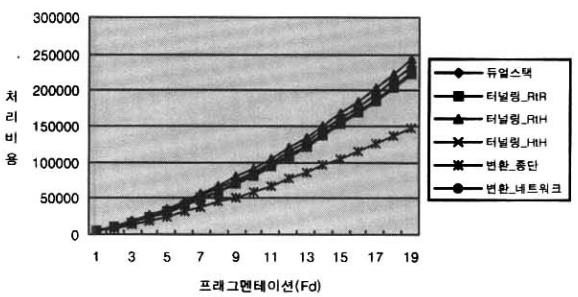
(그림 3) 전송홉수(N) 증가시 Vhth 모델 비용



(그림 4) 호스트수(Nn) 증가시 Vrtr 비용



(그림 5) 호스트수(Nn) 증가시 Vrth 비용



(그림 6) 프레그멘테이션(Fd) 비용 증가시 Vrtr 모델 비용

(그림 4), (그림 5)에서 모델에 따라 다른 증가 수준을 보이는 것은 기본적으로 듀얼스택의 경우 v6 상수에 의해서, 터널링은 Vrtr, Vrth 구성에서 외부 헤더처리에 의한 상대적인 처리 증가량에 의해서 영향을 받고 있음을 보여주고 있다. 네트워크에서 적용 되어지는 변환 메커니즘(표 2-②)의 경우는 (그림 4)에서는 낮은 증가량을 보이고 있다. 그러나 (그림 5)에서는 높은 증가량을 보이고 있으며, 이는 Vrtr 구성시 경로상 변환 메커니즘 처리 결과로서 순차 터널이 구성되기 때문이다. 또한, Vrtr의 증가량이 낮은 이유는 변환 메커니즘 처리 후 종단까지 싱글 VPN 터널을 형성하였기 때문이다. 변환 메커니즘의 경우는 Vhth가 종단간 VPN을 구성할 때 네트워크에서 적용되는 위치에 따라 다중 VPN호스트로부터의 전송 패킷 처리와 종단간 VPN을 구성하기 위한 순차 터널 여부에 의해 소요되는 비용차가 큼을 보여주고 있다.

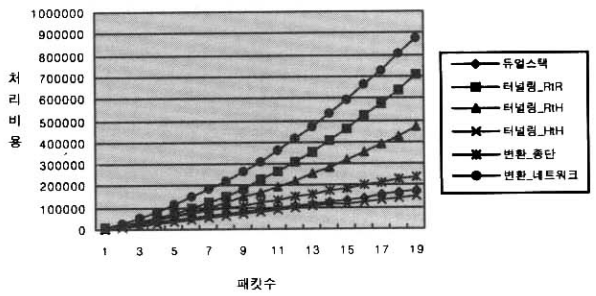
(그림 6)는 Fd 비용 증가시 모델별 상관관계를 보여주고 있다. Fd는 전송패킷수와 Csh, Cip와의 상관 관계를 가지고 있다. Fd의 처리비용은 IP 엔캡슐레이션에서의 PMTU discovery[23] 유무에 따라 패킷 증가시 $Fd = fc * Pkt$ 의 관계를 갖는다. fc는 MTU의 사이즈에 따른 값으로 IP 엔캡슐레이션에서 PMTU discovery가 적용되어지지 않았을 때, 패킷이 증가할수록 프래크멘테이션 처리 비용이 증가함을 나타내고 있다. MTU가 전송 경로상에 임의의 크기로 고정되어 있다고 할 때 fc는 일정 상수가 된다. 또한 프래그멘테이션이 증가할수록 패킷에 대한 Csh, Cip에 대한 처리 횟수도 증가하게 된다. 따라서, VPN 모델 중 Vrtr, Vrth 경우, 터널 종단점인 라우터에서 Csh, Cip 헤더 추가에 따르는 패킷 처리가 발생하기 때문에 Fd 증가시 터널링 메커니즘의 처리 비용이 많은 증가량을 보이고 있음을 보여주고 있다. 프레그멘테이션이 증가함에 따라 변환 종단 노드보다는 네트워크 경로 노드에서 처리되는 노드들이 영향 받고 있음을 보여주고 있다.

(그림 7)~(그림 9)에서는 패킷 증가에 따른 모델별 비용을 나타내고 있다. 네트워크 노드에서 적용되어지는 변환 메커니즘의 경우, (그림 7), (그림 8)은 (그림 6)와는 다르게 패킷이 증가함에 따라 많은 처리비용이 증가함을 보여주고 있다. 이는 Vhth비용에 대하여 전송되어지는 패킷의 수가 증가할수록 Fd가 증가하여 네트워크 노드에서 변환이 적용되어질 때, Csiit와 순차 터널링 구성시 처리해야하는 패킷 처리 횟수가 증가하기 때문이다.

