Journal of Korea Multimedia Society Vol. 7, No. 11, November 2004(pp. 1580-1587)

다중링크 가상사설망을 위한 부하균등 기법

김정우†, 손주영††

요 약

현재 다중링크 연결을 지원하는 가상사설망(VPN: Virtual Private Network) 장비들은 연결된 다중링크를 회선 장애 발생 시 회선간의 전이 기능을 위한 것으로만 활용한다. 전이 방식으로 장애가 발생할 경우를 대비하는 것은 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 늦어지게 되고, 나아가 응용들의 요구 조건을 모두 수용할 수 없게 된다. 본 논문에서는 다중링크를 모두 이용하는 가상사설망을 형성하고, 회선간의 부하균등을 기함으로써 회선의 활용도를 크게 높여 결과적으로 가상사설망의 대역폭을 높이는 효과를 얻을 수 있는 기법을 제안한다. 뿐만 아니라 회선 장애가 발생하였을 때는 기존의 가상사설망 장비가 시행하는 회선 전이 기술을 함께 적용하였다. 결론적으로 다중링크로 연결되어 있는 가상사설망의 가용성을 유지하면서 대역폭을 크게 높이는 효과를 얻을 수 있었다.

A Load Balancing Scheme for Multi-Link VPNs

JungWoo Kim†, Jooyoung Son††

ABSTRACT

Nowadays, VPN(Virtual Private Network) devices supporting multi-link connections only utilize the second link to backup the fail-off primary link. In practice, however, the occurrence of the link fail-off is so rare that the capacity available on the second link is wasted. In this paper, a scheme of establishing a VPN with multi-links, and load balancing between the links under normal circumstances is proposed in order to take advantage of multi-links, and to eventually increase the effective bandwidth of the VPN. Additionally, the transition functionality is also applied for the link fail-off case like existing VPN devices. Consequently, the proposed scheme enables VPNs with multi-links not only to maintain the higher availability but also to highly increase the effective bandwidth.

Key words: VPN(가상사설망), Multi-Link(다중링크), Load Balancing(부하균등)

1. 서 론

VPN(Virtual Private Network)은 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. 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

※ 교신저자(Corresponding Author) : 김정우, 주소 : 부산시 동래구 온천1동 180-4번지(607-833), 전화 : 051)556-0561, FAX : 051)552-2168, E-mail : jwkim@ohsunghq.co.kr
접수일 : 2004년 2월 16일, 완료일 : 2004년 6월 7일
† 준회원, (주)오성사 전산부
†† 정회원, 한국해양대학교 컴퓨터공학과 교수
(E-mail : mmlab@hhu.ac.kr)

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. 앞으로 VPN을 통한 더욱 강화된 보안 데이터와 멀티미디어 데이터 전송의 요구가 증가될 것으로 예상되므로 VPN 회선의 효율성 극대화가 중요하다. 현재, 단일 링크를 이용하였을 때 발생하는 데이터 손실과 회선 결함으로 인한 통신 단절에 대비하여 다중링크를 VPN에 채택하는 추세이다. 그러나 현재 다중링크는 주 링크와 부 링크로 그 기능이 구분되어 있고, 주 링크 상의 문제가 발생하였을 때, 부 링크가 주 링크를 대신하여 기능을 수행하는 방식이 일반적이다. 이 경우, VPN의 결함 복구 능력은 향상되는 반면, 설치되어 있는 링크 전체의 전송 능력을 최대로 활용하지 못하는 결과를 가져온다. 따라서 설치되어 있는 모든 링크를 이용하는 VPN을 형성함과 동시에 VPN을 형성하는 링크간의 부하균등 기능이 필수적으로 요구된다. 본 논문에서는 다중링크를 이용하여 보안이 강화된 가상적 전용선의 기능을 충실하게 하는 VPN 형성 기술을 소개하고, 여기서의 부하균등 문제점에 대해 논의하며, 다중링크 VPN에 적용될 수 있는 부하균등 기술을 제안한다.

