백본 링크상에서의 네트워크 공격 트래픽 특성 분석†

아주대학교 노병희* · 유승화*

1. 서 론

인터넷의 급속한 확대와 고속 네트워킹 기술의 발전에 따라, 다양하고 유용한 응용들이 인터넷을 통하여 제공되는 것이 가능해지고 있다. 그러나 인터넷은 네트워크간, 사용자간의 연결을 최대한으로 제공하기 위한 목적으로 개발되고 있으므로, 근본적으로 악의적인 네트워크 공격에 취약성을 갖고 있다. 이들 악의적인 네트워크 공격들은 개별 서버들뿐만 아니라 인터넷 기반 구조에 장애를 일으키는 것을 목적으로 한다.

인터넷은 최대한의 연결 제공을 위하여 인터넷을 구성하는 다양한 요소들 상호간의 개방성을 요구하므로, 인터넷 기반구조에 대한 공격은 매우 큰 영향을 미치게 된다. Chakrabarti 등은 다양한 네트워크 공격을 이들의 공격 행태에 따라 분류하고, 이에 대응하는 방법론들을 정리하였다[1]. 이들 네트워크 공격에 대응하기 위한 방법론들의 대다수는 개별 망 단위에서의 네트워크 공격에 대응하기 위한 것들이다. 그러나, 분산형의 글로벌한 네트워크 공격들은 이 공격이 목표물에 도달하여 퍼지기 전에 백본망에서 우선적으로 형태가 드러나게 될 것이므로, 개별 망 단위에서 대응하는 것보다는 백본망 단위에서 대응하는 것이 더 효과적일 수가 있다. Kim 등은 백본 링크에서 실시간으로 네트워크 공격들을 찾아내기 위한 방법을 제안하고 있다[2]. 이와 같은 네트워크 공격에 대한 많은 연구들은 의심스러운 패킷들을 분류하고 필터링하는 방법론에 초점이 맞추어지고 있다.

본 논문에서는, 이러한 기존 방법들의 관점에서와 달리 네트워크 공격을 트래픽 분석의 관점에서 다룬다. 즉, 네트워크 공격 트래픽들이 백본 링크에서 나타나게 되는 특징을 분석하고, 이들 네트워크 공격 트래픽이 정상적인 트래픽 흐름에 어떠한 영향을 미치는지를 분석한다. 이를 위하여 한국과 미국을 연결하는 백본 라우터의 한 링크상에서 패킷들을 캡쳐하여, 이 캡쳐한 데이터에 [2]에서 제안된 방법을 적용하여 네트워크 공격 트래픽을 분류해 내었다. 여기에서는 백본 네트워크 공격 방법으로서 서비스 거부(denial of service, DoS), 호스트스캔(hostscan), 포트스캔(portscan)을 고려한다.

본 논문의 2장에서는 본 논문에서 고려하는 네트워크 공격 형태에 대하여 간단히 살펴보고, 3장에서는 네트워크 공격 트래픽과 정상적인 트래픽들의 개별적인 특성을 살펴보고, 네트워크 공격 트래픽이 정상적인 트래픽 특성에 어떠한 영향을 미치는지를 보인다. 제 4장에서는 결론을 맺는다.

2. 네트워크 공격 형태

여기에서는 본 논문에서 대상으로 하는 네트워크 공격 트래픽의 형태에 대하여 간략히 살펴본다. 네트워크 공격 형태로는 source-spoofed DoS, hostscan, portscan을 대상으로 한다.

최근의 가장 보편적인 DoS 공격 형태는 많은 패킷들을 보내어 목표나 망의 프로세싱과 대역폭 자원을 과도하게 소모시킴으로써 서비스를 불가하게 만드는 패킷 플러딩 공격이다[3]. 공격 도구들은 이러한 패킷 플러딩을 유발시키기 위하여 패킷들의 다음과 같은 속성들을 변조한다: 발신지 IP 주소, 발신지와 목적지 포트 번호, 그리고 기타 IP 헤더 필드들. 일반적으로 발신지 IP 주소는 공격 패킷 스트림의 발신지를 숨기기 위하여 변조되며, 발신지와 목적지 포

† 감사의 글 : 본 논문을 위하여 네트워크 공격 트래픽 검출 프로그램을 제공하여 준 고려대학교 김효곤 교수님께 감사드립니다.

* 종신회원

트번호는 서비스에 의하여 필터링 되는 것을 어렵게 하도록 하기 위하여 변조된다.

