다중 링크 가상사설망을 위한 부하균등 기법

A Load Balancing Scheme for Multi-link VPNs

指導敎授 孫 周 永

2004年 2月

韓國海洋大學校 大學院

컴 퓨 터 工 學 科

金 侹 佑

本 論文을 金侹佑의 工學碩士 學位論文으로 認准함

委員長　工學博士　朴 烋 讚　　印

委　員　工學博士　金 載 熏　　印

委　員　工學博士　孫 周 永　　印

2004年 2月

韓國海洋大學校 大學院

컴퓨터工學科　金 侹 佑

목 차

A Load Balancing Scheme for Multi-link VPNs

Jung-woo Kim

Department of Computer Engineering
Korea Maritime University, Busan, Korea

Abstract

VPN (Virtual Private Network) is a technology that offers secure and reliable connectivity over an infrastructure of a shared public network such as the Internet. The VPNs maintain the same security and management policies as those of a private network. They provide the most cost-effective method for establishing a virtual point-to-point connection between a remote user and an enterprise customer's network.

Nowadays, VPN devices supporting multi-link connections use the second link only to backup the fail-off of the primary link. In practice, however, the fail-off of is hardly occurred, so the second link is used inefficiently.

In order to make the efficiency of the links higher, a scheme for balancing loads between the links is proposed in this paper. Additionally, a new scheme for establishing multi-link VPNs by using a new mutual authentication algorithm is proposed. The scheme should be applied before transferring the secured data among the end points, so as to make the load balancing between the links possible.

Consequently, the proposed schemes have shown that the bandwidth and the cost of multi-link VPNs are more effective.

제 1 장 서 론

1.1 연구 배경

가상사설망(VPN: Virtual Private Network)은 공중망을 이용하여 사설망의 효과를 얻기 위한 기술이다. 이는 전용선을 설치하기에는 부족한 재원을 가지고 있거나 전용선을 설치할 만큼 통신 수요가 많지 않은 경우에 사용되며, 회선의 영속성을 보장하기 위한 백업망으로도 사용된다. 오늘날 기업에서 가장 많은 정보를 교환하는 것은 본사•지사 간 통신이다. 기업에서 VPN을 이용하여 본사•지사 간에 정보를 주고받음으로써 전용회선 비용을 절감하는 효과를 거두고 있다.

현재 출시되어 있는 VPN 장비들은 대부분이 단일회선(점대점) 만으로 VPN 센터와 클라이언트가 연결되어 있다. 전용회선을 사용하는 것에 대비하여 VPN으로 비용절감의 효과는 얻을 수 있지만, 단일회선만으로 연결되어 있음으로 인해 안정성 측면에 있어서는 문제를 초래한다. 전용회선보다 공중망의 회선 단절 현상이 많은 점을 고려하면 더욱 그렇다.

회선 단절 문제를 해결하기 위하여 기존의 VPN 장비는 대부분 다중 링크를 한 장비에 연결하도록 되어 있다. 이러한 VPN 장비에서는 각각의 회선이 주(master), 부(slave)로 구분되어 있다.

VPN을 통해 데이터를 전송하는 도중 주회선에 장애가 발생하면 부회선으로 데이터 전송이 전이(transition)되어 데이터 전송의 영속성을 보장한다. 반면 이 방식은 주 또는 부회선을 한 순간에 하나만을 사용하는 결과가 되므로 회선의 대역폭은 하나의 회선만을 이용하는 것과 같다. 전이 방식으로 장애가 발생할 경우를 대비하는 것은 일반적인 경우에 하나의 회선을 이용하지 못하는 것을 의미한다. 물리적인 VPN 회선은 두 개지만 실제 사용은 하나만 하게 되는 것이다.

이에 따라 데이터 전송량이 많은 경우에는 전송 속도가 결과적으로 늦

어지게 되고, 나아가 응용들의 요구 조건을 모두 수용할 수 없게 된다.

향후 보다 강화된 보안 데이터와 멀티미디어 데이터 전송의 요구가 증가될 것으로 예상되므로 다중 링크로 연결된 VPN에서 회선 사용 효율성의 최적화가 중요하다. 그리고, 다중 링크 연결 VPN에서 회선 간의 전이 기능과 부하균등을 동시에 지원함으로서 VPN 장비의 다중 링크 효율성을 최대로 높인다. 다중 링크 VPN에 적용되는 부하균등 기법은 회선 설치에 따른 회선 이용효과를 최대로 높여 기존 다중 링크 VPN 장비의 회선 효율성 단점을 극복하는 기법인 것이다.

1.2 연구 목적 및 제안 기법

다중 링크 VPN의 부하균등을 위해서는 VPN 장비 상호간 다중회선 인증이 필요하다. 기존 장비의 문제점에 대하여 3.1절에 자세히 설명되어 있듯이 장비 상호간 1:1의 정형화된 VPN 구성 방법으로는 부하균등이 불가능하다. 본 논문에서는 VPN 부하균등을 적용하기 위하여 필요한 VPN 장비 간 상호 인증 방법과 VPN 부하균등 정책을 제안한다. 회선 간의 부하균등을 적용함으로써 회선의 활용도를 크게 높여 결과적으로 VPN의 대역폭을 높이는 효과를 얻을 수 있으며 보안이 강화된 가상 전용선의 기능을 충실히 하기 위한 다중 링크 VPN의 부하균등 기법을 제안한다. VPN의 부하균등을 적용함에 있어 부하균등 정책 적용 과정에서의 문제점과 발전과정을 동시에 논의한다. 나아가 향후 기업 네트워크의 보다 중추적인 역할을 할 것으로 예상되는 VPN의 활용성 증대를 도모하고자 한다.

다중 링크 VPN을 위한 부하균등을 하기 위하여 두 가지 세부 기법이 적용 되어야 한다. 첫째, 새로운 부하균등을 위한 다중 링크 VPN 장비의 상호 인증 방법을 채택하여 적용한다. 둘째, 다중 링크 VPN에서 집합 분할(set partition) 알고리즘을 이용하여 링크 간 부하균등을 행한다.

본 논문의 구성은 다음과 같다. 2장에서는 VPN의 개요를 간단히 설명한다. 그리고, VPN 장비에 가장 안전하고, 부하가 적은 VPN 프로토콜을 탑재하기 위하여 VPN 기술별 트래픽 부하를 측정한 후 실험결과를 설명하였다. 3장에서는 본 논문에서 제안하는 VPN 부하균등 기법을 위한 인증방법과 알고리즘에 대해 설명한다. 4장에서는 VPN 부하균등 기법을 적용한 실험 및 결과에 대해 설명한다. 마지막으로 5장에서는 VPN 부하균등의 향후 연구 방향과 결론을 내린다.

제 2 장 관련 연구

2.1 VPN 개요

VPN은 인터넷과 같은 공중망(public network)을 사용하여 사설망(private network)을 구축하게 해주는 기술 또는 통신망이다. 기존의 FR(Frame Relay) 망에서 요구되었던 고비용의 문제를 해결하고, 공중망을 사용하면서도 마치 사설망을 사용하는 효과를 얻게 된다.

지금까지 기업들은 본사와 지사, 거래처 또는 이동 사용자가 지역적 제약 없이 업무를 수행할 수 있도록 통신 사업자에게 전용회선을 임대하여 원격지까지 연결하는 방식으로 사설망을 확대하였다. 이와 같이 구성한 사설망은 각종 통신망 장비와 소프트웨어 투자에 초기 비용이 많이 투자될 뿐만 아니라 회선 사용 요금도 비싸다. 이와 같은 기존 사설망의 고비용과 비효율적인 관리를 해결하기 위한 방법으로 공중망을 마치 전용회선과 같은 사설망을 구축한 것처럼 사용하는 방식이 출현하게 되었는데 이를 VPN이라 한다.