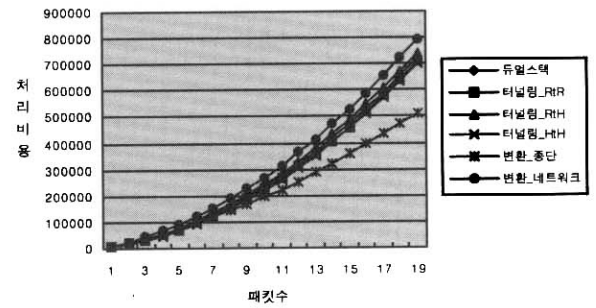
(그림 8)에서는 Vrtr모델일때 터널링_RtR의 경우에 증가 패킷에 대하여 두 터널 종단의 네트워크 노드에서 엔캡슐레이션과 VPN 터널링 처리가 요구되기 때문에 다른 터널링 모델 보다 많은 증가량을 보여주고 있다. (그림 9)의 Vrth 모델에서는 듀얼스택과 터널링_RtH, 터널링_HtH 모델이 상대적으로 적은 비용을 나타내고 있음을 보여주는데 이는 터널링_RtR 모델과 다르게 다중 플로우에 대한 터널링 구성에 대하여 원격의 개별 호스트에서 전송 패킷에 대한 VPN 처리를 수행하기 때문이다.

(그림 10)의 경우는 VPN 호스트의 증가와 함께 전송 패킷량이 증가할 경우의 처리비용을 나타내고 있으며 전송

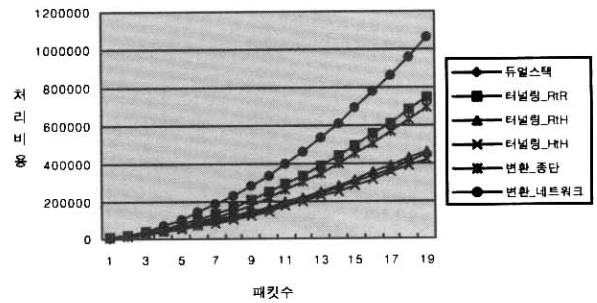
패킷량이 증가함에 따라 변환메커니즘에서는 다른 VPN모델에 비해 급격한 증가를 나타내고 있음을 보여주고 있다.



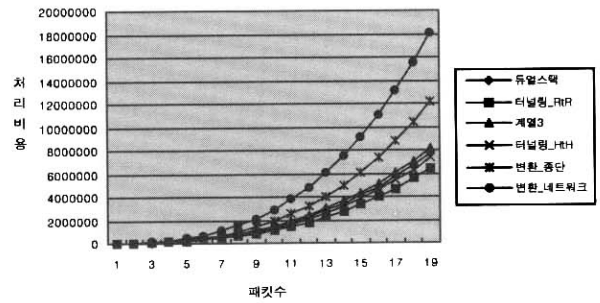
(그림 7) 패킷수(pkt) 증가에 따른 Vhth 비용



(그림 8) 패킷수(pkt) 증가에 따른 Vrtr 비용



(그림 9) 패킷수(pkt) 증가에 따른 Vrth 비용



(그림 10) 패킷량과 VPN호스트 증가시 Vrth 비용

네트워크에서 적용되어지는 변환 메커니즘은 종단간 VPN 채널을 형성하는데 상대적으로 비효율적임을 나타내고 있다. 인자간 상관 관계에 있어서 Csh > Csiit 일때 비용을 산정하였으나, Csiit가 같거나 크다고 하더라도 변환 메커니즘 모델에서의 전체 비용에는 큰 변화가 없었다. 즉, 종단간 VPN을 구성할 때, Csiit에서 사용되어지는 SIIT알고리즘의 처리 비용의 경, 중에 따라 처리해야할 패킷이 증가하는 상황에서 처리 효율성은 순차 VPN처리 비용과 함께 큰 오버헤드가 있음을 나타나고 있다. 그러나 이외의 듀얼 스택이나 터널링_Rth와 같은 모델에서는 종단간 변환이나 VPN의 싱글블럭을 형성하기 때문에 전송 패킷이 증가하는 상황에서도 상대적으로 작은 영향을 받고 있음을 나타내고 있다.

시뮬레이션 결과에 따라, 터널링 메커니즘에서의 VPN 모델의 경우는 터널링의 중복된 사용에 의해서, 변환 메커니즘에서는 종단간 VPN 구성시 순차 터널링 구성에 의해서 VPN 구성비용에 큰 영향을 주는 것으로 나타났다. 또한 프레그멘테이션이 발생하는 터널링 메커니즘의 경우 전송 데이터량의 증가와 VPN 가입 노드들의 증가로 인해 처리비용이 큰 증가량을 나타내고 있다.

