IPv6 기반 트래픽 분석 도구 설계

Design of IPv6 Based Traffic Analysis Tool

김선영*, 이홍규*, 오승희**, 서동일**, 오창석***
충북대학교 컴퓨터공학과*, 한국전자통신연구원**, 충북대학교 전기전자컴퓨터공학부***

Sun-Young Kim(sykim@nwork.chungbuk.ac.kr)*, Hong-Kyu Lee(hklee@nwork.chungbuk.ac.kr)*
Seung-Hee Oh(seunghee@etri.re.kr)** Dong-Il Seo(bluesea@etri.re.kr)**
Chang-Suk Oh(csoh@nwork.chungbuk.ac.kr)***

요약

현재의 인터넷 환경에서는 트래픽 폭주 공격, 웜 공격 등으로 인해 많은 경제적 손실이 발생하고 있으며 이러한 문제들은 향후 IP 주소의 고갈로 인해 IPv6로 대체되었을 경우 더욱 심각해질 것이다. 따라서, 본 논문에서는 IPv6 환경에서 발생할 수 있는 공격을 예상하여 이러한 공격을 탐지할 수 있는 트래픽 분석 도구를 설계하고 구현하였다. 제안한 트래픽 분석 도구는 패킷 생성 모듈, 패킷 수집 모듈, 판별 모듈, X 윈도우 기반 디스플레이 모듈로 구성되며, 실험 결과, IPv6 환경에서 DAD-NA 메시지 공격, TCP SYN 플러딩 공격, UDP 플러딩 공격, ICMP 플러딩 공격 등을 효과적으로 검출할 수 있었다.

■ 중심어 : | IPv6 | 트래픽 분석 | 트래픽 폭주 공격 |

Abstract

In the present internet environment, various traffic flooding attacks and worm attacks cause economical loss. If IPv4 is substituted by IPv6 because of the lack of IP address, it will be more serious. Therefore, we design and implement the traffic analysis tool which can detect attacks by expecting them encountered in the IPv6 environment . Proposed tool is composed of packet generation module, packet gathering module, discrimination module, and display module in X-windows. As a simulation result, it is proved that it can effectively detect DAD-NA message attack, TCP SYN flooding attack, UDP flooding attack and ICMP flooding attack in the IPv6 environment.

■ keyword : | IPv6 | Traffic Analysis | Traffic Flooding Attack |

I. 서 론

인터넷 사용자가 급격히 증가하면서 IP 주소를 확보하는 것이 매우 어려워지고 있다. 현재의 인터넷에서는 32비트의 주소 체계를 사용하고 있지만 IP 주소를 체계적으로 할당하지 못하였기 때문에 실제로는 5억대 정도의 컴퓨터만 공인된 IP 주소로써 인터넷에 연결될 수 있다. 향후 휴대용 단말기를 이용한 무선 인터넷 사용자가 증가하고 홈 네트워킹과 인터넷의 결합으로 인해 IP 주소 문제는 더욱 심각해질 것이다[1]. 이러한 IP 주소

* 본 연구는 한국전자통신연구원 연구과제로 수행되었습니다.
접수번호 : #041127-001
접수일자 : 2004년 11월 27일
심사완료일 : 2005년 01월 25일
교신저자 : 김선영, e-mail : sykim@nwork.chungbuk.ac.kr

고갈 문제를 해결하기 위해 128비트의 주소 체계를 사용하는 IPv6의 도입이 시급한 실정이다. IPv6는 무한한 주소 공간, 주소 자동 설정, QoS 보장 등 많은 장점이 있으나 IPv4와 다른 IPv6 헤더를 사용할 뿐 기존의 TCP와 ICMP는 대부분 그대로 사용하기 때문에 보안상의 취약점도 있다. 그러므로 현재의 인터넷에서 극성을 부리고 있는 트래픽 폭주 공격이 IPv6 환경에서는 보다 더 위협적인 형태로 나타날 가능성이 매우 높다[2]. 따라서, 본 논문에서는 DAD(Duplicate Address Detection) -NA 메시지 공격, TCP SYN 플러딩 공격, UDP 플러딩 공격, ICMP 플러딩 공격 등 IPv6 환경에서 출현할 것으로 예상되는 다양한 공격 시나리오를 설정하고 이러한 공격을 탐지할 수 있는 IPv6 기반의 트래픽 분석 알고리즘을 제안하였다.