VPN은 기업의 내부 통신망과 공중망을 연결만 하면 되므로 별도의 값비싼 장비를 구입하여 관리할 필요가 없어 기존의 사설망 연결방식보다 비용이 대폭 절감되는 효과를 얻을 수 있다. 공중망을 이용하기 때문에 사용자가 늘어나거나 장소를 옮기더라도 유연하게 통신망을 사용할 수 있어 자료 공유가 용이하다. 반면 VPN에서 인터넷이라는 공중망을 이용할 경우 기업에서 요구하는 통신 속도 및 대역폭을 안정적으로 보장할 수 없다는 것이 단점으로 지적되고 있다. 데이터의 안전한 전달을 위하여 VPN은 암호화, 인증기법을 사용하여 교환되는 데이터를 보호한다. 최소의 비용으로 기존의 공중망을 가상사설망으로 변형하는 것이 VPN의 목적인 것이다.

현실적으로 장비에 쓰이는 VPN을 형성하는 대표적인 기법은 크게 2계층에서는 L2TP(Layer2 Tunneling Protocol)와 PPTP(Point to Point Tunneling Protocol)고, 3계층에서는 IPSec(IP Security Protocol)으로써 상호 연동하여 보안화된 VPN을 형성한다[1].

VPN 서비스를 하기 위한 세 가지 기본 요소가 있다.

첫째, 터널링(tunneling)이다. 이는 VPN 내부에 가상의 터널을 형성하여 이 터널(tunnel)을 통해 패킷(packet)을 전달한다. 터널링은 VPN의 핵심 기술로써 가상의 회선을 만들어 패킷을 전달하는 기술이다. 일반적으로 네트워크 프로토콜(IP, IPX(Internetwork Packet Exchange))을 캡슐화(encapsulation)한 다음 그 패킷을 다시 터널링 프로토콜로 캡슐화하는 방법을 사용한다.

둘째, 인증(authentication)이다. 이는 지정된 사용자만이 데이터를 상호 교환할 수 있도록 한다.

끝으로 암호(encryption)화다. 암호화는 일반적으로 128Kbits 암호화를 유지하는 것이 보통으로, 이는 전송되는 패킷의 코드를 변환시켜 외부로 유출되어도 데이터가 읽혀지는 것을 방지한다.

2.2 VPN 구성방법

VPN 터널링 프로토콜은 크게 2계층 프로토콜과 3계층 프로토콜로 구분된다.

2계층 프로토콜은 MAC계층(Media Access Control-Layer)에서 터널을 생성하고, 종단간(end-to-end) 암호화를 수행한다. 대표적인 프로토콜로 L2TP와 PPTP가 있다. 그림 2.1은 2계층 VPN 프로토콜 스택 구조이다.

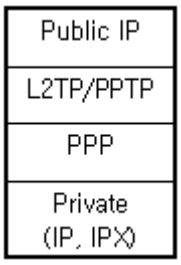

그림 2.1 2계층 VPN 프로토콜 스택 구조

L2TP는 IETF(Internet Engineering Task Force)에서 표준으로 규정한 프로토콜로서 PPTP와 L2F(Layer2 Forwarding)가 결합한 프로토콜이다. IP, IPX, NetBEUI(NetBIOS Extended User Interface) 패킷을 암호화하고, IP 헤더로 캡슐화하여, 인터넷, FR 또는 ATM(Asynchronous Transfer Mode)을 경유하여 전송한다. 동작원리는 다음과 같다. 첫째, 클라이언트(client)와의 접속을 위하여 PPP(Point to Point Protocol)를 이용한다. 둘째, PPP를 통해 연결이 설정되면 L2TP는 네트워크 서버를 통해 사용자를 확인하고, 터널을 통해 사용자에게 서비스를 제공할지를 결정한다. 셋째, 사용자 인증이 확인되면 터널이 생성되고, 통신망을 통해 전달되는 PPP 패킷을 캡슐화하는 역할을 수행한다.

그림 2.2는 L2TP 패킷의 구조이다.

그림 2.2 L2TP 패킷 구조

PPTP는 TCP/IP(Transmission Control Protocol/Internet Protocol) 외에도 NetBEUI나 IPX 같은 LAN 프로토콜을 지원한다. IP, IPX 또는 NetBEUI 트래픽을 암호화하고, IP 헤더로 캡슐화하여 인터넷을 경유하여 전송하는 방식이다. 윈도우 NT 서버 등에 탑재된 보안기능을 이용할 경우엔 별도의 하드웨어 장비가 필요 없다. 클라이언트는 위치만 변동되는 경우에 유용한 방법이다.

그림 2.3 PPTP 패킷 구조

그림 2.3은 PPTP 패킷 구조를 나타낸 것이다. GRE(Generic Routing Encapsulation)는 목적지까지 패킷을 전달하는 데 사용되는 캡슐화 방식의 한 가지이다. PPTP에서 PPP 패킷들을 목적지까지 전달하는 데 필요한 캡슐화된 데이터그램 서비스를 위해서는 흐름제어 및 혼잡제어 기능의 구현이 필요하게 되는데 이를 위하여 사용되는 것이 GRE 메커니즘이다. 흐름제어를 위하여 GRE는 슬라이딩 윈도우 기법을 사용하여 터널 간의 패킷의 전송하며, 재전송이 이루어지지 않는 특성이 있다. 이런 2계층 터널링 기술을 비교한 것이 아래 표 2.1이다.

표 2.1 2계층 터널링 기술 비교

	L2F	PPTP	L2TP
터널형성	UDP 기반	TCP 기반	UDP 기반
터널종단 ID	Tunnel ID	소스 주소	Tunnel ID
가능한 물리매체	모든 망	ATM을 제외한 망	모든 망
터널 동적 IP 할당	불 가	불 가	가 능
터널 형성	2계층	2계층	2계층

L2F와 L2TP는 UDP 기반의 터널형성을 하는 반면, PPTP는 TCP 기반의 터널을 형성한다. 또, PPTP는 ATM에서는 적용되지 않으며, L2TP만이 터널 동적 IP 할당이 가능하다.

3계층 프로토콜은 링크계층과 독립적으로 운영되며, 방화벽(firewall)에 의한 변화가 없는 것이 특징이다. 대표적인 3계층 프로토콜은 IPSec으로 그림 2.4에 그 구조를 나타내었다.

그림 2.4 IPSec 프로토콜 스택 구조

IPSec을 이용해서 VPN을 구성하는 방법은 세부적으로 크게 두 가지로 구분된다. 첫째, IPSec Transfer Mode AH(Authentication Header)이다. 이는 VPN과 VPN 간에 사용되는 방법으로 VPN 간에 패킷의 무결성이 보장된다는 장점이 있지만 암호화가 되지 않음으로 인해 패킷 유출 시 근원지와 목적지 주소가 노출된다는 단점이 있다. 둘째, IPSec Transfer Mode ESP(Encapsulating Security Protocol)이다. 이는 VPN 간에 오가는 패킷을 DES/CBC(Data Encryption Standard/Cipher Block Chaining) 등의 암호화 알고리즘을 이용하여 보내게 되므로 패킷이 유출된다 하여도 패킷의 내용을 알기가 어렵다는 장점이 있지만 고속으로 처리해야하는 패킷의 경우 처리부하가 높게 나타나는 단점이 있다.

표 2.2에서 2계층과 3계층 프로토콜을 비교한다. 캡슐화는 2계층 프로토콜에서 IP와 IPX를 사용하고, 3계층 프로토콜에서는 IP를 사용한다. 패킷인증 및 암호화는 2계층 프로토콜에서 없는 반면, 3계층 프로토콜에서는 AH헤더와 ESP헤더를 사용한다[2, 3].

표 2.2 2계층 프로토콜과 3계층 프로토콜 비교

	Layer 2	Layer 3
프로토콜	PPTP, L2TP	IPSec
서비스	Remote Access	Remote Access LAN-to-LAN
캡슐화	IP, IPX	IP
패킷인증	없음	AH 헤더
패킷암호화	없음	ESP 헤더

2.3 VPN 기술별 부하측정

VPN을 형성하는 기술들이 매우 다양하고, 그 특성도 각기 다르다. 이용하는 측면에서는 어떤 기술에 기반한 VPN을 채택하여야 하는지에 대한 기준이 분명하지 않다. 이런 기준의 하나로 VPN 기술별 트래픽 부하를 들 수 있다. 본 논문에서는 가장 안정적이고, 부하가 적은 VPN 기술을 채택하여 다중 링크 VPN을 적용하기 위하여 현존하는 VPN 기술들에 대하여 트래픽 부하를 측정하고, 그 결과를 상호 비교 분석하였다.