VPN 서비스를 제공하기 위한 세 가지 기본적인 기술 요소는 터널링(Tunneling), 인증(Authentication), 그리고 암호화(Encryption)이다[1]. 1990년대 전용선을 설치하는데 드는 비용보다 저렴하면서도 전용선과 비슷한 기능을 제공해 주는 프레임 릴레이(Frame-Relay) 망이 등장을 하면서 전용선은 프레임 릴레이로 차츰 바뀌게 되었다. 그리고 신속한 패킷 전송을 위한 비동기전송모드(ATM) 기술이 등장하면서 일부 백본망들은 비동기전송모드로 구성되어 왔다. 그러나 이들 망들은 원격 접근(Remote Access)에 적절치 못한 단점을 안고 있었고, 이점을 해결하기 위해 L2F (Layer 2 Forwarding)를 계승한 L2TP(Layer 2 Tunneling Protocol)가 등장하게 되었다. L2TP는 IETF를 통하여 표준화된 IP 터널링 프로토콜 중 한 가지로서 PPP 프레임을 캡슐화한 다음 X.25, IP, 프레임 릴레이, 비동기전송모드 등의 망으로 전송하게 된다. L2TP가 등장하면서 ISP (Internet Service Provider)측에 다이얼 업(dial-up) 서비스 등을 제공하게 되었으며 ISP측은 기반통신망이 없이도 사용자에게 서비스를 제공할 수 있게 되었다.

Microsoft에서 개발한 PPTP(Point to Point Tunneling Protocol) 기술은 터널링 프로토콜 중에서 개선된 GRE(Enhanced Generic Routing Encapsulation)를 사용하여 터널을 형성한다. PPTP는 터널의 유지보수를 위해 TCP 연결을 사용하며 인증과 암호화를 제공하기 위해 PPP를 이용하며 GRE(Generic Routing Encapsulation)를 이용하여 내부의 데이터는 숨겨 전송한다[3]. 또, 응용 계층에서 사용자 ID와 암호로써 인증된 사용자를 구분하므로 장비와 IP 주소를 기반으로 인증을 하는 IPSec(IP Security)과는 달리 사용자 단위의 인증을 할 수 있다는 장점이 있다. PPTP는 L2TP/IPSec이나 L2TP/PPP, 그리고 IPSec 등과 달리 NAT(Network Address Translation)와 연동되는 장점이 있다. 그러나, 현재까지 드러난 PPTP의 가장 큰 문제점은 종단 대 종단이 아닌 중간 장치를 거쳐서 터널을 형성하므로 패킷 자체에 대한 무결성 검사를 할 수 없기 때문에 보안상 취약점으로 가지고 있다는 점과, 터널당 한 개의 세션만 연결이 가능하여 사용할 수 있는 환경이 한정적이라는 점이다. 그리고, PPTP는 비동기전송모드 망을 지원하지 못한다는 점을 단점으로 가진다.

최근에는 계층 2 터널링 기술인 L2TP와 계층 3 터널링 기술인 IPSec을 동시에 사용하는 경우도 많다. 이는 L2TP의 동적 터널 할당(Dynamic Tunnel Allocation) 기능에 IPSec을 사용함으로써 더욱 보안이 강화된 환경에서 사용 가능하며 패킷의 무결성도 보장해 줄 수 있기 때문이다[4]. 이후 인터넷이 보급되고 백본망이 MPLS 망이나 IP 망으로 대체되면서 IP-VPN이 등장하게 되었고 IETF에 의해 IP Security(IPSec) 기술이 등장하게 되었다. IPSec 기술은 현재 종단간(end-to-end) 기술보다는 원격접근(remote-access) 쪽에 많이 사용되는 기술이며 사용자 지점부터 SP의 POP 지점까지를 연결하여 서비스를 제공하고 있다[5]. 그러나 IPSec은 부하를 가장 많이 가지는 특성에 따라 제한적으로 사용되고 있으며 높은 보안성을 요구하는 분야에서 주로 사용되고 있다[2,3].