패킷 플러딩 공격들은 이러한 변조된 패킷 속성들을 갖는 플로우들로서 구분되는데, 이러한 플로우 구분을 위하여 [2]에서는 <발신지 IP 주소, 목적지 IP 주소, 목적지 포트>의 3개의 파라메터로 구성되는 플로우(flow)를 정의하고 있다. 이러한 플로우의 정의에 따른 본 논문에서 고려하는 네트워크 공격 트래픽의 성질은 다음과 같다.

Source-spoffed DoS 공격은 목적지의 포트 번호가 고정된 경우(fdos)와 이 포트 번호가 변하는 경우(vdos)의 두 종류로 세분된다. 이들의 기본적인 특징은 다음과 같다. 우선, fdos는 목적지 IP 주소와 목적지 포트 번호는 고정되나 발신지 IP는 변하는 형태이다. 이에 반하여, vdos는 목적지 IP 주소는 고정되나, 발신지 IP 주소와 목적지 포트 번호는 변화한다. Hostscan은 발신지 IP 주소와 발신지 포트 번호는 고정되고 목적지 IP만 변화하는 형태이다. 그리고, portscan은 목적지 포트 번호만이 변화하고, 발신지 IP 주소와 목적지 IP 주소는 변하지 않는다. 이를 표 1에 정리하였다.

표 1 네트워크 공격 특징

tuple / attacks	source IP	destination IP	destination Port
vdos	varied	fixed	varied
fdos	varied	fixed	fixed
hostscan	fixed	varied	fixed
portscan	fixed	fixed	fixed

3. 네트워크 공격 트래픽 특성

여기에서는 앞장에서 서술한 네트워크 공격들에 대한 트래픽 특성에 대하여 기술한다. 네트워크 공격 트래픽의 특성 분석을 위하여, 우선적으로 미국과 한국을 연결하는 T-3 인터넷 백본 링크상에서 패킷을 캡쳐하였고, 이들 캡쳐된 데이터를 Kim 등이 제안한 방법[2]을 적용하여 네트워크 공격 패킷들을 구분하였다.

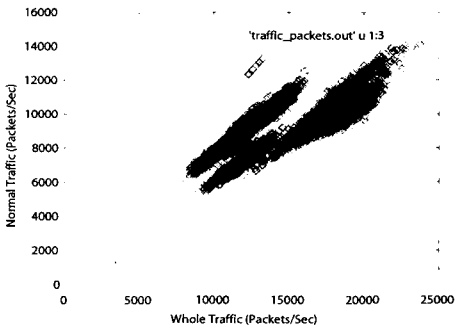
3.1 전체 특성

캡쳐는 2001년 12월 18일 오전 11시부터 5시간 동안 수행되었으며, 캡쳐된 패킷중 하나의 백본 링크로 유입되는 패킷들을 대상으로 분석하였다. 캡쳐된 패킷의 수는 약 2.1x108 정도이고, 이들의 거의 99% 대부분이 IP를 사용하였고, 이들 IP 패킷들 중에서 95%이상이 트랜스포트 프로토콜로서 TCP와 UDP를 사용하였으며 TCP와 UDP의 비율은 9:1 정도였다. TCP 패킷들중에서 40% 정도가 네트워크 공격으로 분류되었으며, UDP 패킷들중에서는 13% 정도가 네트워크 공격으로 분류되었다. 네트워크 공격으로 분류된 패킷들중에서 44% 정도는 vdos, 39%는 hostscan, 9%는 portscan, 8%는 fdos를 사용한 것으로 분석되었다.

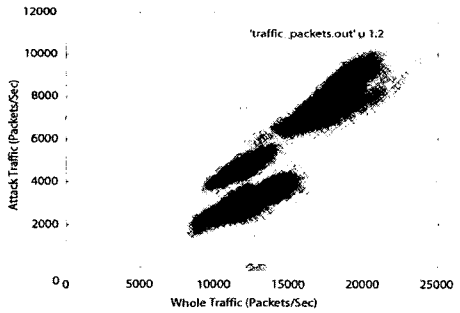
3.2 발생 패킷수와 트래픽 크기 특성

네트워크 공격 패킷들이 백본 링크상의 트래픽 특성에 어떠한 영향을 주는지를 분석하기 위하여, 네트워크 공격 패킷들로만 이루어진 공격 트래픽(attack traffic), 정상적인 패킷들로만 이루어진 정상 트래픽(normal traffic), 그리고 이들이 모두 합쳐진 전체 트래픽(whole traffic)의 유형으로 구분하여 1초의 시간 간격 동안 발생된 패킷수와 이들 패킷들의 총 바이트 크기인 트래픽 크기를 구하였다.