그림 2.5는 ping 서비스에 대한 VPN 기술별 부하를 비교한 것이다. 실험에서 두 VPN 간에 각각의 기술별 모드를 설정하였으며, 각각의 기술 모드에서 ping 서비스를 발생시켜 VPN을 통과하는 패킷의 크기를 측정한 후 평균화하였다. ping 서비스는 client-1에서 client-2로 보내졌다.

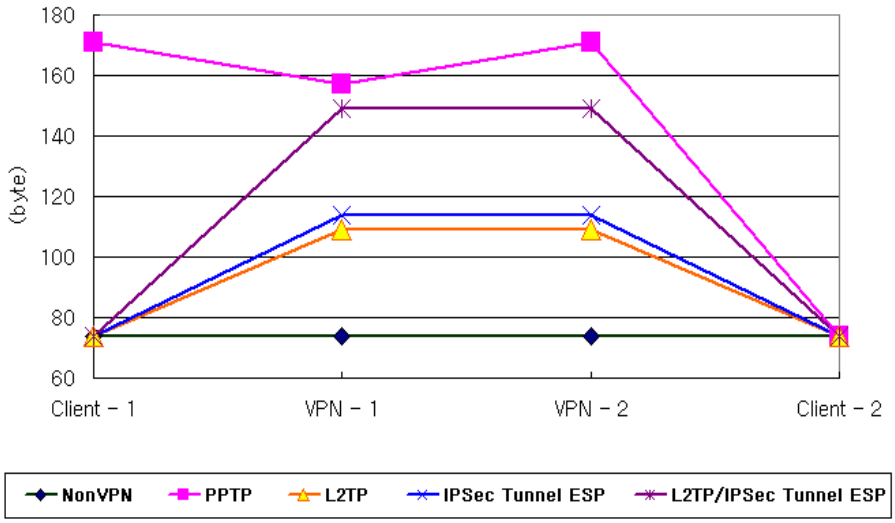

그림 2.5 VPN 기술별 ping 서비스 부하비교

Client-1에서는 부하가 모두 일정하게 나타났지만 PPTP만이 유일하게 다른 모드의 약 2.31배의 부하가 발생하였다. 이는 PPTP의 GRE터널을 통과하는 과정에서 발생한 부하였다. Client-1과 Client-2에서 PPTP를 제외한 나머지 기술들은 NonVPN에 비해 전체적으로 약 1.47~2.01 배

의 부하가 발생하였으며 VPN 사이의 터널 간에는 부하가 대칭적으로 발생하였다.

실험에서 PPTP 기술이 VPN 기술별 모드 중 부하가 가장 많았으며 특히 ping과 같은 OSI(Open System Interconnection) 하위 계층에서 처리되는 패킷의 경우 가장 큰 부하가 발생하였다.

그림 2.6은 Transport Mode에서의 ping 서비스가 발생할 때 VPN 부하를 비교한 것이다. L2TP/IPSec Transport AH와 L2TP/IPSec Transport ESP는 L2TP 터널에 IPSec Transport AH와 ESP Mode를 적용하였다.

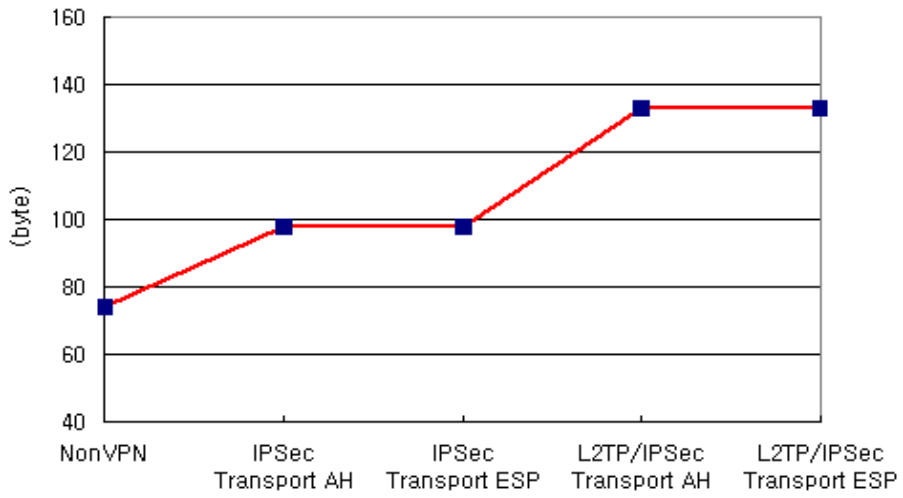

그림 2.6 Transport Mode에서의 VPN 기술별 ping 서비스 부하 비교

IPSec Transport Mode는 NonVPN보다 약 1.3배의 부하가 발생하였으며, L2TP/IPSec Transport Mode는 NonVPN보다 약 1.8배의 부하가 발생하였다. ping 서비스에 따른 AH와 ESP Mode 간의 부하는 동일하게 발생하였다[4]. ESP에 의해 암호화된 패킷은 해독키를 알기 전에는 쉽게 분석할 수 없다는 장점 때문에 오늘날 AH보다 ESP가 많이 사용되고 있다.

가장 큰 부하를 발생시키는 것은 L2TP/IPSec이다. 이것은 보안에 초점을 맞춘 것으로서 이중으로 터널을 구성하기 때문이다. IPSec이 단독으로

사용될 때 여러 프로토콜을 전달할 수 없는 문제는 L2TP와 같이 사용하게 되면 해결된다. L2TP/IPSec의 가장 큰 장점은 패킷을 암호화할 수 있는 것인데 이것은 패킷의 무결성을 보장해 준다.

본 논문에서는 위의 실험결과 분석을 통하여 보안을 중시하는 응용은 패킷의 무결성 보장을 위하여 L2TP/IPSec기술을 채택한 VPN을 적용하고, 시간 제약적인 실시간 또는 멀티미디어를 중시하는 응용은 L2TP에 의한 VPN을 적용하는 것이 트래픽 측면에서 좋다는 것을 알 수 있다.

2.4 VPN 부하균등 기법

라우팅 정보를 이용하는 부하균등 기법은 크게 두 가지 방식이 있다[5].

첫째, 출발지 또는 목적지 주소(IP address)에 의한 목적지별 부하균등이 있다. 이 방법은 주소범위에 대한 정보를 미리 라우터 등에 할당한 후 해당 범위의 주소만을 통과시키는 방법으로 하나의 네트워크를 n개 이상으로 구분하는 것과 동일한 개념이다. 이와 같은 부하균등은 적용 시 속도가 빠르다는 장점이 있으나 네트워크별 사용빈도가 불균형적으로 발생할 때는 부하균등의 의미는 매우 약해지게 된다.

둘째, 출발지 또는 목적지 응용(port)에 의한 부하균등이 있다. 이 방법은 응용별로 구분하여 라우터 등에 할당한 후 해당되는 응용들만을 통과시키는 방법이다. 이 방법 역시 특정 응용의 사용빈도가 불균형적으로 발생하면 부하균등의 의미는 약해진다.

위와 같은 두 가지 방식에 의하여 기존의 부하균등 기법은 응용과 링크의 특성을 고려하지 않는 것이다. 이런 단점을 극복하기 위하여 라우터 등에 부하균등 대상을 미리 할당하지 않고, 데이터를 처리할 때 실시간 부하균등을 하여 할당해 주는 동적인 부하균등 정책이 필요하다. 즉, 회선의 사용 상태를 파악하거나 응용의 크기를 미리 파악하여 부하균등을 하여야 한다. 동적인 링크 부하균등 기법은 전체 회선들 간의 부하 균등

을 이루면서 응용의 특성을 고려할 수 있고, 회선 상황을 즉시 반영할 수 있는 유리한 기법이다.

