다중 VPN 환경에서의 분산 Perimeter defence 모델에 관한 연구

임 형 진† · 김 태 경†† · 정 태 명†††

요 약

본 논문에서는 다중 VPN을 수용하는 대규모 네트워크에서 인터넷 액세스를 지원할 때, 보안 정책에 따라 신뢰구역(Trust zone)의 불확실한 경계설정으로 발생할 수 있는 보안 문제를 해결하기 위한 적용방안을 제시하였다. 관련연구로 기존 적용모델과 다중 VPN 네트워크에서의 보안 위협을 분석하고, 외부 네트워크로부터의 보호를 위해 신뢰구역 분리와 분산 정책 적용을 고려한 시뮬레이션을 수행하였다. 시뮬레이션을 통해 다중 VPN 수용과 인터넷 액세스에 의한 신뢰구간의 불확실한 경계는 신뢰되지 않은 경계로부터의 분산 계층적인 Perimeter defence 정책 적용을 통해서 개별 VPN간의 신뢰구간을 축소할 수 있었고, 하위 개별 사이트로부터의 적용보다 정책 적용횟수가 줄어 전송 지연에 영향을 줄일 수 있었다.

Cascade Perimeter Defence Model in Multiple VPN Environment

Hyung J. Lim† · Tae-Kyung Kim†† · Tai M. Chung†††

ABSTRACT

This paper analyzed the proper methods to solve the security problems of establishing trust zone which is changed by security policy in large scale networks containing multiple VPNs. Therefore, we surveyed the vulnerability of VPN technologies, it analyzed various models suitable for trust zone. By simulations of various models, we propose the cascade perimeter defence policy model having the merit as such an efficient transit cost and the strictly isolation for trust zone. This model can protect the trust zone from the public network by dividing the trust zone according to each VPN group and it shows the better transit performance by cascading the position of perimeter defence policy.

키워드 : 가상사설망(VPN), MPLS, IPSec

1. 서 론

최근 도입되고 있는 MPLS VPN 망에서는 ISP(Internet Service Provider)의 에지(Edge) 라우터에서 NAT(Network Address Translation), 방화벽(Firewall) 등의 통합기능과 MPLS 프로토콜에 의한 3 레이어 방식에 의한 논리적 회선을 구성하여 가입자들에게 인터넷으로의 트래픽을 하나의 전용회선에 수용할 수 있도록 제공하고 있다. 이로 인해서 ISP에서 제공하는 MPLS VPN은 사용자당 하나의 물리적 전용선으로 인터넷 접속과 VPN 서비스를 통합하여 제공하는 확장성, 유연성을 갖게 된다. 이에 반하여 기존 CPE (Customer Premises Equipment) 기반 VPN 기술에서는 주로 IPSec을 지원하는 장비의 종단(End-to-end)간 VPN 액세스 노드를 이용하여 NAT 기능 제공이나 방화벽 장비들과의 토폴로지 변형을 이용하여 인터넷 접속을 가능하게 하고 있다[1, 5, 7].

사설 네트워크와 인터넷이라는 내부 망과 공중망과의 접합점으로서 CPE VPN 액세스 노드와 MPLS 인터넷 게이트웨이는 보안상 같은 토폴로지에 위치하고 있다. 따라서 CPE 방식에서 요구되던 보안, 운용, 관리에 관한 정책들은 여전히 MPLS 인터넷 게이트웨이에서도 요구되어지며, 논리적인 회선 구분에 의한 여러 VPN을 수용하기 때문에 MPLS 노드들은 많은 VPN 설정 정보들을 유지하고 관리하는 지점이 되며, 악의적인 침입 행동들에 대해서는 치명적이 될 수 있다. 이처럼 인터넷의 발전과 더불어 VPN은 ISP측에서의 서비스 제공 형태로 지원되는 네트워크 기반 VPN 기술로 진화하고 있다. ISP에서의 이러한 다중 VPN 수용과 인터넷 액세스 서비스의 제공으로 인해서 전통적인 로칼 망(Local Area Network)과 인터넷 망과의 접촉 경계에서 구성되던 방화벽에 의한 Trust/Untrust라는 영역의 구분이 불분명해져 가고 있다[1, 12]. 따라서 다중 VPN 환경에서 기존에 로칼 망에서 적용되던 방식과는 다른 확장

※ 성균관대학교 응급의료 정보시스템 개발센타

본 논문은 보건복지부 보건의료기술진흥사업회 지원에 의하여 이루어진 것임 (과제번호 : 02-PJ3-PG6-EV08-0001).

† 정 회 원 : 성균관대학교 대학원 정보통신공학부
†† 준 회 원 : 성균관대학교 대학원 정보통신공학부
††† 종신회원 : 성균관대학교 정보통신공학부 교수

논문접수 : 2003년 8월 11일, 심사완료 : 2003년 12월 3일

된 영역 구분 방식을 정의하는 것이 필요하다고 할 수 있다.

네트워크를 보호하는 정책을 결정하는데 있어서 보호되어져야 할 자원 여부, 즉 대상을 결정하는 것이 무엇보다도 중요하며, 보호할 영역이 외부영역에 대하여 어떻게 안전이 보장 될 것인가 그리고 경계를 구분을 짓는 방안은 무엇인가가 이러한 외부와의 경계지점에 Perimeter defense 메커니즘을 적용하게 되는 동기가 된다[1].

MPLS와 같은 VPN 기술의 진화를 통해 다중 VPN을 수용하는 대규모 네트워크나, 피어 투 피어(Peer-to-Peer) 형태로 발전하는 통신환경에서는 Perimeter Defence 정책으로서 안전하지 못한 외부 네트워크와의 경계구분에 대한 정의가 더욱 명확하게 구성되어야 한다[3, 12] 하지만 다중 VPN을 지원하는 MPLS는 가입자당 논리적인 가상 회선구분 이외에 보안에 관련된 어떤 메카니즘도 제공하지 않는다.