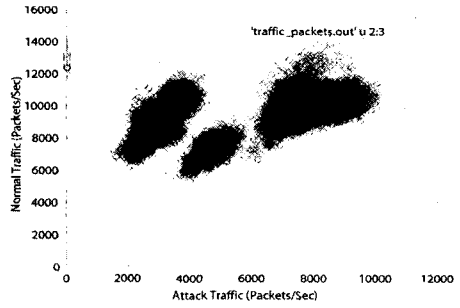
그림 1은 같은 시간(초) 동안 발생한 패킷수를 트래픽 유형별로 비교하여 나타내었다. 그림 1 (a)와 (b)에서 볼수 있듯이 전체 트래픽의 발생 패킷수는 정상 트래픽의 발생 패킷수 뿐만 아니라, 공격 트래픽의 발생 패킷수와 비례 관계를 갖는다. 즉, 정상 트래픽과 공격 트래픽에 의한 발생 패킷의 증가는 전체 트래픽의 발생 패킷의 증가에 가시적으로 반영되어 나타난다. 반면에, 그림 1 (c)에서 보듯이 정상 트래픽의 발생 패킷수와 공격 트래픽의 발생 패킷수는 연관 관계가 없다.



(a) 전체 트래픽 대 정상 트래픽



(b) 전체 트래픽 대 공격 트래픽



(c) 공격 트래픽 대 정상 트래픽

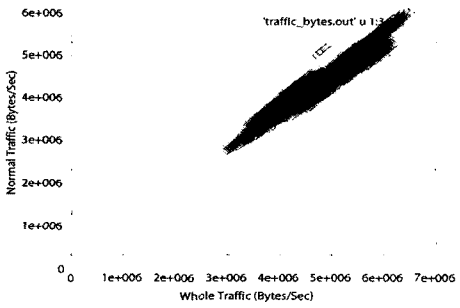
그림 1 발생 패킷수 상관관계

그림 2는 같은 시간(초) 동안 발생한 트래픽 크기(바이트 수)를 트래픽 유형별로 비교한 것이다. 그림 2 (a)에서 보듯이 전체 트래픽 크기는 정상 트래픽의 크기와 비례관계를 갖는다. 반면에 공격 트래픽의 크기는 전체 트래픽 크기와 정상 트래픽의 크기와 특별한 상관관계를 갖지 않음을 알 수 있다. 그림 1과 그림 2에서 볼수 있듯이, 공격 트래픽의 발생 패킷수는 전체 트래픽에서 가시적으로 보일정도로 나타나지만, 트래픽 크기 측면에서는 정상 트래픽에 비하여 상대적으로 매우 작은 크기를 보이게 되어 가시적인 영향을 미치지는 않는 것으로 보인다. 이것은 다음절에서의 개별 패킷의 특성에 의하여 설명이 가능해진다.

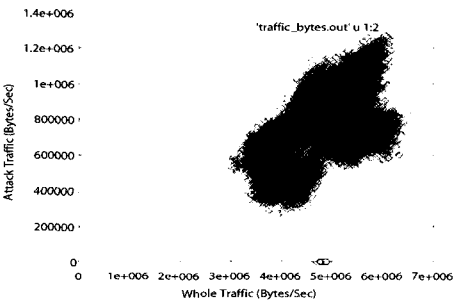
3.3 개별 패킷에 대한 통계 특성

앞에서는 유형별로 합쳐진 트래픽에 대한 특성을 보았고, 여기에서는 유형별로 개별 패킷들에 대한 통계 특성을 보인다.

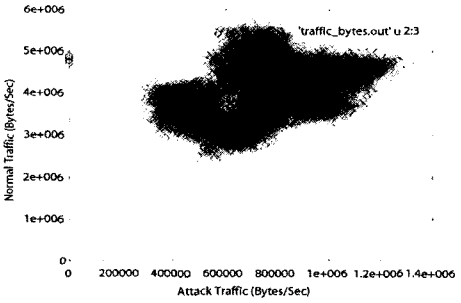
그림 3 (a)는 트래픽 유형별 각 패킷 크기에 대한 누적 확률 분포를 보여준다. 공격 트래픽 패킷들은