제 3 장 다중 링크 VPN 부하균등 기법

3.1 다중 링크 VPN 인증 기법

그림 3.1과 같이 VPN 클라이언트에 두 개의 회선을 설치한 후 다중 링크 VPN 부하균등을 하기 위해서는 회선이 각각 A:주(master), B:부(slave)가 되어야 한다. 또, 회선 단절(fail-off)에 대비한 A와 B 간의 상호 이전(transition)이 원활해야 한다. 그림 3.1은 클라이언트에서 센터로의 정보 요구가 많은 경우에 대한 다중 링크 VPN 구성방법이다. 만약 센터에서 클라이언트로의 정보가 많을 경우는 센터에 다중 링크를 연결하여야 하고, 상호 정보가 많을 경우엔 센터, 클라이언트 양쪽 모두 다중 링크를 연결하여야 한다. 본 논문에서는 그림 3.1과 같이 클라이언트에서 센터로의 정보 요청이 많은 경우를 적용하였다.

그림 3.1 다중 링크 VPN 구조

기존 장비로는 그림 3.1과 같은 구성으로 VPN의 부하균등을 할 수 없다. 기존 장비 구성은 장비 대 장비 간이 서로 1:1의 정형화된 구성으로만 인식되어지므로 인증 역시 두 개의 회선이라 할지라도 클라이언트 장비엔 하나밖에 할당되지 않게 된다[6].

구체적으로 VPN 통신을 하기 위한 첫 단계인 터널링 생성 시 다중 링크에 의한 터널링 형성이 불가능한 것이다. 하나의 장비에 두 개의 클라

이언트에 대한 키인증이 승인되지 않기 때문에 다중 링크를 형성할 수 없는 것이다[7]. 그림 3.1과 같은 구성에서 VPN 부하균등을 하려면 VPN 센터가 논리적으로 VPN 클라이언트를 서로 다른 장비로 인식해야 한다. 그림 3.2와 같이 물리적으로 VPN 클라이언트 장비는 한 대지만 센터에서 보았을 때 논리적으로 두 개의 VPN 클라이언트가 되어야 한다. 즉, VPN 센터는 클라이언트를 각각 클라이언트 A, 클라이언트 B로 인식해야 하는 것이다.

기존의 VPN 센터와 클라이언트 간의 장비간 하드웨어적인 인증 방법은 단방향 인증 방식이다[8]. 이런 하드웨어적인 인증 방식은 부하균등을 위하여 하드웨어적으로 두 개의 회선을 VPN 클라이언트에 물리적으로 연결하였을 경우에 키인증이 다중화 되지 못한다. 또, 다중회선이 연결 되더라도 VPN 클라이언트 장비는 하나의 장비로만 인식하게 되므로 다중 링크 간 부하균등을 할 수 없게 된다.

하나의 장비에 키인증이 1:n[多]인 경우 현재 하드웨어적으로 해결하지 못하고 있는 VPN 클라이언트 장비의 한계를 극복하기 위하여 하나의 장비에 논리적으로 두 개의 VPN이 형성될 수 있도록 소프트웨어적인(논리적인) 방법을 병행한 다중회선 연결을 제안한다.

그림 3.2는 하드웨어적인 1:n 구성에서 소프트웨어적으로 VPN 센터가 VPN 클라이언트를 각각 1:1 구성을 하기 위한 것을 보여 준다.

그림 3.3의 다중 링크 VPN 키인증 동작 알고리즘은 그림 3.2와 같은 구성에서 VPN 센터 장비에서 하나뿐인 VPN 클라이언트 장비를 논리적으로 두 개의 VPN 클라이언트 장비로 형성하기 위한 방법이다. VPN 클라이언트에서 센터를 찾는 것이 아니라 VPN 센터에서 VPN 클라이언트 각각의 링크를 찾는 것이다. 부하균등 VPN 인증에 앞서 소프트웨어적으로 먼저 VPN 클라이언트 장비를 다중 링크 개수만큼 논리적으로 분리한 후에야 비로소 VPN 센터와 클라이언트 장비 간에 상호 인증이 가능하게 된다.

그림 3.2와 같이 VPN 장비를 구성한 후, 그림 3.3과 같은 키인증 작업을 실행한다.

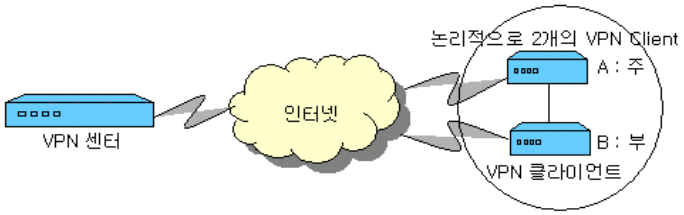

그림 3.2 다중 링크 VPN 부하균등 상세 구조

1. VPN 센터에서 클라이언트 정보 입력
2. 클라이언트에 키 값을 미리 할당
3. 클라이언트는 자신의 정보를 메모리에 할당하여 부 클라이언트라는 개체를 복제
4. 소프트웨어 복제 시 일정 순서에 의한 값을 할당
5. 각 할당된 키인증 값이 상호 일치할 때 각각의 클라이언트를 분리된 독립 개체로 인식하여 다중 링크 VPN 통신 연결

그림 3.3 다중 링크 VPN 키인증 동작 알고리즘

그림 3.2와 그림 3.3을 바탕으로 그림 3.4와 같이 부하균등 VPN을 위한 인증 과정을 거치게 되면 다중 링크 VPN이 부하균등이 가능하도록 형성된다.

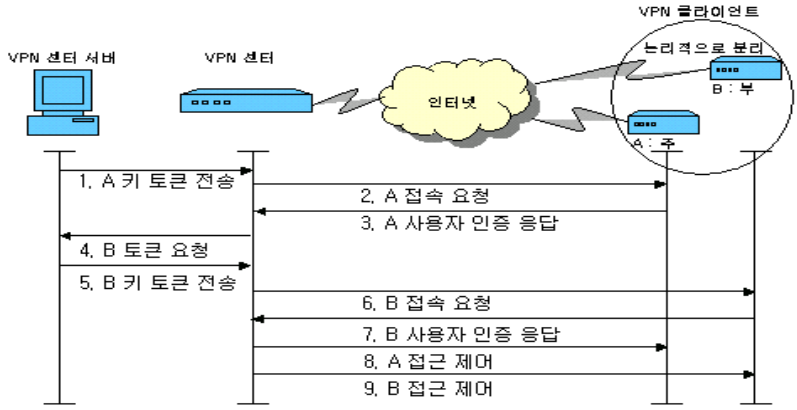

그림 3.4 부하균등 VPN을 위한 인증 과정

부하균등 적용 시 한번 연결 후 다시 연결할 때는 VPN 클라이언트에서 키토큰을 이미 가지고 있기 때문에 재송신할 필요가 없어지게 되어 그림 3.4의 1, 4, 5 과정이 생략된다.

3.2 다중 링크 VPN 부하균등 알고리즘

VPN 부하균등을 동적으로 하기 위하여 집합 분할(set partition) 알고리즘을 적용하였다. 패킷의 원활한 흐름과 VPN 클라이언트의 주/부 회선 간의 부하 차이를 최소화할 수 있게 하므로 링크 효율성을 증대 시킬 수 있다.

(1) 집합 분할 알고리즘의 개요

하나의 유한집합 A가 있을 때 A의 부분집합들인 A_1, ..., A_k가 다음의 조건들을 만족해야 한다.

모든 i에 대하여 $A_i \neq 0$ 이고, $i \neq j$ 에 대하여 $A_i \cap A_j = 0$ 이어야 한다. 또, $A_1 \cup A_2 \cup \ldots \cup A_k = A$ 일 때, $\{A_1, A_2, \ldots, A_k\}$를 A의 분할이라 하고, A_i를 블록(block)이라 한다[9,10].

(2) 집합 분할 알고리즘의 적용

집합 분할 알고리즘을 이용하여 부하균등을 적용함에 있어 가장 중요한 것은 어떤 기준으로 다중 링크에 패킷을 할당하는가이다. 본 논문에서는 부하균등을 위한 기준값으로 응용(port)을 사용하였으며 응용을 이용한 부하균등 알고리즘을 주기적으로 적용하는 것을 원칙으로 하였다. 부하균등 주기가 T_t($t \geq 0$)고, 주기별 응용의 개수가 A일 때, T_t마다 A는 유한집합을 가진다. 다중 링크의 개수가 M_k($k>1$)이면, 부하균등 주기 T_t에서는 A_k의 블록을 갖게 된다.