계층 3 기반 라우팅 정보를 이용하는 부하균등 기법에는 크게 두 가지 방식이 있다. 목적지 주소에 의

거한 목적지별 부하균등과 패킷 단위로 이루어지는 패킷별 부하균등이다. 목적지별 부하균등은 특정 목적지를 향하는 패킷들은 하나의 링크를 통해 전송되는 방식이다. 여기서는 호스트의 망 이용 빈도에 따라 링크의 사용 빈도가 불균형을 이룰 수 있다. 패킷별 부하균등은 동일한 목적지로 향하는 패킷이더라도 서로 다른 링크를 통해 전송되어 링크간의 부하균등을 이루는 방식이다. 여기서는 패킷의 도착순서가 뒤섞이는 현상이 발생할 수 있는 단점을 가진다. 기존의 부하균등 기법은 응용과 동적인 링크의 특성을 고려하지 않는다. 본 논문에서 제안하는 응용에 따른 동적인 링크 부하균등 기법은 링크간의 부하균등을 달성할 때 응용에서 발생시키는 트래픽 특성을 고려하면서 동적인 링크 상황을 즉각적으로 반영할 수 있는 점에서 유리한 기법이다.

논문의 구성은 다음과 같다. 2 장에서는 다중링크를 활용하는 VPN 형성 기법과, 링크간의 부하균등 기법에 대해 설명한다. 3 장은 시뮬레이션 환경을 구축하고 그 환경에서 제안된 기법의 성능을 분석한다. 마지막으로 결론을 4장에서 제시한다.

2. 다중 링크 VPN

2.1 응용별 VPN 부하

부하균등의 기준을 설정하기 위해 응용이 발생하는 트래픽의 특성을 관찰하였다. 관찰 대상인 응용의 종류는 통신망에서 활용되는 가장 대표적인 것으로 선정하였다. 프로토콜 상의 낮은 계층에서 매우 짧은 패킷 크기를 송수신하는 Ping, 대표적인 문자(text) 위주의 크기가 작은 데이터를 발생시키는 telnet, 그리고 상대적으로 크기가 큰 데이터를 발생시키는 http 등이다. 이들 응용을 VPN이 적용되지 않은 환경과, 다양한 VPN 형성 기술(PPTP, L2TP, IPSec Tunnel ESP, L2TP/IPSec Tunnel ESP)에 의해 형성된 VPN 환경에서 각각 실행하여 발생되는 트래픽 부하를 관찰하고 분석하였다. 부하 측정 실험을 위한 통신망 구성은 그림 1과 같다. 부하 측정은 터널의 각 종단점 양쪽 즉, 그림 1의 A, B, C, 그리고 D 등 네 곳에서 이루어졌다.

그림 2, 3, 4에서 VPN이 형성되어 있지 않은 경우(non-VPN)를 제외하고, 모든 응용에 대해 부하가 사다리꼴 형태로 형성되는데 이는 두 게이트웨이 간에 형성되어 있는 VPN 터널 간에 일정 크기의 부하가 대칭적으로 발생함을 나타낸다. 특히 클라이언트 측에서는 모든 기술에 대해 부하가 non-VPN과 동일하게 작용하는 반면, PPTP만 약 2.31배의 부하가 발생했으며, PPTP 서버로 가기 위해 GRE 터널을 통과하는 과정에서도 약 2.12~2.31배의 부하가 발생하는 것을 볼 수 있다. L2TP나 IPSec, L2TP/ IPSec은 전체적으로 약 1.47~2.01 배의 부하가 발생하며 게이트웨이사이의 터널 간에는 부하가 대칭적으로 발생하였다[4].

ping과 같이 하위계층에서 처리되는 패킷을 발생하는 응용의 경우 PPTP가 가장 큰 트래픽 부하를 발생하였다. 문자 데이터 전달을 위한 대표적인 서비스인 telnet의 경우, 그림 3과 같이 대부분의 부하가 사다리꼴 형태로 발생하고 있으며, 두 게이트웨이 간에 형성이 되어 있는 터널 간에는 일정한 크기의 부하가 대칭적으로 발생하였다. PPTP만 부하가 클라