네트워크노드에서 IP 엔캡슐레이션과 VPN 터널링의 중복된 사용은 전송 패킷의 증가와 프레그멘테이션에 따라 노드에서의 처리비용 증가를 가져오게 된다. 따라서 경로상에 터널링 종단점이 일치할 경우 IPSec의 터널모드를 통해 IP 엔캡슐레이션을 대체할 경우, 터널링 메커니즘의 모델에 따라 Vhth 경우 2 * Cip * Pkt, Vrtr과 Vrth 경우 2 * Cip * Pkt * Nn 만큼의 비용 감소를 가져올 수 있다.

변환 메커니즘 처리에 대한 비용(Csiit)이 증가하더라도, 종단 호스트에서 적용될 경우보다 네트워크 노드에서 적용되어질 때, 다른 VPN모델과 전환메커니즘에 비해 더 많은 비용 증가량을 보여주고 있다. 이는 종단간의 안전한 전송 채널을 구성하기 위해서 순차 VPN을 구성하였기 때문에 전송 데이터의 증가와 호스트수이 증가는 처리비용의 급격한 증가를 발생함을 보여주었다.

따라서 VPN에 대한 적용 모델은 보안 요구사항에 따라 채택되어 도입되어 질 수 있다 그러나 이 때 상이한 IP버전을 구성하는 네트우크의 경우 다양한 구성이 고려되어 질 수 있으며, Vhth일 경우는 경로상의 네트워크 노드에서의 변환처리를 지양하고, Vrtr, Vrth일 경우는 터널링 메커니즘과 터널 종단점에 대한 처리 과정의 통합을 고려하는 것이 처리비용 효율적이다.

5. 결 론

본 논문에서는 각 전환 메커니즘에 따라 VPN 시나리오의 적용 가능성을 분석하였다. 이러한 적용 가능성에 따른 모델간 비용은 VPN 도입시 해당 토폴로지에 따른 적절한 모델을 선택하는데 기준을 제시할 수 있다. 또한 다른 IP환

경에서 종단간 VPN을 구성하기 위한 요구사항으로서 IPSec의 무결성, 기밀성 메커니즘이 침해되지 않으며, 처리효율성을 고려한 변환 기능을 수행해야 한다. 이에 VPN 적용 모델에 따른 처리 비용을 산정하고 시뮬레이션을 통해, VPN 터널링 종단점과 IP 엔캡슐레이션 터널링 종단점의 일치여부, 변환 메커니즘의 적용 위치, 변환 메커니즘에 따른 적용 VPN 모델이 소요비용에 영향을 주는 요소임을 제시하였다.

보안 요구사항에 따라, VPN 적용 모델과 변환 메커니즘의 종류 그리고 터널링 모델의 혼용은 계층적 혹은 순차적 터널링 형성을 통해 연결성을 구성하게 된다. 즉, 종단간 VPN을 구성하기 위해서 적용 위치에 따라 전환메커니즘의 경우는 순차터널링을, 터널링 메커니즘의 경우는 계층적 터널링을 구성하게 된다. 따라서 이러한 터널링은 전송 데이터의 중첩 헤더처리나 IPSec 적용 구간의 다중 연결 형태는 처리상의 오버헤드를 갖게 되므로, 최소화 할 수 있는 적용모델을 고려해야한다. 또한 다중 VPN 플로우를 처리해야 하는 네트워크 노드에서의 전환 메커니즘의 도입은 VPN처리와 함께 많은 계산량의 처리를 부담하게 되므로 노드에서의 처리능력에 대한 비용문제가 고려되어야 한다.

참 고 문 헌

[1] Hyun-Ku Kim, et. al., "A Study on IPSec Possibility of Adaptation in IPv6 Transition Mechanisms," Proceedings of the 19th Korea Information Processing Society(KIPS) Spring Conference, May, 2003.

[2] Naganand Doraswany, "IPSec," Prentice Hall, 1999.

[3] Fangzhe Chang and Daniel G. Waddington, "Realizing the Transition to IPv6," IEEE Communications Magazine, June, 2002.

[4] Gilligan, R. and E. Nordmark, "Transition Mechanisms for IPv6 Hosts and Routers," RFC 2893, August, 2000.

[5] Tsirtsis, G. and P. Srisuresh, "Network Address Translation-Protocol Translation (NAT-PT)," RFC 2766, February, 2000.

[6] Nordmark, E., "Stateless IP/ICMP Translator (SIIT)," RFC 2765, February, 2000.

[7] H. Kitamura, "A SOCKS-based IPv6/IPv4 Gateway Mechanism," RFC 3089, April, 2001.

[8] J. Hagino, K. Yamamoto, "An IPv6-to-IPv4 transport relay translator, RFC 3124," June, 2001.

[9] Seungyun Lee et al., "Dual Stack Hosts using "Bump-in-the-API"(BIA)," RFC 3338, October, 2002.