이를 기초로 얼마나 자주 부하균등 알고리즘을 적용하여 회선에 패킷을 할당하여야 VPN 라우터에서 가장 작은 부하와 최적의 부하균등을 수행할 수 있는지를 실험과 분석 과정을 거쳐 파악한다.

기존의 부하균등 방법인 IP별 또는 응용별 부하균등과 같은 강제적으로 할당하는 부하균등이 아닌 응용의 시간대별 흐름을 분석한 후 회선에 가장 적합한 부하균등을 제공한다. 이를 위하여 본 논문에서는 응용별 전송률(bits per second)을 이용한다. 응용별 전송률을 구하기 위하여 응용이 회선을 이용한 후 응용에 대한 전송률을 데이터베이스에 저장한다. 전송될 응용이 발생하게 되면 저장되어 있던 해당 응용의 전송률을 이용하여 부하균등을 적용한다. 부하균등을 적용한 응용별 전송률은 지속적으로 갱신되어 응용별 부하균등을 하기위한 기초 데이터로 활용된다.

실험에서는 실시간적인 데이터를 기준값(port)으로 사용하였으며 실험의 정확성과 다양한 기준값을 얻기 위하여 모든 응용들에 대하여 적용하였다.

본 실험에서는 부하균등을 위하여 고려한 회선이 두 개이므로 집합 분할 알고리즘에 의하여 두 개의 블록이 적용된다. 실험 결과에 대한 성능은 부하균등 적용 시 시간별 두 블록 간의 차이에서 얻어지며 각 결과 값의 분포도상 전체 표면량이 가장 작은 표면 분포값를 나타내는 것이 가장 성능이 우수한 것이 된다. 평균적으로 두 블록 간의 가장 작은 차이값을 나타내는 것이 부하균등 시 가장 좋은 성능을 갖게 된다.

제 4 장 다중 링크 VPN 실험 및 결과

4.1 부하균등 VPN 라우터 시뮬레이션

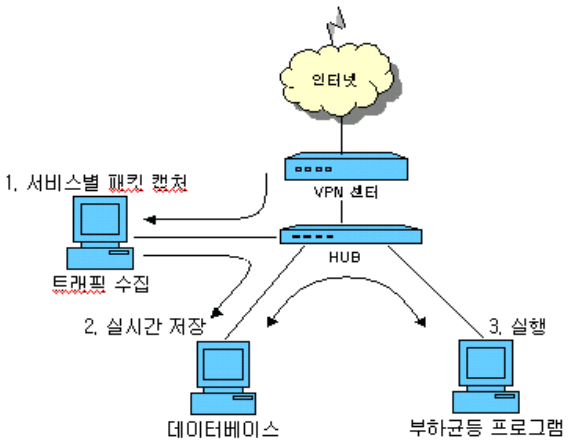

그림 4.1 부하균등 VPN 시뮬레이션 구조

그림 4.1과 같이 부하균등 VPN 라우터 시뮬레이터의 운영 환경은 윈도우 95 이상, 메모리 16MB, 펜티엄 133MHz 이상이다. 데이터베이스 서버는 MS-SQL을 사용하며 VPN은 하드웨어 VPN을 사용한다.

전체적인 동작 흐름은 다음과 같다. 첫째, VPN을 통과한 모든 패킷은 허브를 지나게 되는데 이때 패킷을 복제하여 분석한 후 응용에 대한 종류와 크기를 파악한다. 둘째, 분석이 완료된 응용은 실시간으로 데이터베이스 서버에 저장된다. 셋째, 부하균등 VPN 라우터 시뮬레이터는 미리 설정된 시간 간격에 맞춰 부하균등 알고리즘을 수행한다. 여기서 부하균등을 수행하기에 앞서 해당 응용에 대한 전송률을 데이터베이스 서버에서 가져온다. 가져온 응용별 전송률로 부하균등을 적용하여 각 회선에 응용을 할당한 후 회선에 할당된 크기에 대한 차이값을 산출한다. 넷째, 부하

균등 적용 후 부하균등을 한 실제 응용별 크기를 구해 데이터베이스 서버의 해당 응용을 찾아 전송률을 갱신한다. 끝으로 차이값은 다시 해당 데이터베이스의 결과 및 결과 이력 테이블에 저장된다.

이러한 일련의 과정을 거쳐 생성된 데이터는 다음의 분석 과정을 거쳐 부하균등 알고리즘을 적용하기 위한 가장 최적인 적용 간격(주기)을 얻는데 사용된다.

4.2 다중 링크 VPN 부하균등 알고리즘 적용 정책

부하균등 적용 시 기준값(port)의 이력을 이용하여 집합 분할 알고리즘을 적용하고, 적용 후 해당값의 크기(byte)를 기존의 이력과 재계산하여 새로운 전송률을 이력으로 남긴다.

패킷은 특성상 전송 후에 전송 패킷의 크기를 라우터가 파악할 수 있으므로 이력을 이용한 부하균등 방법은 보다 원활하고, 신속하게 부하균등을 적용할 수 있다. 본 논문에서는 응용별 이력을 응용이 발생할 때 마다 적용하였다.

4.3 적용 간격별 부하균등 시뮬레이션 결과

부하균등 VPN 시뮬레이션은 모두 데이터의 일반화 작업을 위하여 수주에 걸쳐 실행되었으며, 하루 24시간 동안 1초에서 7초까지 부하균등 적용 간격을 달리하여 실행하였다. 이는 적용 간격이 길어질수록 데이터의 정확성이 떨어지는 것을 최소화하기 위한 것이다.

적용 간격별 부하균등 시뮬레이션을 하는 과정은 다음과 같다. 첫째, 적용 간격마다 발생한 응용에 대하여 데이터베이스에 해당 응용의 전송률이 있는지 여부를 확인한다. 둘째, 해당 응용이 있으면 데이터베이스로부터 전송률을 가져오고, 없다면 해당 응용에 대한 전송률은 보류된다. 셋째,

우선 각 응용 중 전송률이 있는 것에 한해 부하균등 알고리즘을 적용한다. 넷째, 데이터베이스에 전송률이 없는 응용의 경우엔 셋째의 과정을 수행 후 부하가 작은 회선으로 할당된다. 끝으로 부하균등이 적용되고 난 후 각 응용들의 전송률은 데이터베이스에 갱신•추가된다. 이런 다섯 가지 과정을 적용 간격별로 반복 적용한다. 일정 기간 반복 적용하면 적용 대상에 대한 특성이 나타나게 되고, 적용 간격을 정확히 파악할 수 있게 된다. 적용 간격을 크게 하면 각 응용의 전송률은 커지게 된다. 이와 같은 방법으로 부하균등을 하고 난 후 양측 링크에 걸린 트래픽 부하 간의 차이값을 나타낸 것이 그림 4.2에서 그림 4.8이다.