(a) 전체 트래픽 대 정상 트래픽



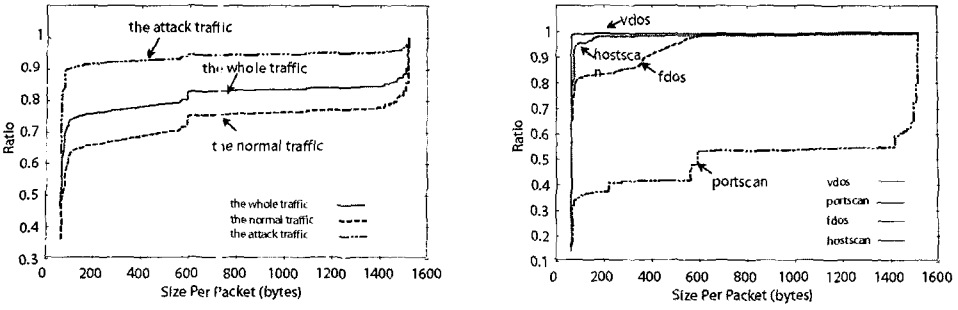
(b) 전체 트래픽 대 공격 트래픽



(c) 공격 트래픽 대 정상 트래픽

그림 2 발생 트래픽 크기 상관관계

정상 트래픽 패킷들에 비하여 매우 작은 크기의 패킷들을 사용하고 있음을 볼수 있다. 실제로, 90% 이상의 공격 트래픽 패킷들은 80 바이트 이하의 크기를 갖는 것으로 분석되었다. 이에 반하여 정상 트래픽 패킷들은 70 바이트 이하, 590 바이트 근처, 그리고 1450 바이트 이상에서 많은 비율을 차지하며 나머지 크기에는 일정한 수준을 유지하며 산재되어 있다. 그림 3 (b)는 공격 트래픽의 각 형태에 대한 패킷 크기의 누적 확률 분포를 보여준다. 그림 3 (b)에서 볼수



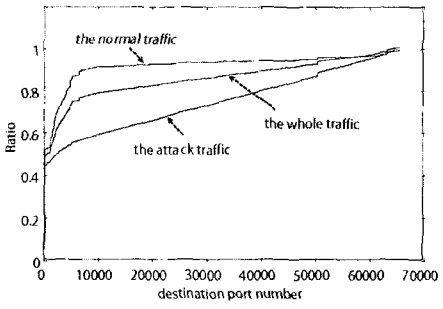
(a) 트래픽 유형별 (b) 공격 유형별

그림 3 패킷 크기에 대한 누적 확률 분포

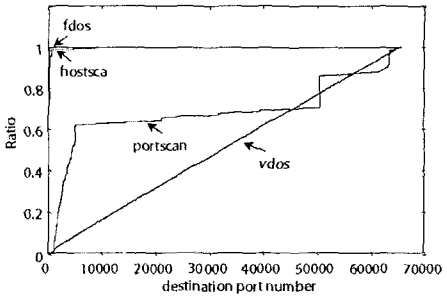
있듯이, vdos의 98% 이상은 60 바이트 크기의 패킷들을 사용하고 있으며, hostscan은 95% 이상이 100 바이트 이하 크기의 패킷들을 사용하고 있다. fdos의 경우는 vdos와 hostscan 보다는 다소 큰 크기의 패킷들을 사용하고는 있으나, 대체적으로 작은 크기의 패킷들을 사용하고 있다. 반면에, portscan은 1500 바이트 크기까지의 다양한 크기의 패킷들을 사용하고 있다.

그림 4 (a)는 트래픽 유형별 패킷들의 목적지 포트 번호 사용 빈도에 대한 누적 확률 분포를 보여준다. 정상 트래픽은 대체적으로 1024 이하의 well-known 포트 번호 사용이 많으며, 특히 80번(HTTP)이 48%, 53번(DNS)이 8%, 25번 (SMTP)이 5%로 사용 빈도가 많았다. 공격 트래픽은 전체적으로 80번이 30%, DNS가 8%, SMTP가 0.9%의 사용 빈도를 보여주었으나, 대체적으로 전 포트 번호 영역에 산재되는 특징을 보여준다. 이를 좀더 자세히 보기 위하여, 각 공격 유형별 포트 번호 사용 빈도를 그림 4 (b)에 나타내었다. vdos 공격은 전 포트 번호 영역을 균등하게 사용하고 있으며, fdos와 hostscan은 특정 포트 번호에 집중되는 특징을 보여준다. 특히, fdos의 경우에는 87% 이상이 포트 번호 80을 사용하는 웹 서버들을 대상으로 하고 있으며, hostscan의 경우에는 포트 번호 80이 63%, 포트 번호 53이 7%, 포트번호 111이 20%의 사용을 보이고 있다. portscan은 일부 큰 포트 번호 부근의 사용이 있으나 5000번 까지에서 균등한 사용 빈도를 보여준다.