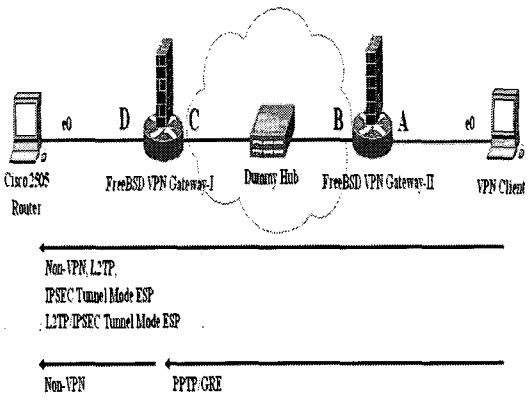

그림 1. 응용별 트래픽 부하 실험을 위한 망구성도

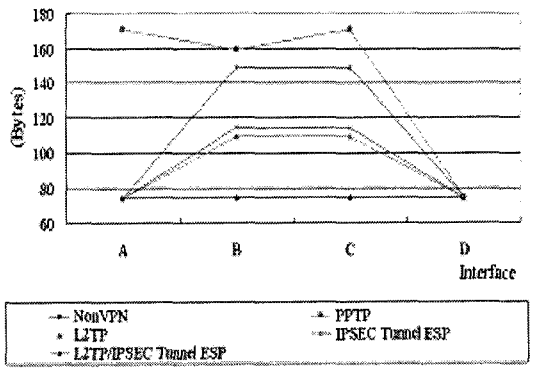

그림 2. ping 응용 트래픽 부하 비교

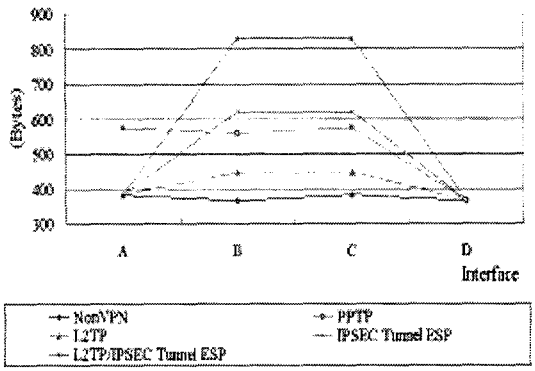

그림 3. telnet 응용 트래픽 부하 비교

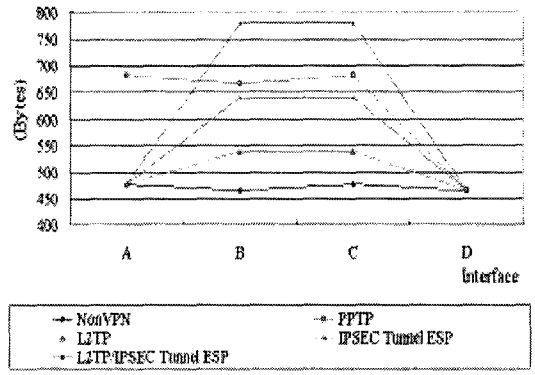

그림 4. http 응용 트래픽 부하 비교

이언트 쪽에 약 1.5배 정도로 크게 발생한다는 점이 특징이나 터널 내에서도 약 1.5배의 부하가 발생해 약 2.0배 이상 부하가 발생하는 IPSec보다는 부하가 적게 발생하는 것을 알 수 있다. 가장 부하가 크게 나타난 것은 L2TP/IPSec 이었으며 약 2.2배의 부하가 발생하였다. 웹페이지 전송 프로토콜인 http의 경우, 그림 4와 같이 L2TP/IPSec이 Non-VPN의 약 1.7배의 부하를 발생하였다. 또, PPTP가 약 1.5배를, IPSec이 그 다음으로 1.4배의 부하를 각각 나타내었다. 가장 큰 부하를 발생시키는 것은 L2TP/IPSec이었는데 이것은 보안에 초점을 맞춘 것으로서 이중으로 터널을 구성하기 때문이다. 특이한 점은 L2TP/IPSec 경우, telnet의 부하가 http의 부하보다 많은 점이다. 이는, telnet에 의해 발생되는 데이터의 크기가 http보다 작고, 그 개수가 많아 터널링에 의한 추가적인 트래픽 발생이 더욱 많아진 것을 의미한다.