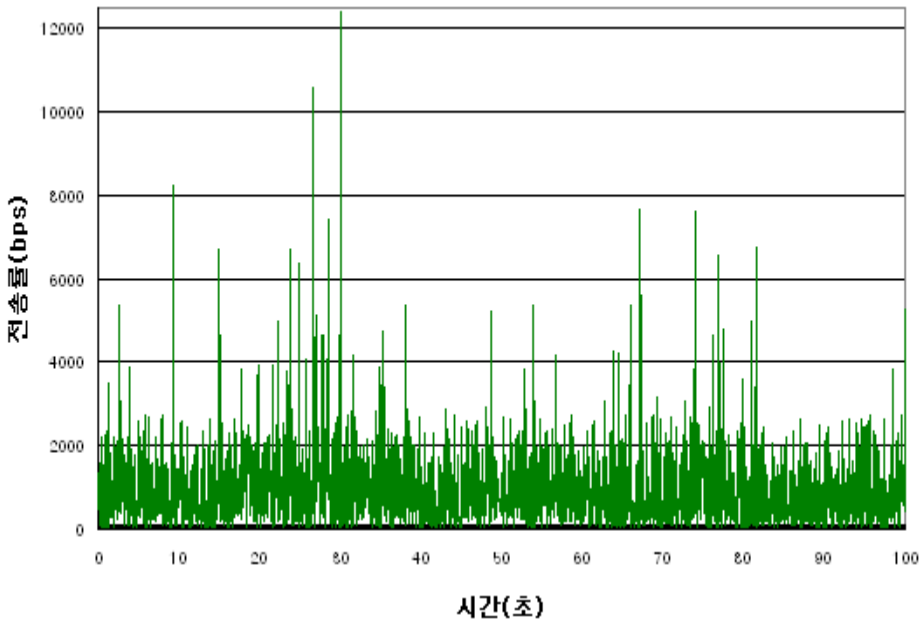

그림 4.2 1초 간격 부하균등 적용 시 링크 간 차이값

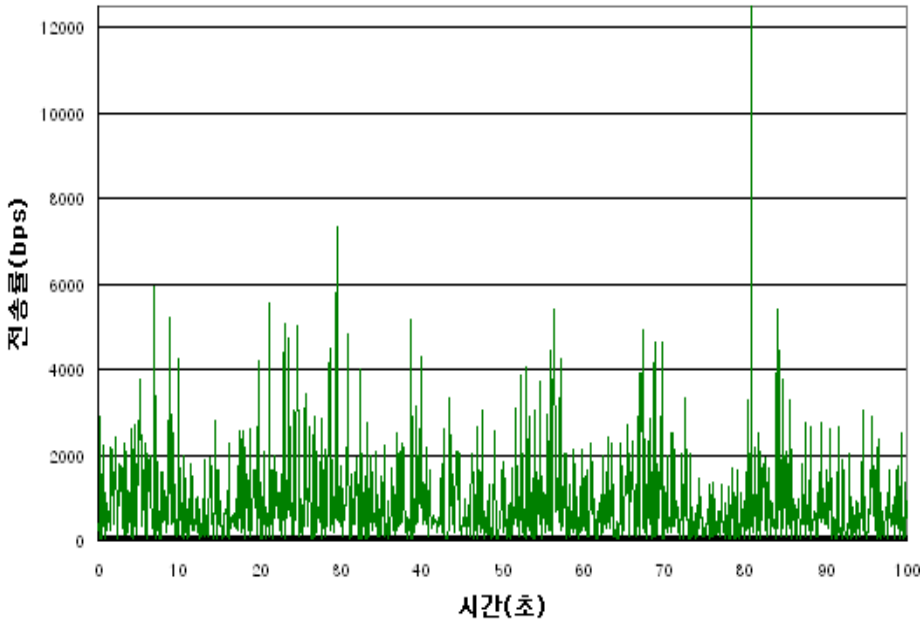

그림 4.3 2초 간격 부하균등 적용 시 링크 간 차이값

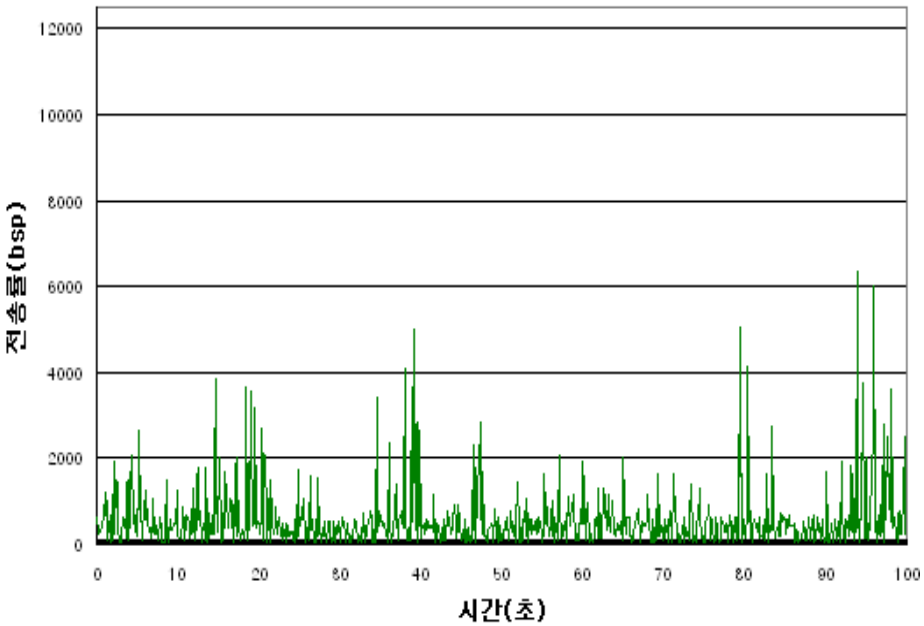

그림 4.4 3초 간격 부하균등 적용 시 링크 간 차이값

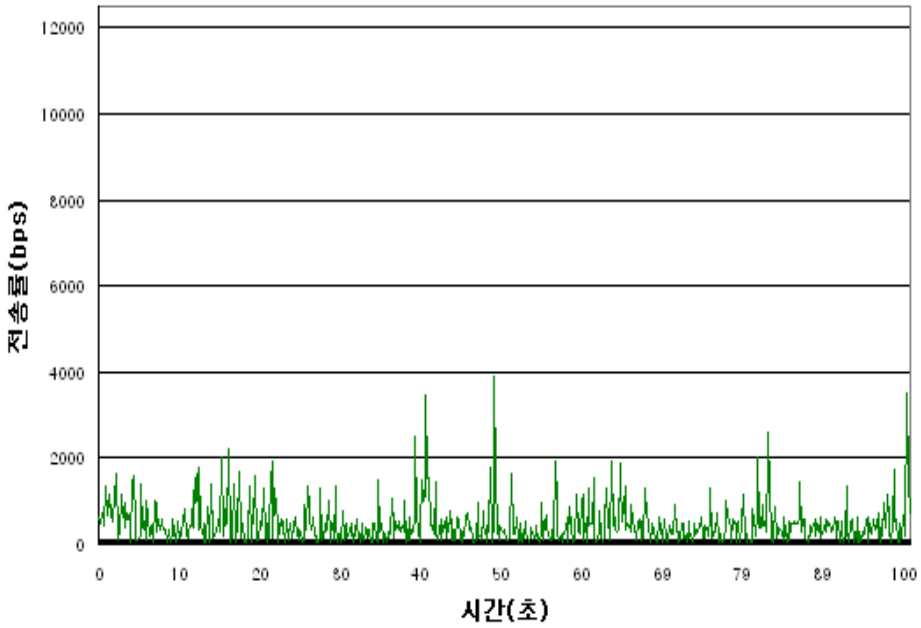

그림 4.5 4초 간격 부하균등 적용 시 링크 간 차이값

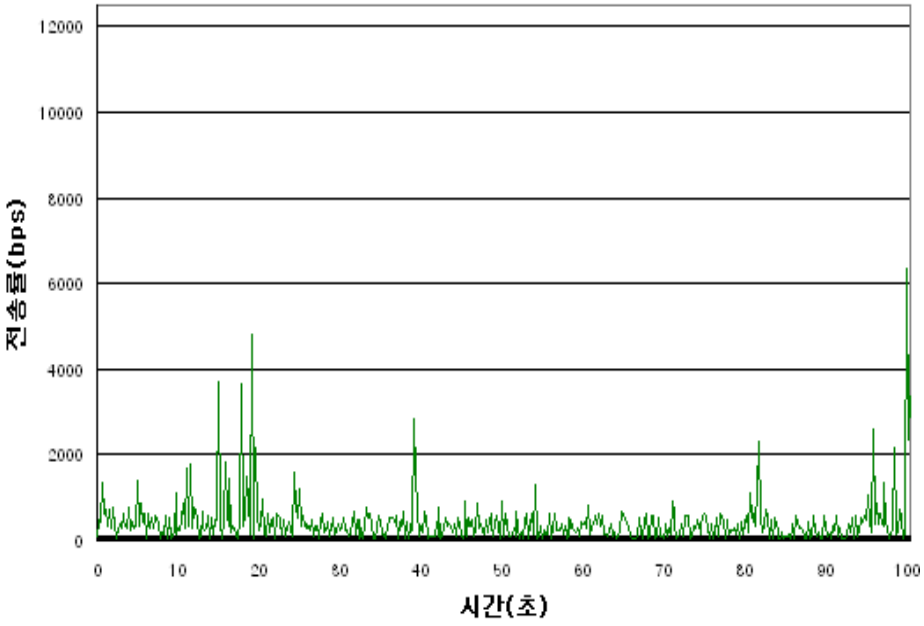

그림 4.6 5초 간격 부하균등 적용 시 링크 간 차이값

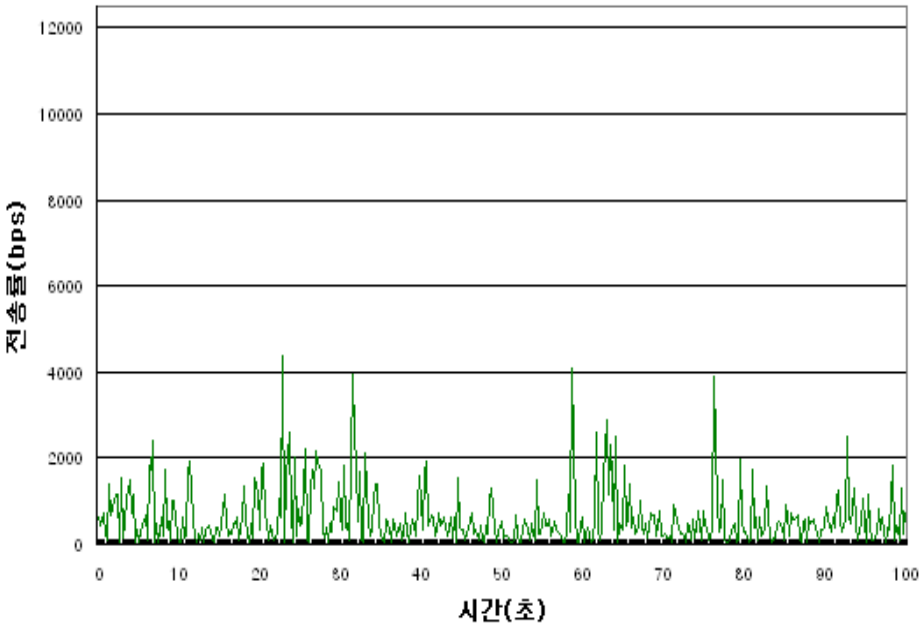

그림 4.7 6초 간격 부하균등 적용 시 링크 간 차이값

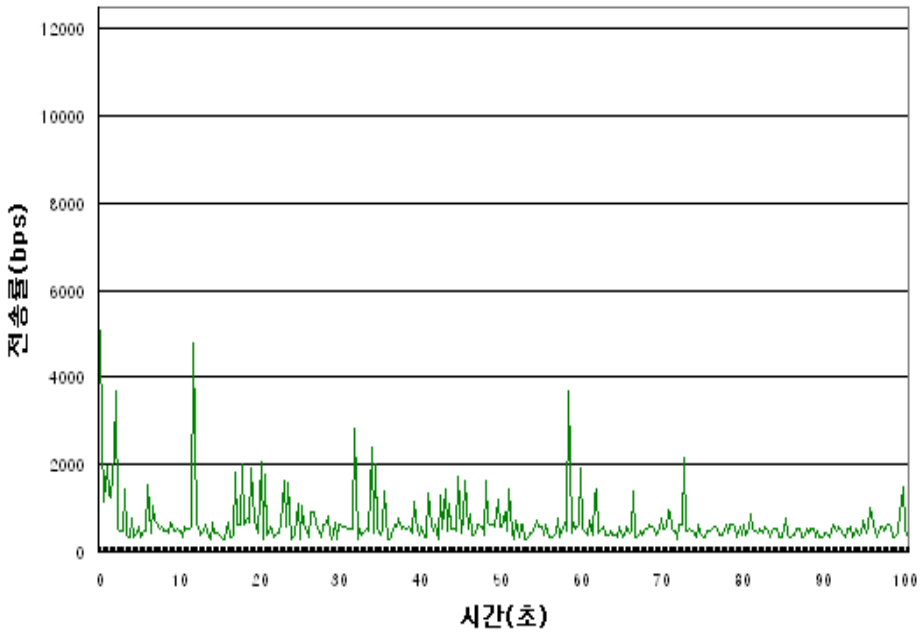

그림 4.8 7초 간격 부하균등 적용 시 링크 간 차이값

위의 결과에서 2초 이하의 부하균등 적용 시에는 특정 시간에서 아주 높은 차이값을 나타나는 것을 확인할 수 있다. 이것은 같은 응용이 연속적인 시간에 나타나는 경우에 응용별 부하균등 정책을 적용하게 되면 부하균등이 원활히 적용되지 않기 때문이다. 