3.4 자기유사(Self-Similar) 특성



(a) 트래픽 유형별



(b) 공격 유형별

그림 4 목적지 포트 사용 빈도에 대한 누적 확률 분포

이더넷 트래픽은 자기유사(self-similar) 성질을 갖고 있음이 알려져 있다[4]. 자기유사 성질은 소스 트래픽 모델링 뿐만 아니라 네트워크 혼잡 제어 방식의 개발에 큰 영향을 준다. 자기유사 성질은 Hurst 파라메터로서 표현되며, Hurst 파라메터가 클수록

자기유사 성질이 더 커진다. 일반적으로 husrt 파라메터가 큰 트래픽은 평균 비트율, 네트워크 부하의 동일한 환경에서 링크 이용율, 소통율, 손실율 등과 같은 네트워크 성능에 더 큰 영향을 미치게 된다[5]. 이러한 자기유사 특성이 네트워크 공격 트래픽에 의하여 어떠한 영향을 미치는지를 보이기 위하여 variance-time-plot (VTP) 방법[4]을 사용하여 Hurst 파라메터를 계산하였다.

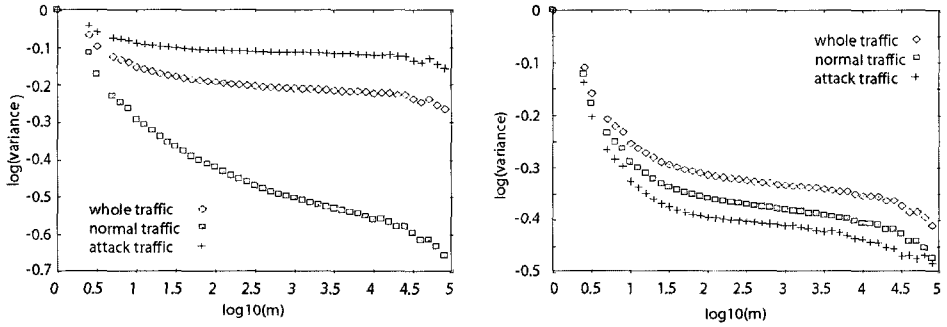
그림 5와 그림 6은 각각 트래픽 유형과 공격 유형에 따른 VTP를 보여준다. 이들 VTP에 의하여 계산된 Hurst 파라메터들을 표 2에 나타내었다. 이들로부터, 공격 트래픽이 정상 트래픽보다 더 큰 자기유사 성질을 갖음을 알수 있다. 또한, 전체 트래픽의 자기유사성은 공격 트래픽의 추가에 의하여 증가됨을 알 수 있다. 이것은 공격 트래픽의 증가는 단순히 네트워크에 흐르는 트래픽의 양만을 증가시키는 것이 아니라, 자기 유사성을 크게 만들어 동일한 수준의 네트워크 부하에 대하여도 네트워크에 더 심각하게 영향을 미칠 수 있음을 의미한다. 따라서, 공격 트래픽의 증가는 해당 목표에 대한 피해 뿐만 아니라, 전체적인 네트워크의 성능에 직접적인 피해를 가중시키게 된다.

표 2 Hurst 파라메터

	발생 패킷수	발생 트래픽 크기
전체 트래픽	0.990	0.985
정상 트래픽	0.966	0.982
공격 트래픽	0.993	0.984
vdos	0.994	0.995
fdos	0.930	0.933
portscan	0.919	0.950
hostscan	0.976	0.968