본 논문은 MPLS와 같은 다중 VPN을 수용하는 대규모 네트워크의 인터넷 액세스 모델에서 신뢰구역에 대한 재정의와 효율적인 Perimeter defence 정책을 제시하고자 한다. 이에 2장에서는 관련연구로서 인터넷 접속을 포함하는 IP-VPN 망에서의 취약성 구역(Vulnerability Zone), 보안에 대한 위협 그리고 이에 대한 기존의 Perimeter defence적용모델을 분석하고 3장에서는 다중 VPN 구조를 가지는 네트워크환경에서 제안 망에 적용될 정책의 계층적 분산방식을 정의한다. 또한 4장에서는 시뮬레이션 한 결과를 분석하여, 5장에서는 결론을 제시하고자 한다.

2. 관련 연구

2.1 VPN과 신뢰 구역

VPN 기술이 진화함에 있어서 가장 범용으로 구축되고 있는 기술로서 IPSec VPN과 MPLS VPN이 있으며, MPLS 네트워크는 IPSec과는 달리 보안상 요구이기보다는 다른 필요에 의해서 발전하게 되었다. 이에 대한 대표적인 이유로는 IP 트래픽을 더 확장성 있는 방식을 사용하여 ATM으로 전송하고, 전통적인 라우팅 기법의 기능을 확장하기 위해서였었다[4, 5]. 이러한 MPLS는 ISP에서 서비스 형태로 제공 가능한 네트워크 기반의 VPN으로 진화하고 있으며 또한 전통적인 레이어 2 VPN인 X.25나 Frame Relay의 보안 수준에 이를 정도로 서비스가 제공되고 있다.

MPLS 망에서는 보안상 전송 데이터에 대한 기밀성, 무결성을 지원하지 않는다는 단점이 있으며, 가장 취약할 수 있는 부분으로는 다중의 VRF(VPN Routing/Forwarding instance)를 가진 SP(Service Provider) 네트워크에서 VPN 설정의 복잡성에서 발생하는 문제가 있다[4]. 또한, SP(Service Provider)에서 MPLS 망에 VPN 기능이외에 인터넷의 접속을 제공할 경우에는 개별적인 VPN에 대한 보안 정책이 적용되어야 한다.

IPSec VPN에서는 사이트간(Site-to-Site)에 독립적인 VPN 설정을 하고, 인터넷 접속의 경우는 사이트별로 수행되었다. 반면에 MPLS는 인터넷 액세스를 제공하기 위해서 3가지 형태로 제공되어 질 수 있다. 첫 번째로 물리적으로 분리된 별도의 연결을 하는 경우로서 X.25, Frame Relay를 사용한 VPN과 같이 보안상 안정성을 제공할 수 있지만 MPLS의 장점인 확장성(Scalability)를 제공할 수 없다[4, 5]. 두 번째와 세 번째의 경우로 VRF(VPN Routing and Forwarding Tables)나 가상 방화벽(Virtual Firewall)을 사용하는 경우 사설 주소와 잠재적인 보안 위협문제가 있다[12].

다중 VPN 환경에 정의되는 신뢰구역에서 사설 주소를 사용하는 경우는 NAT 기능을 사용하여 PE(Provider Edge router)나 CE(Customer Edge router) 장비에서 주소 변환을 처리해주어 글로벌한 라우팅 문제를 해결하고, 잠재적인 보안 위협 문제는 방화벽이나 침입탐지 시스템 같은 트래픽 분석 기능을 통해서 해결이 가능하다. 인터넷으로 향하는 VRF에 대한 보안 설정은 개별 VPN 사이트 내에 트래픽 분석 정책을 적용하거나 SP가 각 VPN에 대해 정책을 제공할 수 있다[4, 6-8, 10]. 최근에는 Cosine사의 IPX 제품군과 같이 PE 장비에서 가상 방화벽을 사용하기도 한다[14].

다중 VPN을 수용하는 MPLS VPN 네트워크에 인터넷 액세스 서비스를 제공함에 있어서, 발생 가능한 잠재적인 보안에 대한 위협을 <표 1>와 같이 사설망을 구성하는 VPN기술에 대해서 네트워크의 침입 영역에 따라 분류하여 볼 수 있다[2, 8, 11].

〈표 1〉 보안에 대한 위협

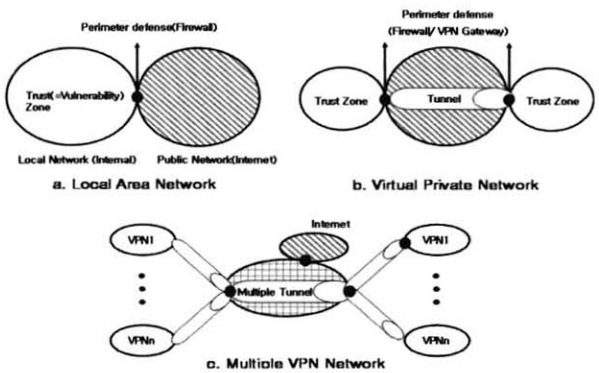
타 입	IPSec VPN	MPLS VPN	공격 패턴
외부로 부터의 침입(인터넷과의 경계 외부)	Public 구간에 위치한 사용자	Public 위치한 사용자	Service Denial, Virus Intrusion Leakage, Malicious user, Authorized user, Masqueraders, Misuser
내부로부터의 침입 (인터넷과의 경계 내부)	내부의 승인된 사용자나 원격 사용자	• 원격사용자 • 내부 승인된 사용자 • 다른 VPN 사용자 (Shared IP infra. 사용)	

외부와의 단순한 경계에 의해서 구분되어지는 보호영역과 보호되지 않는 영역 관점에서 살펴본다면 다중 VPN을 수용하는 MPLS 망에서 인터넷 액세스 모델을 위해 Perimeter defence정책을 어떻게 적용하느냐에 따라서 신뢰구역의 영역이 달라질 수 있게 된다[4, 17]. (그림 1)에서는 전통적인 네트워크와 MPLS 설정에 따르는 신뢰영역의 변화를 인터넷 접속의 항목 구분에 기반하여 나타내었다.