다중링크사이에 부하균등을 하는 기준을 응용이 활용하는 전송 프로토콜의 포트 번호로 한다면, L2TP/IPSec를 제외한 경우에는 (ping+telnet), (http)로 분할하여 링크에 할당하면 가장 좋은 부하 분산을 이룬다. 그러나 L2TP/IPSec 경우에는 위의 이유로 해서 (ping+http), (telnet)로 분할하여 링크에 할당하는 것이 좋을 것이다. 이것을 통해 부하균등을 위한 트래픽 분산은 특정 VPN 기술과 응용을 모두 고려하여 동적으로 이루어져야 함을 할 수 있다[5].

2.2 다중링크 VPN 인증 기법

현존하는 장비는 VPN 센터와 VPN 클라이언트 간에 서로 1:1 이라는 정형화된 구성으로밖에 인식이 되지 않으므로 클라이언트 측의 다중링크를 하나의 VPN으로 형성하지 못한다[6]. 즉, 장비에 두개 회선을 설치된 상황에서 부하균등은 이뤄지지 않는 것이다. 이는 VPN 장비 상호 간은 한 회선으로만 터널링이 가능함을 뜻한다. 문제는 하나의 장비에 두개의 키 인증을 할 수 없는 것이다[7,8].

그림 5와 같이 VPN 클라이언트에 두개의 회선을 설치한 후 다중링크 VPN을 형성하고, 평상시에는 부하균등이 A:주(Master), B:부(Slave)사이에 이루어지고, 회선 단절(Fail-Off)에 대비해 A와 B간의 상호 이전(transition)이 원활하여야 한다. VPN을 통해 데이터를 전송하는 도중 주회선에 장애가 발생하면 부회선으로 데이터 전송이 전이(transition)되어 데이터 전송의 영속성을 보장한다.

하나의 장비에 키 인증이 1:다[多]인 경우 현재 하드웨어적으로 해결하지 못하고 있는 VPN 클라이언트 장비의 한계를 극복하기 위하여 논리적으로 다중링크를 이용하는 VPN 형성 과정이 가능하다. 이를 위해 다중링크 VPN은 그림 6과 같은 논리적인 구조를 가진다. VPN 클라이언트는 표 1의 키 인증 알고리즘을 실행한다. 키 인증 절차는 그림 7과 같은 순서로 실행된다.

2.3 다중링크 VPN 부하균등 알고리즘

다중링크 VPN에서 여러 클라이언트 사이에 부하

그림 5. 다중링크 VPN 구조

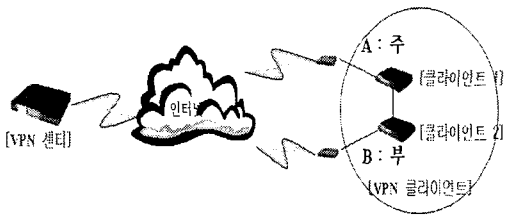

그림 6. 다중링크 VPN 논리적 구조

표 1. 다중링크 VPN 키 인증 알고리즘

1. VPN 센터에 먼저 클라이언트 정보 입력 2. 클라이언트에 키 값을 미리 할당 3. 클라이언트는 자신의 정보를 메모리에 할당하여 클라이언트 2 객체 복제 4. 소프트웨어 복제 시 일정 순서에 의한 키 인증 값을 할당 5. 각 할당된 키 인증 값이 상호 일치할 때 각각의 클라이언트를 분리된 독립 개체로 인식하여 다중링크 VPN 통신이 가능

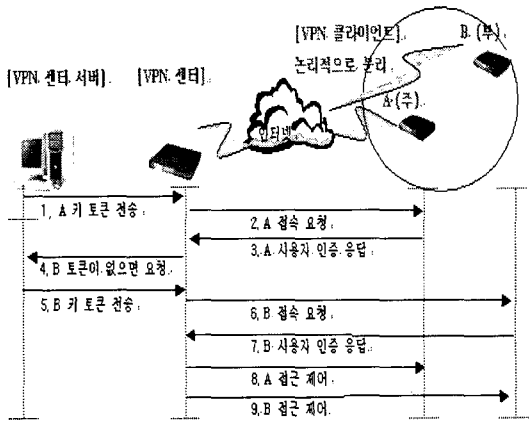

그림 7. 다중링크 VPN 인증 절차

균등을 하기 위한 알고리즘으로 집합 분할(set partition) 알고리즘을 적용하였다. 이를 통해, 패킷의 원활한 흐름과 VPN 클라이언트 주/부 간의 부하 차이를 최소화할 수 있어 결과적으로 전체 링크의 효율성을 증대시킨다.