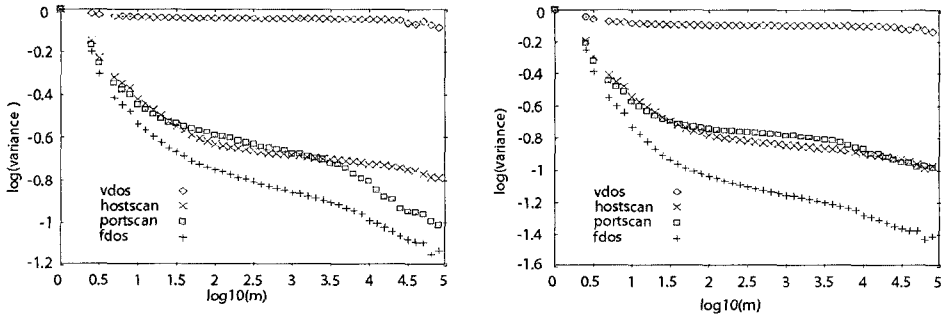
4. 결 론

본 논문에서는, 백본 링크에서의 네트워크 공격의 특성을 트래픽 분석의 관점에서 살펴보았다. 즉, 네



(a) 전체 트래픽 대 정상 트래픽 (b) 발생 트래픽 크기

그림 5 트래픽 유형별 자기유사 특성



(a) 전체 트래픽 대 공격 트래픽 (b) 발생 트래픽 크기

그림 6 공격 유형별 자기유사 특성

트워크 공격이 백본 링크상에서 어떠한 형태로 나타나는지와, 이들이 정상적인 트래픽 특성에 어떠한 영향을 미치는지를 조사하였다. 많은 통계적인 관점에서 네트워크 공격 트래픽은 정상 트래픽의 특성과 다른 특성을 갖으며, 전체 트래픽의 특성을 변화시킬 정도로 영향을 줌을 보였다.

앞으로 네트워크 공격의 형태는 더 다양하여지고, 더 증대하여 질 것으로 예측된다. 따라서, 기존의 정상 트래픽을 대상으로 설계된 네트워크 구조에 심대한 영향을 줄 것으로 예상되며, 이에 따른 새로운 네트워크 모델의 개발이 필요할 것으로 판단되어진다. 또한, 네트워크 공격의 징후를 감지하는 것은 매우 어려운 작업이고, 많은 컴퓨팅 자원을 요구한다. 이것은 대부분의 공격 징후 검출 방법들이 개별 플로우 단위로 감시를 수행하기 때문인 것으로 생각되어진다. 반면에, 개별 플로우 단위가 아니고 이들이 결합된 트래픽 영역에서 이러한 작업을 수행할수 있다면, 복잡성과 자원 요구량은 매우 줄어들수 있을 것으로 생각된다. 이것은 이러한 전체 트래픽 영역에서의 감시는 망 관리를 위하여 현재도 이루어지고 있기 때문이다. 이와 같은 네트워크 공격의 징후를 전체 트래픽 관점에서 찾아내는 구체적인 방법론은 더 연구가 되어야 할 것이다.

참고문헌

[1] A. Chakrabarti and G. Manimaran, Internet Infrastructure Security: A Taxonomy, IEEE Networks, Vol. 16, No. 6, November/December, 2002, pp.13-21

[2] H. Kim, J. Kim, S. Bahk, and I. Kang, Fast Classification, Calibration, and Visualization of Netowrk Attacks on Backbone Links, Technical Report, June, 2003, http://net.korea.ac.kr/papers/RADAR.html

[3] K. Houle and J. Weaver, Trends in Denial of Service Attack Technology, CERT Coordination Center, Oct. 2001

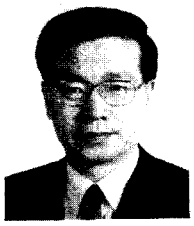
[4] W.E.Leland, M.S.Taqqu, W.Willinger, and D.V. Wilson, On the Self-Similar Nature of Ethernet Traffic (extended version), IEEE/ ACM Tr. on Networkig, Volume 2, No. 1, February, 1994, pp.1-15

[5] W. Stallings, High-Speed Networks and Internets: Performance and Quality of Service, 2ndEd., Prentice Hall, 2001

노 병 희

1987 한양대학교 전자공학과(학사)
1889 한국과학기술원 전기및전자공학과(석사)
1998 한국과학기술원 전기및전자공학과(박사)
2000~현재 아주대학교 정보통신전문대학원 조교수
1989~1994 한국통신 통신망연구소
1998~2000 삼성전자
관심분야 : 멀티미디어 통신, 유/무선 인터넷 응용
E mail : bhroh@ajou.ac.kr

유 승 화



1972 서울대학교 공과대학 응용수학과(학사)
1980 University of Kansas Computer Science(석사)
1983 University of Kansas Computer Science(박사)
1983~1988 AT&T Bell Labs
1989~1999 삼성전자 전무
1997~1998 한국정보과학회 부회장
1998~1999 한국 네트워크 연구조합 이사장
1999~현재 아주대학교 정보통신전문대학원 교수
관심분야 : 유/무선 인터넷, ENUM, 유비쿼터스 통신, RFID 네트워크
E mail : swyoo@ajou.ac.kr