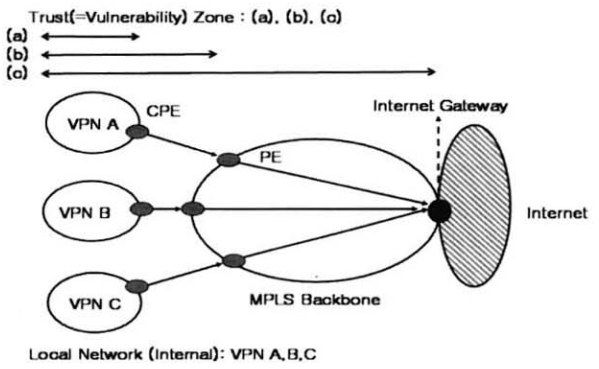
(그림 1)은 로컬 망에서의 전통적인 인터넷 접속시 신뢰구역과 VPN 기술이 발전함에 따라 (c)와 같이 다중 VPN을 수용하는 형태를 나타내고 있다. 이러한 개별 VPN들은 IP 인프라를 공유하기 때문에, 망 내부에서 VPN간 경계와 터널 종단점이 중첩되어 형성된다. 이 경우 MPLS 망에 적용되는 Perimeter defence 정책을 어느 지점에 적용하는가

에 따라 (그림 2)에서와 같이 신뢰구역이 (a), (b), (c)의 다양한 영역으로 나뉘어 질 수 있다. (a)의 경우는 전통적인 로컬 네트워크의 ISP와의 경계에 정책을 적용하는 것이다. 이 방식은 로칼 망에서의 모델을 MPLS 망에서도 그대로 적용한 경우이다. 이 경우에 Perimeter defence 정책의 권한을 로칼 망에서 소유하거나, ISP에서 관리 서비스 형태로 제공할 수 있다. (b), (c)의 경우는 ISP에서 Perimeter defence 정책을 적용하고 관리하는 형태이다. (b)의 경우는 네트워크 에지에서 정책적용을 하였고, (c)의 경우는 다중 VPN 망의 인터넷 게이트웨이 지점에 적용하는 경우이다.

로컬 망 혹은 ISP의 보안 정책에 따라 (그림 2)와 같이 다양한 신뢰구역 영역이 형성될 수 있다. 이러한 다중 VPN 터널 종단 점과 전송망 구간을 고려하지 않은 신뢰구역의 설정은 VPN 외부 영역에 대하여 분명하지 않은 경계구분을 만들게 될 수 있다[15, 17, 20].



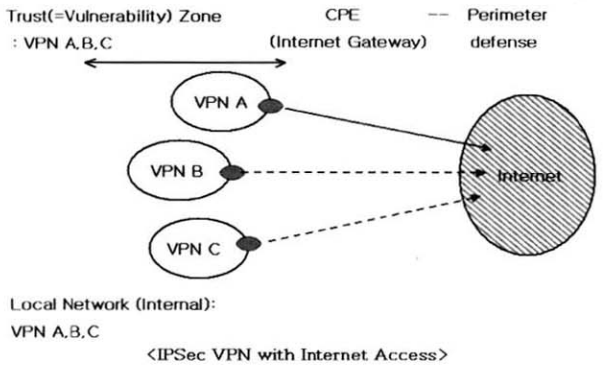
(그림 1) 로컬 망에서의 신뢰구역 모델



(그림 2) 다중 VPN과 신뢰구역

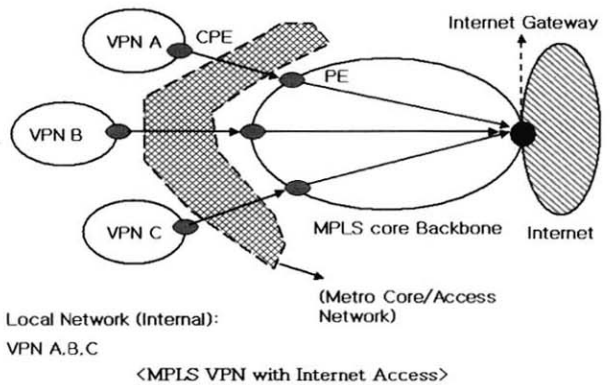
2.2 다중 VPN 수용 네트워크

인터넷 액세스를 하는 IP VPN에 대한 모델은 MPLS-CE 기반 모델, MPLS-PE 기반 모델, CPE 기반(IPSec) 모델 등이 제시되고 있다[13, 17-19]. (그림 3)는 IPSec VPN의 경우로 CPE 장비에서 VPN의 터널 종단기능과 인터넷 게이트웨이, Perimeter defense의 기능을 수행하고, CPE 내부를 신뢰구역으로 한정한다. (그림 4)는 인터넷 액세스와 다중 VPN을 수용하는 MPLS 망을 나타내고 있다. 망의 규모에 따라 CPE 사이트와 MPLS 백본사이에는 VPN을 지원하는 메트로망(Metro Area Network)으로 확장되어 질 수 있다. 네트워크 토폴로지 상에 다중 VPN을 수용한다는 의미는 망 내부에 개별 VPN의 터널 종단점이 존재하고 개별 VPN들이 전송인프라를 공유한다는 의미이다.