(1) 집합 분할 알고리즘의 개요

하나의 유한집합 A가 있을 때 A의 부분집합들인 $A_1, ..., A_k$가 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, $A_1 \cup A_2 \cup ... \cup A_k = A$ 일 때, $\{A_1, A_2, ..., A_k\}$를 A의 분할이라 하고, A_i를 블록(block)이라 한다[9,10].

(2) 집합 분할 알고리즘의 적용

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 증대시킬 수 있다. 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 부하균 등 알고리즘을 주기적으로 적용하는 것을 원칙으로 하였다. 부하균등 주기가 $T_t (t \geq 0)$고, 주기별 응용의 개수가 A일 때, T_t마다 A는 유한 집합을 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 부하균등은 크게 두 가지로 구분된다.

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 의한 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.

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. 전송 될 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 분포값을 나타내는 것이 가장 성능이 우수한 것이 된다. 평균적으로 두 블록 간의 가장 작은 차이값을 나타내는 것이 부하균등 시 가장 좋은 성능을 갖게 된다.

3. 실험 및 성능 평가

3.1 실험 모델

그림 8은 부하균등 VPN이 실험되는 환경을 나타낸다. 부하균등 VPN 라우터 시뮬레이터의 운영 환경은 윈도우 95 이상, 메모리 16M, 펜티엄133MHz 이상이다. 스니퍼에 의해 각 응용이 발생하는 트래픽들을 수집하고 그것의 양을 지속적으로 저장하는 데 쓰이는 데이터베이스 서버는 MS-SQL을 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, 부하균등 적용 후 부하균등을 한 실제 응용

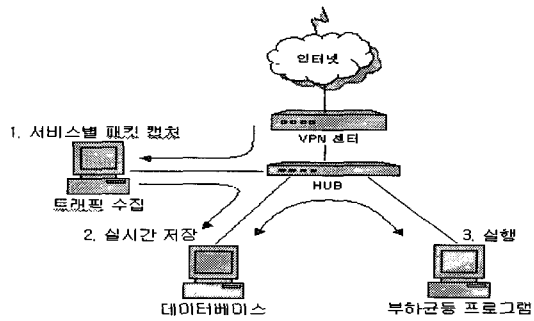

그림 8. 부하균등 VPN 시뮬레이션 환경

별 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 얻는 데 사용된다.

3.2 부하균등 VPN 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.

기존의 부하균등 방법인 응용별 부하균등과 같이 강제적으로 할당하는 부하균등방식 적용 시 적용 간격별 평균치를 주기별로 표시한 것이 그림 9이다.

그림 9에서 적용 간격이 증가 할수록 지속적으로 전송률이 증가함을 알 수 있고, 전송률도 높게 나타나는 것을 알 수 있었다.

그림 9와 같은 응용별 부하균등 방식과 같은 기존의 부하균등 기법은 응용과 링크의 특성을 고려하지 않기 때문에 나타난다. 이런 단점을 극복하기 위한 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 전송

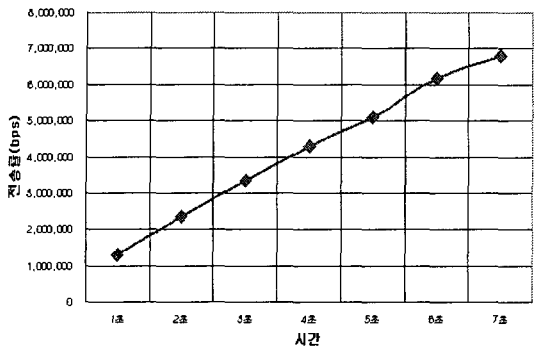

그림 9. 기존 응용별 부하균등시 부하차이값 평균

률이 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 평균한 후 평균치를 주기별로 표시한 것이 그림 10이다.

그림 10에서 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 경우 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 그림 11의 응용별 연속 전송 평균 횟수와 연관이 있다.