다시 말해 다른 기준값보다 크기가 큰 응용이 일정 시간 동안 주기적으로 반복해서 흐르거나 같은 응용만이 일정 시간 동안 주기적으로 반복 발생할 때 나타난다. 3초 간격 이상으로 적용하였을 때에도 같은 현상이 있지만 회선의 부하균등 측면에서는 훨씬 안정적으로 처리되고 있음을 확인할 수 있다.

위의 그림 4.2에서 그림 4.8까지의 적용 간격별 부하균등 시 링크 간 차이값을 평균한 후 이를 적용 간격별로 나타낸 것이 그림 4.9이다.

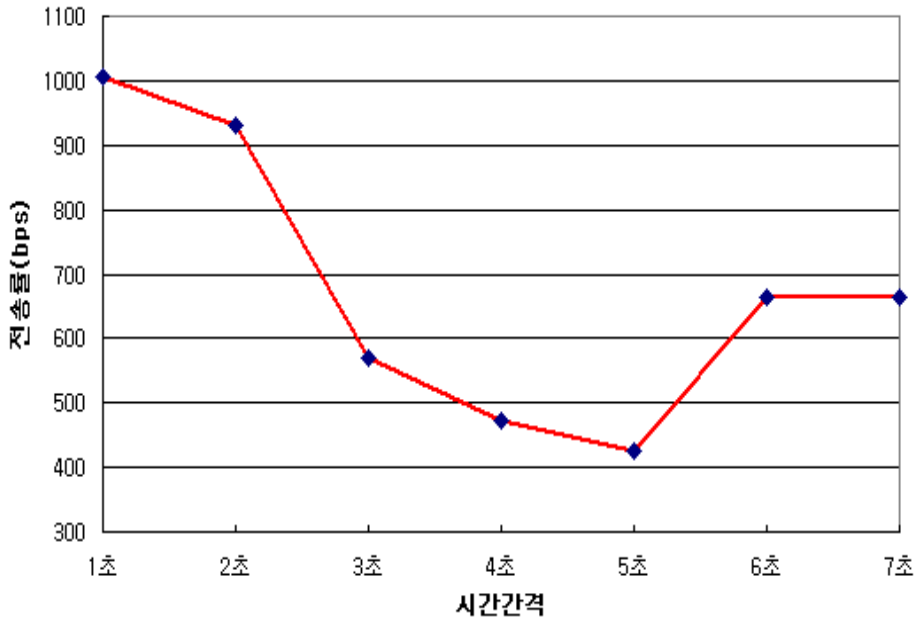

그림 4.9 부하균등 적용 시 적용 간격별 차이값 평균

그림 4.9에서 적용 간격이 5초까지 지속적으로 감소하다 적용 간격 6초 이상부터 다시 상승하는 것을 확인할 수 있다. 적용 간격 5초에서 가장 낮은 부하차이를 나타냈다. 적용 대상에서는 해당 응용이 5초 간격일 경

우 가장 좋은 부하균등을 할 수 있는 것이다. 적용 간격 5초에서 각 응용별 전송률의 합이 가장 균형적으로 구성되어지는 것을 의미한다. 적용 간격이 늘어난다고 해서 전송률이 반드시 균형적으로 되는 것이 아니라 적용 대상의 특성에 따라 가장 균형적인 부하균등 적용 간격이 있음을 확인할 수 있다. 이것은 아래 그림 4.10의 응용별 연속 전송 평균 횟수와 연관이 있다.