<IPSec VPN with Internet Access>

(그림 3) IPSec VPN with Internet Access



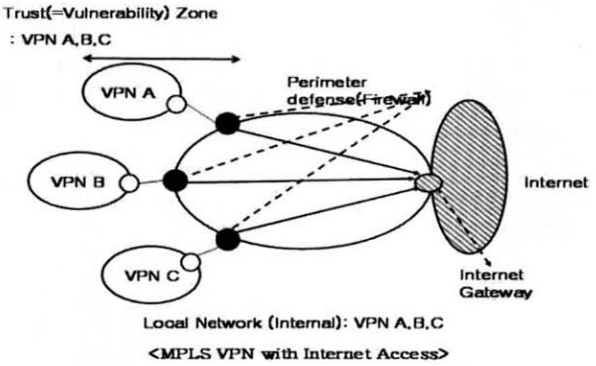
<MPLS VPN with Internet Access>

(그림 4) MPLS VPN Internet Access

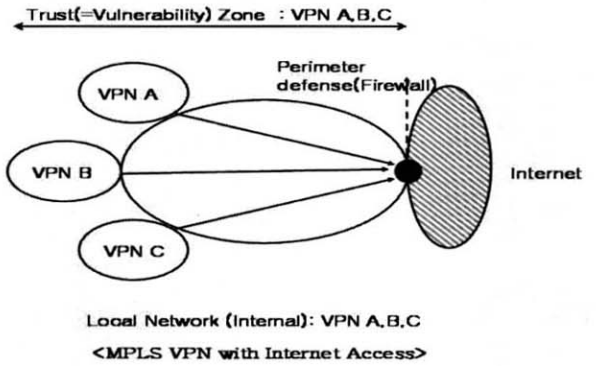
CPE VPN을 사용하는 (그림 3)의 경우는 신뢰할 수 없는 망인 인터넷과의 접촉점이 Perimeter defence 정책 적용점이 되며 VPN 터널의 종단점도 된다. 따라서 신뢰구역은 인터넷과의 접촉점 내부가 된다. 하지만 (그림 4)와 같은 다중 VPN을 수용하는 망에서는 하나의 VPN에 속한 CPE 입장에서 볼 때 인터넷과의 경계와 터널 종단점이 일치하지 않을 수 있으며 Perimeter defence 정책 적용 지점에 따라 인터넷과의 경계는 CPE나 PE 혹은 MPLS 게이트웨이 중에서 설정될 수가 있다. 어떤 VPN 정책을 사용하느냐에 따라서 신뢰구역의 범위는 확장되거나 축소되어 질 수 있다[9, 15].

(그림 5)과 (그림 6)은 인터넷 액세스 모델로서 인터넷 게이트웨이 지점에 Perimeter defence 정책이 적용되는 경우와 인터넷 게이트웨이가 아닌 PE 장비에 적용되어지는 경우를 나타내고 있다. 마지막으로 IPSec VPN의 모델처럼 CPE와의 경계에 Perimeter defence가 적용되어질 수 있는

모델로서 CE-기반 MPLS 모델이 있다[13, 17-19, 21].



(그림 5) PE에 Perimeter defence 적용



(그림 6) 인터넷 게이트웨이에 Perimeter defence 적용

3. 정책의 분산 적용 모델

3.1 정책 구조와 벡터

임의의 공격으로부터 네트워크를 보호하기 위해 다양한 Perimeter defence 정책들이 구성되고 적용되는데, 다중 VPN 네트워크 환경에서 VPN간의 신뢰 구역 설정을 위해서 Perimeter defence 정책은 방화벽, 침입탐지 시스템, IPSec을 통해서 네트워크 보안을 제공할 수 있다. 이러한 Perimeter defence 정책이 제공할 수 있는 보안 속성은 다양하여 방화벽기반, 침입탐지시스템 기반, IPSec 터널모드 기반의 보안 보호영역을 통해 분류하고자 한다. 방화벽은 침입자로부터 보호되어져야 할 자원을 보호하기 위한 네트워크 정책 요소이다. 반면 침입탐지시스템은 네트워크와 시스템에 대하여 내, 외부의 공격과 이상행동을 탐지해 내는 정책 요소이다. 방화벽은 네트워크 계층상의 가장 낮은 계층에서부터 응용계층에까지 구현되며 크게 라우터, 프락시, Stateful inspection 형태 기술을 구현한 경우로 나뉠 수 있다[12]. 이에 반하여 IDS는 크게 네트워크 기반, 호스트 기반 형태로 구분되어지고 침입을 탐지해내는 패턴에 따라 다양한 형태를 가지게 된다. IPSec은 네트워크로 전송되는 패킷에 기밀성, 무결성을 제공하여주고 인증된 사용자만이 네트워크에 접속 할 수 있도록 하는 기능을 제공하여 준다[4, 5, 10, 16].

본 논문에서는 방화벽, 침입탐지 시스템, IPSec 터널의 속성을 구분할 수 있는 8튜플(tuple)로서 Perimeter defence 정책 구조를 정의한다. 8개의 요소는 address(A), protocol (P), service(S), user(U), direction(D), Network-based IDS (N), IPSec(I) Host-based IDS(H)로 구성된다. N과 H는 침입을 탐지해 내는 패턴에 따라서, I는 IPSec이 지원하는 트랜스포트 모드, 터널모드, 중첩모드에 따라서 하위 튜플(Tuple)로 세분될 수 있다. A는 MAC address, IP address, Port number를 포함하고, P는 IP, TCP, ICMP, UDP 등을 포함한다. U는 사용자 그룹이나 사용자 등을 포함한다. 또한 S는 FTP, SMTP, SNMP, TELNET, HTTP 등을 포함하며, D는 Read(in flow), Write(out flow), 원격 실행의 특징을 가리키게 된다. Perimeter defence 정책의 8가지 튜플 특징은 신뢰할 수 없는 구역(untrust zone)에서 신뢰구역에 대한 Perimeter defense 정책들을 기능적인 세분화를 통하여 사용자에게 종단간 보호에 대한 함축성, 신뢰성, 투명성의 정도를 확장할 수 있도록 한다.

신뢰구역의 경계로부터 네트워크 경로 상에 Perimeter defence 정책은 8가지 요소의 조합인 튜플로서 적용되어질 수 있으며, 다음과 같이 정의할 수 있다. 일련의 Perimeter defence 정책 적용횟수를 k라 하면, 이는 보호되어져야 할 네트워크 자원과 침입자 사이에 경로상의 Perimeter defence 정책이 적용된 횟수를 나타낸다. 높은 k일수록 종단간의 보안에 있어서 신뢰성이 증가하게 된다. K(A)는 A 속성을 가지는 방화벽, K(P)는 P 속성을 가지는 방화벽으로 나타내어 질 수 있으며, 보안 수준에 있어서 K(A), K(P)가 반드시 동일한 보안 수준을 가지는 것은 아니다. 개별적인 이러한 속성들은 네트워크 보안 정책에 따라 조합되어 질 수 있으며, 예를 들어 라우터 기반의 방화벽은 A속성을 포함하고, 서버기반 방화벽은 A, P, S의 속성을 갖게 된다. 또한 침입탐지시스템 기능을 갖는 방화벽들의 조합은 N, H의 속성들을 포함하게 된다. 경로 상에 이러한 정책 속성들이 적용되어 질 때마다 전송지연과 이러한 정책을 지원하기 위한 장비나 소프트웨어의 투자 등의 비용으로 산출되어질 수 있을 것이다. 신뢰할 수 없는 네트워크로부터의 침입에 대한 일련의 Perimeter defence 정책을 적용할 때 k에 대한 전체 소요 비용과 경로상의 전송지연이라는 두 가지 요소를 고려하여야 한다.