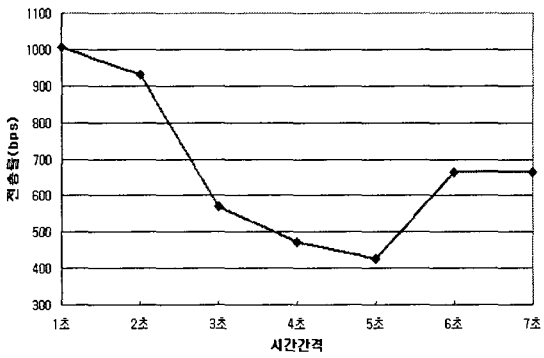

그림 10. 부하균등 적용시간 간격별 전송률 차이 평균

그림 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 링크 간 차이값이 높아지는 원인이 된다.

다중 링크 VPN 부하균등을 적용함에 있어 함께 고려되어야 하는 사항이 처리지연시간이다. 처리지

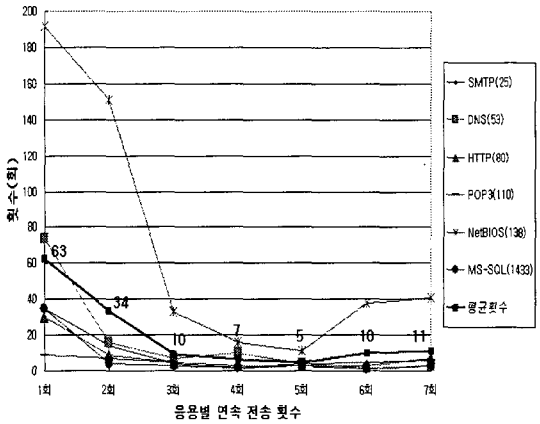

그림 11. 응용별 연속 전송 평균 횟수

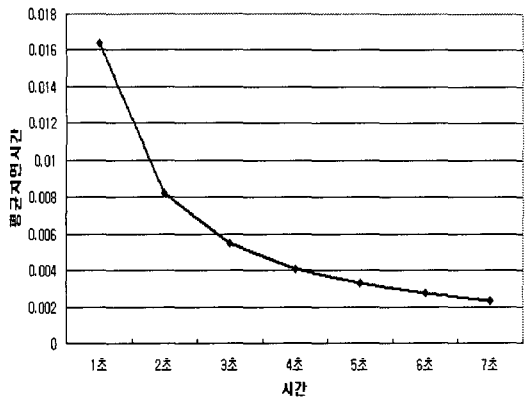

그림 12. 부하균등 적용 간격별 평균 지연시간

연시간은 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. 이것을 그림으로 나타낸 것이 그림 12이다.

그림 12와 같이 다중 링크 VPN 부하균등 적용 간격에 큰 영향을 미치지 않는 시간이므로 부하균등 적용 간격에 대한 처리지연시간은 무시할 수 있다.

4. 결 론

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.

참 고 문 헌

[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, Vol. 8-C, No. 6, pp. 3-5, 12. 2001.

[4] 박진형, 손주영, "VPN 기술별 트래픽 부하 비교", 한국멀티미디어학회 춘계학술논문집, Vol. 6, No. 1, pp. 179-182, 5. 2003,

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

[6] Microsoft, 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", California Univ. USA, pp. 6-7.

김 정 우

1994년~2001년 한국해양대학교 컴퓨터공학과 졸업
2002년~2004년 한국해양대학교 컴퓨터공학과 졸업(석사)
2000년~현재 (주)오성시 전산부 재직

관심분야 : VPN, MANET, 무선 네트워크 프로토콜

손 주 영

1981년~1985년 서울대학교 계산통계학과 졸업
1991년~1993년 서울대학교 컴퓨터공학과 졸업(석사)
1993년~1997년 서울대학교 컴퓨터공학과 졸업(박사)
1985년~1998년 LG전자(주) 책임연구원
1998년~현재 한국해양대학교 컴퓨터공학과 교수
관심분야 : 인터넷 기반 멀티미디어 통신 프로토콜, VoIP MANET, Sensor Network, RFID.