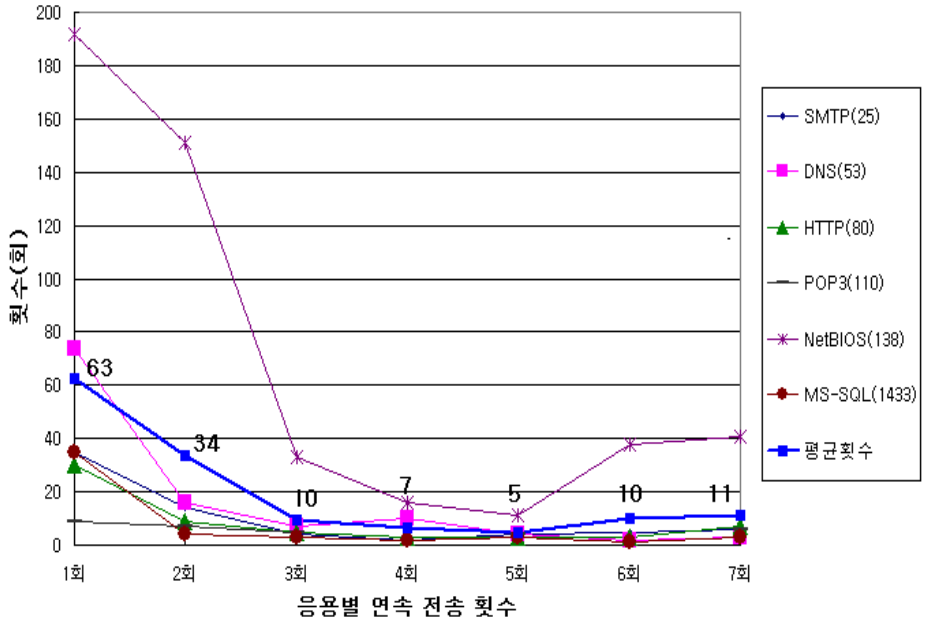

그림 4.10 응용별 연속 전송 평균 횟수

그림 4.10은 적용 간격별 부하균등 시 대부분의 트래픽을 차지하였던 대표적인 응용들에 대하여 시간당 연속적으로 전송되었던 횟수를 나타낸 것이다. 평균화하여 확인해 보면 5회 이하에서는 지속적인 감소를 나타내다 6회 이상부터 조금씩 상승하고 있다. 응용의 연속 전송 횟수가 증가하는 것은 다중 링크 VPN 부하균등 적용 시 응용의 전송률이 커지는 것을 뜻한다. 이것은 응용별 다중 링크 VPN 부하균등을 적용할 경우에 링크간 차이값이 높아지는 원인이 된다.

다중 링크 VPN 부하균등을 적용함에 있어 함께 고려되어야 하는 사항이 처리지연시간이다. 처리지연시간은 부하균등을 적용할 때마다 발생하는 시간이다. 다중 링크 간 부하균등 처리 시 발생하는 처리지연시간을 같이 계산하여야지만 부하균등 적용을 위한 최적의 적용시간을 얻을 수 있다. 본 논문의 경우, 부하균등 1회당 평균 지연시간은 0.016384초 이다.다중 링크 VPN 부하균등 적용 간격에 큰 영향을 미치지 않는 시간이므로 부하균등 적용 간격에 대한 처리지연시간은 무시할 수 있다.

제 5 장 결론 및 향후 연구과제

VPN 한 장비에 회선을 두개 이상 연결하게 되면 이중 투자비용을 감소할 수 있고, 안정성 있는 서비스가 가능하다. 이는 현재 VPN을 사용하거나 앞으로 VPN을 사용할 기업 및 인터넷 회선을 사용하는 대부분의 장소에 부하균등 기능이 포함된 다중 링크 VPN을 적용하게 되면 회선 사용 효율성을 최적화할 수 있다. 다중 링크 VPN의 부하균등은 적용 대상에 대한 사용 그룹의 특성이 먼저 분석되어진 후 적용대상에 적용되어야 한다.

향후 보다 효율적인 QoS를 보장하기 위해서는 다중 링크에 의한 VPN은 본 논문에서 제안한 다중 링크 부하균등에 의한 부하균등 기법을 적용하여야 할 것이다. 그리하면 송수신 패킷에 대한 안정성도 함께 높아질 것으로 예상된다. 본 논문에서는 VPN 한 장비에 다중 링크를 사용한 부하균등 정책을 적용하여 시스템 자원의 이중 낭비를 막을 뿐만 아니라 실시간적인 부하균등 알고리즘을 제안하여 망 상태 적응력을 높일 수 있는 방법도 제안하였다.

향후 연구 과제로는 부하균등 적용 시 패킷 손실을 최소화하는 방법과 지연시간을 최소화할 수 있는 방법에 대해 연구할 것이며, 나아가 획일화된 정보 전송이 목적인 VPN이 아닌 다양한 사용자 환경에 쉽게 적용할 수 있는 다중 링크 부하균등 VPN 처리 방법에 대해 연구할 계획이다.

[참고문헌]

[1] ADTRAN, Understanding Virtual Private Network, pp. 10-11, ADTRAN Inc, 2001.

[2] 김광호, 임채훈 "PPTP와 L2TP의 비교 분석", Cryptography & Network Security Center, Technical Report, pp. 15-17, Sep. 25, 2000.

[3] 오승희, 채기준, 남택용, 손승원, "다양한 트래픽을 이용한 VPN 프로토콜 성능 평가", 정보처리학회 논문지 C, 제 8-C권 제6호, pp. 3-5, 2001. 12.

[4] 박진형, 손주영, "VPN 기술별 트래픽 부하 비교", 멀티미디어 춘계학술 발표 논문집, (페이지 추가) 2003.

[5] Jeff Doyle, Routing TCP/IP Vol.1, Cisco Press, pp. 109-112, 1998.

[6] Micorsoft, Network Load Balancing Technical Overview, Microsoft Windows 2000 Server, White Paper, pp.12-13, 2000.

[7] Stamatis Karnouskos, Ingo Busse, Stefan Covaci, "Place oriented virtual private networks", Proceedings of the 33rd Hawaii International Conference on System Sciences, pp. 3-4, 2000.

[8] Eli Herscovitz, "Secure virtual private networks: The future of data communications", International Journal of Network Management, pp. 2-3, 1999.

[9] P. C. Chu and J. E. Beasley, "A genetic algorithm for the set partitioning problem", The Management School Imperial College, pp. 1-2, April. 1995.

[10] Zbigniew J. Czech, "Heuristic algorithms for solving the set-partitioning problem" Silesia Univ. of Technology, p. 1, June.

1997.

[11] Huican Ahu, Oscar H. Ibarra, "On some approximation algorithms for the set partition problem", pp. 6-7, California Univ. USA

감사의 글

지난 2년간의 대학원 생활 동안 제 삶의 많은 부분을 가르쳐 주신 손주영 교수님께 먼저 감사의 말씀을 전합니다. 지금까지 제가 가르침을 받았던 많은 스승님들 중에 가장 잊지 못할 따뜻한 기억을 제게 주셨습니다. 항상 모자란 저를 이해해 주시던 손주영 교수님의 따뜻한 마음 잊지 않겠습니다.

그리고 심사를 맡아 지도와 조언을 해 주신 박휴찬 교수님과 김재훈 교수님께도 감사를 드립니다.

연구실에서 같이 생활한 연구실 동료들에게 고마움을 전합니다. 같이 공부하면서 많은 것을 도와주었던 진형이와 시간에 쫓기던 나를 위하여 많은 시간 할애해 준 성미에게 감사의 말을 전합니다. 그리고, 다른 연구실에 있는 많은 선•후배님들께 감사드립니다.

또, 대학원을 마무리할 수 있었던 원동력이 되어준 (주)오성사 전산부 여러분들에게 깊은 감사의 말씀드립니다. 처음 대학원 가겠다던 저를 적극 지원해 주신 윤영재 부장님, 학교 가면서 일하면 부담된다며 대신 일을 해주셔서 저의 어깨를 가볍게 해 주신 이해심 많으신 김현찬 과장님, 학교 후배지만 언제나 친절하게 많은 도움을 주는 승철, 예쁘고 침착한 홍일점 최은옥씨, 이 분들에게 다시 한번 정말 감사하다는 말씀 올립니다.

저의 학업에 대한 열정만큼이나 더 큰 열정을 가지고 계신 사랑하는 나의 부모님, 언제나 믿음이 가는 형과 형수들 그리고, 예쁜 조카들 끝으로 나에게 따뜻함만을 전해주어 나의 이 모든 일들을 가능하게 해준 주희에게 영광을 바칩니다.