3.2 Perimeter defence 분산 정책

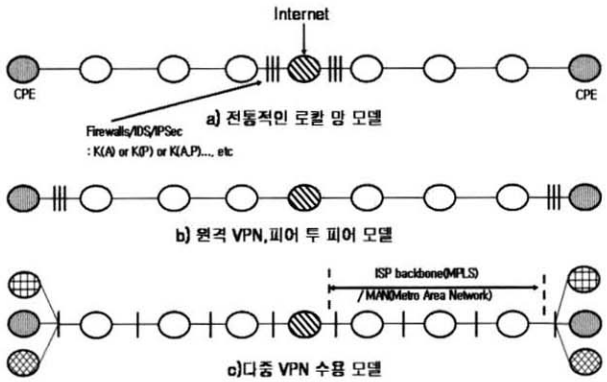
다중 VPN을 수용하는 MPLS 망의 경우 신뢰구역은 크게 두 가지로 구분될 수 있다. 첫째로, 백본 망 자체는 망에 수용된 개별적인 VPN들이 공유하는 IP 인프라로서 신뢰할 수 없는 외부 망에 대한 신뢰구역이 될 수 있다. 둘째로, 백본 망 내부에는 개별적인 정책을 가지는 VPN들이 터널 종단 점을 형성하게 되고, 이때 전통적인 로컬 망에서 사용하던 Perimeter defence 정책 방식을 적용할 경우, 다른 신

뢰구역이 형성 될 수 있다. 이때 각 VPN별 사이트마다의 요구되는 보안정책도 다를 수 있으며 일관된 정책을 유지할 수 없을 경우 신뢰구역이 중첩되거나 필요 이상의 비용이 소요될 수 있다.

Perimeter defence 정책 적용 방식에 있어서 (그림 7)과 같이 세 가지 설정방식을 고려할 수 있으며 전통적인 로칼망과 원격의 VPN 사이트나 원격 VPN 클라이언트의 경우는 (그림 7)에 a, b의 형태를 가진다고 할 수 있다.

(a) 전통적인 로칼 망 모델

인터넷을 액세스하는 전통적인 로컬 망에서 적용되던 모델로서, 인터넷 전용선과 로컬 망과의 경계지점에 외부 망과의 경계를 설정할 목적으로 방화벽과 침입탐지 시스템을 적용하게 된다. 이는 신뢰할 수 없는 외부 망과의 경계지점인 인터넷 망과의 접촉 경계로부터 전체 네트워크를 보호하는 경우이다.



(그림 7) Perimeter defence 정책 적용 방식

(b) 원격 접속 모델 혹은 피어 투 피어 모델

VPN의 확장 형태로서 네트워크 내부 혹은 보호되어져야 할 호스트 자체적으로 Perimeter defence 정책을 적용하는 경우이다. 원격 접속 VPN 클라이언트의 경우 VPN 설정과 인터넷 액세스를 위하여 개인 방화벽(Personal Firewall)내지 NAT 기능과 같은 Perimeter defence 정책이 적용될 수 있으며, 피어투피어 모델의 경우 이러한 정책이 요구되어질 수 있음을 나타내는 방식이다

(c) 다중 VPN 수용 모델

다중 VPN 환경에서는 기존에 적용되던 Perimeter defence 방식을 적용할 경우 다른 VPN간의 접촉 노드에 대하여 해당되는 모든 노드에 정책을 적용한다는 것은 과도한 비용으로 나타나게 될 수 있지만 신뢰영역을 엄격히 구분할 수 있다는 점에서 상관관계가 있다고 할 수 있다. 따라서 다중 VPN 환경에서 Perimeter defence 정책의 적용을 통해서 개별 VPN당 신뢰구역을 축소하고, 망 입장에서는 보안 견고성을 만족할 수 있는 효율적인 적용정책이 요구된다고 할 수 있다.

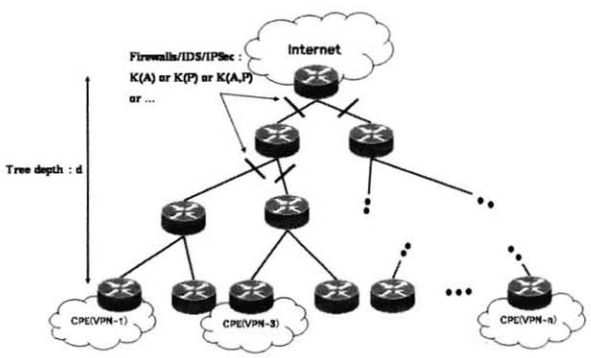
Perimeter defense 지점이 어느 지점에 적용되느냐에 따라 신뢰구역의 영역은 변경되어지며 다중 VPN을 수용하는 MPLS 망일 경우에 (그림 7)(c)는 (그림 7)(a)의 경우보다 신뢰구역이 축소된 상태로서 취약성 구역의 축소관점에서 볼 때 더 적합한 구성이라고 할 수 있다. 대규모 망에서 신뢰구역이 클 경우는 구역내부의 취약성 구역이 커진다는 말이며, 보호와 관리 되어야할 자원의 영역이 넓어짐을 의미한다. 하지만 인터넷과의 경계는 여전히 인터넷 망과의 접촉점인 인터넷 게이트웨이이고, VPN 전용선 서비스를 제공하는 ISP의 MPLS망 자체도 신뢰할 수 없는 인터넷 망으로부터 그리고 VPN 사용자와 내부 사용자들로부터 보호될 수 있는 정책이 적용되어야 한다. 또한 MPLS망의 인터넷 게이트웨이와 CPE 혹은 PE 사이는 다중 VPN이 교차하거나 터널 종단점들이 존재할 수 있는 지역으로 보안 수준에 따라 어떤 Perimeter defence 정책도 적용되어지지 않거나 (그림 7)(c)와 같이 중첩노드마다 모두 적용되어 질 수 있다.

위의 세 가지 Perimeter defence 적용을 위한 모델의 차이는 다중 VPN 환경에서 보호되어져야 할 자원들에 대하여 주어진 네트워크에서 인터넷 게이트웨이까지의 경로상에 정책을 전체노드에 적용을 하거나 혹은 VPN당 개별적인 적용을 하느냐에 따라 구분할 수 있다. 즉, 망에서 요구되는 보안 수준에 따라서 적용되는 Perimeter defence 정책은 정책의 분산과 집중에 따라 구분되어질 수 있다.