[10] K. Tsuchiya, H. Higuchi, Y. Atarashi, "Dual Stack Hosts using the "BUMP-In-the-Stack" Technique (BIS)," RFC 2767, February, 2000.

[11] A. Durand, "IPv6 Tunnel Broker," RFC 3053, January, 2001.

[12] Jim Bound et al., Dual Stack Transition Mechanism (DSTM), <draft-ietf-NGtrans-dstm-05.txt>, November, 2001.

[13] Fred L. Templin, "Intra-Site Automatic Tunnel Addressing Protocol(ISATAP)," <draft-ietf-NGtrans-isatap-02.txt>, November, 2001.

[14] Marc E. Fiuczynski, et. al., "The Design and Implementation of an IPv4/IPv6 Network Address and Protocol Translator," USENIX Annual Technical Conference, June, 1998.

[15] Sherali Zeadally, et. al., "Impact of IPv6 on End-User Applications," IEE/IEEE International Conference on Telecommunications (ICT 2003), Tahiti, Papeete, French Polynesia, February, 2003.

[16] Sherali Zeadally, et. al., "Evaluating IPv4 to IPv6 Transitin Mechanisms," IEE/IEEE International Conference on Telecommunications (ICT 2003), Tahiti, Papeete, French Polynesia, February, 2003.

[17] 임형진, 권윤주, 정태명, "IP 계층에서의 VPN 전송성능에 관한 연구," 한국통신학회논문지, 제26권 제11호, 2001.

[18] Jun MURAI, et al., "Performance Evaluation of Data Transmission Using IPSec over IPv6 Networks," INET 2000, July, 2000.

[19] Takefumi Yamazaki, et al., "Application Performance Analysis in Transition Mechanism from IPv4 to IPv6," IWS2000, Japan, February, 2000.

[20] V. Ganapathy, et al., "IPv6 Performance Analysis on FreeBSD Workstation Using Simple Applications," ASIAN 2000 : 6th Asian Computing Science Conference, Penang, Malaysia, November, 2000.

[21] Perkins, Charles E. "IP Encapsulation within IP," RFC 2003, IETF, October, 1996.

[22] R. Callon, D. Haskin, "Routing Aspects Of IPv6 Transition," RFC 2185, September, 1997.

[23] Mogul, Jeffery, and Stephen Deering, "Path MTU Discovery," RFC 1191, November, 1990.

임 형 진

e-mail : hjlim@rtlab.skku.ac.kr

1998년 한림대학교 컴퓨터공학과(학사)

2001년 성균관대학교 정보통신공학과(석사)

2003년~현재 성균관대학교 대학원 컴퓨터공학과(박사과정)

관심분야 : 네트워크 관리, 네트워크 보안, 시스템 보안, IPv6, 이동컴퓨팅

양 진 석

e-mail : jsyang@imtl.skku.ac.kr
2003년 성균관대학교 정보공학과(학사)
2003년~현재 성균관대학교 컴퓨터공학과 석사과정
관심분야 : 액티브 네트워크, 침입감내, 유비쿼터스 보안, IPv6, 네트워크 보안

이 은 선

e-mail : eslee99@imtl.skku.ac.kr
2003년 성균관대학교 정보통신공학부(학사)
2003년~현재 성균관대학교 컴퓨터공학과 석사과정
관심분야 : VPN, IPv6, 네트워크 보안, 이동 멀티캐스트

김 희 승

e-mail : hskim@imtl.skku.ac.kr
2003년 성균관대학교 정보통신공학부(학사)
2003년~현재 성균관대학교 컴퓨터공학과 석사과정
관심분야 : 액티브 네트워크, 해킹기법 분석, IPv6

김 태 경

e-mail : tkkim@rtlab.skku.ac.kr
1997년 단국대학교 수학교육(학사)
2001년 성균관대학교 정보통신공학과(석사)
1996년~1997년 기아정보시스템
1997년~2001년 서울신학대학교 종합전산실 주임대리
현재 성균관대학교 정보통신공학부 박사과정 수료
관심분야 : 네트워크 관리, 네트워크 보안, Mobile Agents

정 태 명

e-mail : tmchung@ece.skku.ac.kr
1981년 연세대학교 전기공학과(학사)
1984년 일리노이 주립대학 전자계산학과 (학사)
1987년 일리노이 주립대학 컴퓨터공학과 (석사)
1995년 퍼듀 대학 컴퓨터공학(박사)
1984년~1987년 Waldner and Co., System Engineer,
1987년~1990년 Bolt Bernek and Newman Labs.Staff Scientist
1995년~현재 성균관대학교 정보통신공학부 부교수
관심분야 : 실시간시스템, 네트워크 관리, 네트워크 보안, 시스템 보안, GRID 네트워크, 전자상거래