4. 분산 Perimeter defense 정책 시뮬레이션과 분석

4.1 다중 VPN 네트워크 모델

본 논문에서는 시뮬레이션 모델로서 (그림 7)(c)와 같은 인터넷 망과의 경계를 가지고 다중 VPN을 수용하며, 인터넷 액세스를 지원하는 MPLS 망에 정책 적용을 고려하였다. 따라서 단일 VPN을 구성하는 망에서의 정책 적용방식과 비교, 분석하여 일련의 분산방식을 사용하는 정책적용 방식을 제안하게 되었다.



(그림 8) Depth 4의 다중 VPN 네트워크

인터넷 망과의 경계로부터 CPE까지 네트워크 토폴로지

를 구성하여 볼 때, 개별 VPN들의 인터넷 액세스 경로들은 트리 형태 구조를 가지게 되며, 인터넷 망과의 경계를 나타내는 지점이 트리 구조의 루트 노드가 되며 리프(leaf) 노드는 CPE 구간이 된다. 여기서 그래프에 나타나는 노드의 전체 수는 망의 규모를 나타낸다. (그림 8)은 이러한 Depth 4를 가지는 다중 VPN 네트워크 토폴로지를 나타내고 있다.

이 시뮬레이션에서 사용된 토폴로지는 완전이진트리가 아닐 경우 시뮬레이션 결과의 분산도가 높아 어떤 패턴을 찾아내기 어려웠다. 가입자(CPE)당 정규화된 비용을 계산하기 위해 완전 이진트리(completed binary tree)를 사용하였다. 또한 적용모델에 나타난 최소 경로(Internet gateway -> PE -> CPE) 이상이 될 수 있도록 트리 depth를 3 이상으로 하였으며 이는 MPLS 다중 VPN의 기본 구성 요소들을 구성할 수 있는 구조이다.

인터넷과의 경계까지 경로(path)상 요구되는 Perimeter defence 정책 적용 횟수인 k값은 정의된 정책 구조들 중 망에서 신뢰구역을 설정하기 위해 요구되는 전체 튜플들의 조합을 의미하며, 노드간에 적용할 때마다 1씩 증가시켰다. 실제 망에서는 ISP 혹은 로컬 망의 VPN 보안 정책이나 네트워크 토폴로지에 따라서 k값은 경로마다 달라질 수 있기 때문에 시뮬레이션을 정규화하기 위해서 조합 튜플 수에 대한 가중치는 두지 않았다. 따라서 적용횟수가 네트워크의 보안 강도를 의미하지는 않으며, 적용 횟수와 적용 범위의 분산도에 따라 신뢰구간의 분리와 축소를 가능하게 하는 척도로서 사용하였다. 네트워크에서의 신뢰구간은 점진적인 분산 정책 적용에 따라 외부네트워크와의 경계로부터 혹은 CPE에 인접한 노드로부터의 분산도가 높을수록 불명확한 신뢰구간을 축소할 수 있다. 정책을 트리의 리프 노드에 할당할 경우 이는 CPE의 보안정책을 의미한다. Perimeter defence 정책 적용 횟수가 0인 경우에 k는 0이며, 네트워크 상에 어떤 Perimeter defence 정책도 적용되지 않았음을 나타낸다.

입력값으로서는 전체 노드에서의 정책 적용 횟수 k와 트리의 depth d값을, 출력 값으로서는 인터넷 경계로부터 CPE (=리프) 노드까지의 경로상의 지연(delay)과 망 전체에 대한 비용을 계산했다. 다중 VPN을 수용하는 네트워크에서 정책에 대한 비용은 적용되어진 총 정책(Perimeter defence)의 횟수로 나타냈고, 경로상의 지연은 리프 노드로부터 루트 노드까지의 Perimeter defence의 적용회수로 나타냈다.

네트워크의 non-perimeter defence 요소에 대하여서는 경로상의 지연에 영향을 받지 않는 것으로 가정했다. 신뢰구역의 확장, 축소는 정책의 분산도가 높으면 축소되는 것으로 간주했으며 이를 위한 세부적인 정책정의는 사용하지 않았다. 이 시뮬레이션은 신뢰구역의 축소와 이에 따르는 비용을 최적화하기 위해서 사용하며, 분산방식에 따라서 전체 망에서 소요되는 비용과 신뢰구간의 상관관계를 비교할 수 있다.

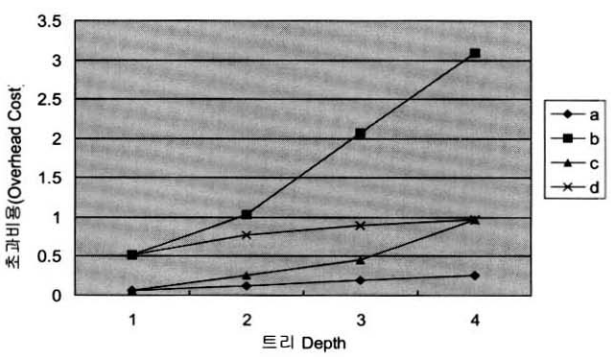
정규화된 Perimeter defence의 비용은 다중 VPN을 수용한 MPLS 망에 전체 정책 적용 횟수를 노드의 전체수로 나눈 값으로 나타낸다. 이는 전체 노드에서 적용되어지는 Perimeter defence 정책에 대한 초과 비용(Overhead cost)을 의미한다. 시뮬레이션 결과는 (그림 9)과 (그림 10)에 트리 depth가 각각 4, 7일 때를 나타내고 있다. 두 결과 모두(a)와 (b)는 전통적인 로컬 망 모델과 원격 VPN 모델에서의 Perimeter defence 정책을 적용한 결과를 나타내고 있다. 기존의 보안 수준을 유지하고, 신뢰구역을 축소할 수 있는 방안으로서 (c)는 (a)의 분산 모델로서, (d)는 (b)의 분산모델로서 정책을 적용하였다. (그림 7)(c)와 같이 정책의 분산을 통해 다중 VPN간의 신뢰영역을 축소하고자 하였으며, (a), (b) 두 모델 관점에서 일련의 정책 분산을 고려하였다.

4.2 정책 적용 방식에 따른 비용 분석

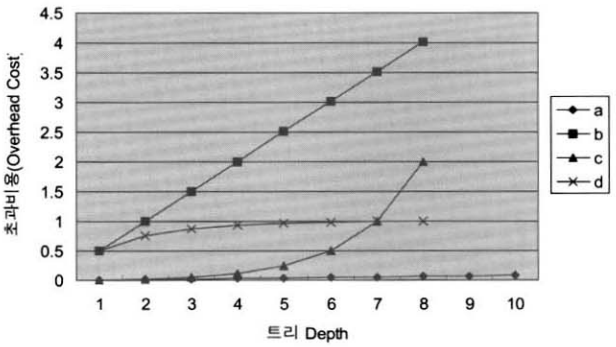
3.2절에서 제시한 정책 적용에 대한 접근 방식들에 대하여, VPN간 요구되어지는 분리 정책을 모든 구간에 적용하는 것이 아닌 각 접근 방식별로 점진적으로 증가하며 비용 분석을 하였다.

(a)에 대한 비용 : 인터넷과의 경계지점과 인접한 경로에만 다중 Perimeter defence 정책을 점진적으로 적용하였을 때 나타난 값이다. 여기서 VPN 가입자가 증가하거나 적용되는 정책 횟수가 증가하더라도 비용에는 거의 영향을 주지 않았다.

(b)에 대한 비용 : (그림 7)에서와 같이 Perimeter defence 정책을 CPE에 인접한 경로에만 적용하기 때문에, 그 사이트가 증가함에 따라 Perimeter defence 정책 적용 횟수(k)의 증가율보다 더 큰 비용의 발생이 나타났다. 이는 VPN 가입자가 증가할 때 가입자마다 Perimeter defence 정책을 리프 노드에 인접한 곳에 적용할 경우 망 입장에서는 가입자의 증가만큼 비용이 늘어나게 됨을 의미한다.



(그림 9) 트리 depth가 4일 경우



(그림 10) 트리 depth가 7일 경우

(c)에 대한 비용 : 일련의 Perimeter defence 정책을 적용함에 있어서 인터넷과의 경계로부터 Top-down 방식으로 분산 적용한 경우이고, 이에 대한 비용은 망 전체의 경로마다 적용 정책이 분산될 때 비용이 점진적으로 증가함을 보여주고 있다.

(d)에 대한 비용 : 리프 노드에 인접한 경로부터 Bottom-up 방식으로 분산 적용한 경우로서, 이에 대한 비용은 적용 정책의 증감에 관계없이 망 전체에 적용된 비용에 근접한 값을 나타내고 있다.

완전 이진 트리의 노드의 증가와 적용방식에 따라 비용의 증감치를 수식으로 표현하면 다음과 같다. 트리의 depth를 d라 하고, Perimeter defence 적용회수를 k, 총 노드수가 t 일 때 비용은 아래의 식과 같다.

(a)경우 : $2k/2^i$ (b)경우 : $k*2^d / \sum_{i=0}^{d} 2^i$

(c)경우 : $\sum_{i=1}^{k} 2^i / \sum_{i=0}^{d} 2^i$ (d)경우 : $\sum_{i=d}^{0} 2^i / \sum_{i=0}^{d} 2^i$

분산 방식을 적용한 (c)와 (d)의 비용은 트리의 모든 경로에 정책을 적용했을 때 교차지점이 나타나게 된다. (그림 8)과 (그림 9)에서처럼 트리의 depth가 증가하면 교차점이 오른쪽으로 이동하고 감소하면 왼쪽으로 이동한다. 이는 망의 전체 노드수가 작아질 경우 전송경로상의 홉(hop)수도 줄어들게 되며, 신뢰구역을 축소하기 위해 요구되는 분산 정책 적용의 횟수가 감소함을 나타낸다.

4.3 정책 적용 방식에 따른 비용과 신뢰 구간간의 상관 관계

(a)와 (c)의 상관관계 : 루트 노드로부터의 분산여부에 따른 정책적용 방식인 (a)와 (c)를 비용의 오버헤드 측면에서 비교해보면 루트와 인접된 노드에만 정책을 적용한 (a)가 분산 적용한 (c)보다 망 전체의 비용이 적게 나타나고 있다. 반면에 분산 적용한 (c)는 (그림 7)에서와 같이 정책적용 횟수에 따라 신뢰구역이 축소되어가고 있다. (a)는 인접한 노드에 집중하여 정책을 적용한 결과 인터넷 경계로부터 CPE(리프)까지의 전 구간을 하나의 신뢰구역으로 설정하게 된다.

(b)와 (d)의 상관관계 : 리프 노드로부터의 분산여부에 따른 정책적용 방식인 (b)와 (d)를 분석하면 CPE(리프)에 인접한 노드에 집중된 정책적용 방식인 (b)는 정책 적용회수가 증가하거나 depth가 증가하는 만큼 비용이 증가하고 있으며 (d)의 경우는 트리 노드의 전 경로에 정책 적용을 점진적으로 증가하여 최대 비용 값에 근접하게 나타나고 있다. 신뢰구역의 축소관점에서 보면 (b)의 경우 (그림 7)과 같이 인터넷과의 경계부터 CPE(=리프 노드)까지의 경로 상에 어떤 정책도 적용되지 않고 있으며, 신뢰구역은 단지 CPE 내부만으로 한정된다. (d)의 경우 분산적용 결과 정책 적용의 횟수가 증가함에 따라 다중 VPN을 수용하는 네트워크 내부를 신뢰구역으로 포함해 가고 있다.

Perimeter defence 정책 적용의 4가지 형태에 따른 시뮬레이션을 통해서 신뢰구역과 비용에 영향을 미치는 방식을 분석하여 보았다. 다중 VPN 네트워크에서 최적화된 비용을 나타내는 방식은 인터넷과의 경계지점에 가능한 정책을 집중시키는 방식이었으며, 신뢰구역의 축소에 대하여서는 (c)와 (d)방식이 정책 적용횟수에 따라 점진적으로 신뢰할 수 없는 영역인 인터넷으로부터 다중 VPN 네트워크 내부를 신뢰구역으로 설정해 나가는 모델이었다. (d)의 경우는 전체경로에 정책이 적용되기 전까지 인터넷과의 경계지점에서의 신뢰할 수 없는 영역에 대한 defence 정책이 누락되게 된다. 따라서 (c)에서 인터넷과의 경계로부터의 정책 적용 방식이 네트워크 전체를 보호하는 신뢰구역을 형성하는데 적합하다고 하겠다. 시뮬레이션 결과인 (그림 9)과 (그림 10) 그리고 증감치를 통해서 볼 때 신뢰구역을 보장하고 비용을 최소화할 수 있는 방식으로 (c)의 방식이 가장 효과적인 방식으로 나타났다.

5. 결 론

본 논문에서는 다중 VPN을 수용하는 대규모 네트워크에서 인터넷 액세스를 지원할 때, 다중 VPN간의 경계를 구분 짓고, 인터넷 액세스에 의한 신뢰구간의 불확실한 경계에 대하여 일련의 분산된 Perimeter defence 정책을 적용함으로서 신뢰구간을 축소하여 보안의 취약성을 완화할 수 있는 모델을 제시하였다. 시뮬레이션을 통해 다중 VPN 수용과 인터넷 액세스에 의한 신뢰구간의 불확실한 경계는 대규모 네트워크일수록 신뢰되지 않은 경계로부터 일련의 분산된 Perimeter defence 정책을 적용함으로서 엄격한 신뢰구간 설정과 전송지연을 최소화 할 수 있는 정책모델임을 제시하였다.

다중 VPN 네트워크 내부를 신뢰할 수 없는 외부 네트워크(=인터넷)로부터 보호하고, 개별적인 VPN 가입자간의 신뢰구역을 엄격히 분리할 수 있는 정책 적용 방식이었다. 이

는 네트워크의 규모가 작을 때 보다 네트워크의 규모가 클 때 다른 접근 방식에 비해 비용과 지연, 신뢰구역의 범위가 상반되게 나타났다. 따라서 본 논문에서 제시한 일련의 분산 Perimeter defence정책은 네트워크에 대한 자원의 보안을 더 견고하게 해줄 수 있는 효율적인 정책임을 보였다. 이러한 모델은 실제 네트워크에서는 ISP 혹은 CPE의 보안 정책에 따라 다양한 혼합된 방식이 적용되어 질 수 있으나 전체 네트워크의 효율성과 보안 견고성 관점에서 본 논문에서와 같이 신뢰영역 분리와 비용간의 상관관계를 고려한 정책이 적용되어야한다.

참 고 문 헌

[1] Landwehr & Goldschlag, "Security Issues in Networks with Internet Access," Proc. IEEE, Vol.85, No.12, December, 1997.

[2] Dorothy E. DENNING, "Intrusion Detection Model," IEEE Transactions on Software Engineering, Vol.SE-13, pp.222-232, February, 1987.

[3] 윤재우, 이승형, "IP 기반 VPN 프로토콜의 연구동향 : 확장성과 보안성", 한국정보보호학회, 정보보호학회지, 제11권 제6호, pp.53-43, 2001.

[4] Internet URL, http://rr.sans.org/encryption/mpls2.php.

[5] Frame Relay Forum, "The Path to MPLS," WAVESMITH NETWORK, white paper, 2001.

[6] Paul Knight, Bryan Gleeson, "Network based IP VPN Architecture using Virtual Routers," IETF Internet Draft Provider Provisioned VPN WG, July, 2002.

[7] Ananth Nagarajan, "Generic Requirements for Provider Provisioned VPN," IETF Internet Draft Provider Provisioned VPN WG, December, 2002.

[8] ITU-T, Recommendation Y.1311,"Network Based VPNs-Generic Architecture and Service Requirements," ITU-T, 2002.

[9] Michael Behringer, "Analysis of the Security of the MPLS Architecture," IETF Internet Draft Provider Provisioned VPN WG, October, 2002.

[10] R. Callon, M. Suzuki, "A Framework for Layer 3 Provider Provisioned Virtual Private Networks," IETF Internet Draft Provider Provisioned VPN WG, October, 2002.

[11] Internet URL, http:www.acm.org/xrds2-4/intrus.html.

[12] Internet URL, http://staff/ashington.edu /gray/papers/credo.html.

[13] ITU-T Recommendation Y.1311-1, "Network Based IP VPN over MPLS architecture," ITU-T, 2001.

[14] Internet URL, http://www.cosinecom.com.

[15] Robert N. Smith, Sourav Bhattacharya, "Firewall Placement In A Large Network Topology," IEEE FTDCS '97, p.40, October, 1997.

[16] Herve Debar, Marc Dacier, "Toward a Taxonomy of Intrusion-Detection Sysetms," IBM R&D, 1998.

[17] Jeremy de Clercq, Cliff Wang, "An Architecture for Provider Provisioned CE-based Virtual Private Networks using IPsec," IETF Internet Draft Provider Provisioned VPN WG, June, 2002.

[18] Eric C. Rosen, "Use of PE-PE IPsec in RFC2547 VPNs," IETF Internet Draft Provider Provisioned VPN WG, August, 2002.

[19] M. Carugi, "Service requirements for Layer 3 Provider Provisioned Virtual Private Networks : ," IETF Internet Draft Provider Provisioned VPN WG, October, 2002.

[20] Samuel Patton, David Doss, William Yurcik, "Distributed weakness in virtual private networks," IEEE LCN '00, p.96, 2000.

[21] Ananth Nagarajan, "Generic Requirements for Provider Provisioned VPN," IETF Internet Draft Provider Provisioned VPN WG, December 2002.

임 형 진

e-mail : hjlim@rtlab.skku.ac.kr
1998년 한림대학교 컴퓨터공학과(학사)
2001년 성균관대학교 정보통신공학과(석사)
2003년 성균관대학교 정보통신공학부 컴퓨터공학과(박사과정)
관심분야 : 네트워크 관리, 네트워크 보안, 시스템 보안

김 태 경

e-mail : tkkim@rtlab.skku.ac.kr
1997년 단국대학교 수학교육(학사)
2001년 성균관대학교 정보통신공학(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 성균관대학교 정보통신공학부 부교수
관심분야 : 실시간시스템, 네트워크 관리, 네트워크 보안, 시스템 보안, GRID 네트워크, 전자상거래