II. IPv6 환경에서의 트래픽 폭주 공격

IPv6에서는 호스트가 자신의 MAC 주소와 라우터의 프리픽스를 이용하여 [그림 1]과 같이 IPv6 주소를 자동 생성할 수 있다[3].

1단계 : 라우터로부터 서브넷 프리픽스를 얻음
서브넷 프리픽스 : 12AB:0:0:CD30::/64
2단계 : MAC 주소를 이용하여 64비트의 인터페이스 ID를 생성 00:40:2B:0E:0A:AD →
0240:2BFF:FE0E:0AAD
3단계 : 서브넷 프리픽스와 인터페이스 ID를 결합하여 IPv6 주소 생성
IPv6주소 :
12AB:0:0:CD30:0240:2BFF:FE0E:0AAD/64

그러므로, 주소를 수동 설정하거나 MAC 주소의 중복 또는 라우터 정책에 따른 주소 자동 설정 알고리즘에 의해 IPv6 주소가 충돌할 가능성이 있다.

따라서, 비상태형 주소 자동 설정 방법에서는 DAD를 이용하여 동일한 네트워크 상에 있는 호스트의 주소 충돌 여부를 검사한다[4]. DAD-NA 메시지 공격은 다음과 같다. 우선 공격자는 공격 목표가 되는 라우터의 내부에 에이전트를 설치한다. 에이전트는 NS, NA메시지를 이용하여 동일한 네트워크 상에 있는 호스트들의 주소들을 수집한다. 에이전트는 수집한 주소들의 테이블을 가지고 있으므로 공격자가 공격 명령을 내리면 테이블에 있는 주소를 목적지 주소와 근원지 주소에 동일하게 넣고 NA 메시지를 보낸다. 이렇게 되면 그 주소를 가지고 있는 호스트는 같은 주소에 의해 NA를 받았으므로 주소 충돌이라고 인식하게 된다[5]. 주소 충돌을 감지한 호스트는 주소 자동 재설정을 실행하는데 이때 라우터와 RA, RS 메시지를 이용해 네트워크의 프리픽스 및 기타 주소 설정에 필요한 정보를 가져와 새로 주소를 설정하게 된다[6]. 만약 라우터 내부에 있는 호스트의 주소가 많으면 많을수록 동시 다발적으로 발생하는 RS, RA 메시지가 많아지게 되어 결국 라우터의 성능이 저하된다[7]. [그림 2]는 DAD-NA 메시지 공격에 사용되는 헤더 포맷이다.

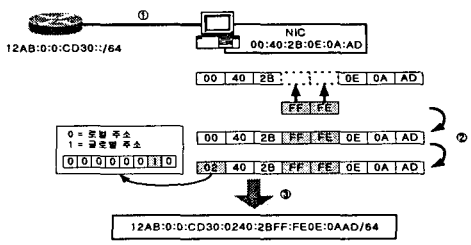


그림 1. IPv6 주소 자동 설정

version(6)	Traffic Class(0)	Flow Label(0)	
Payload Length		NextHeader(58)	HopLimit(255)
Source Address			
Destination Address			
Type(136)	Code(0)	Checksum	
R S O 0 1	Reserved		
Target link-later Address			

그림 2. DAD-NA 메시지 공격의 헤더

TCP SYN 플러딩 공격은 TCP 연결 설정의 취약점을 이용한 공격으로서 악의적인 공격자가 요청(SYN)을 하고 응답(SYN+ACK)을 받은 후 ACK를 보내지 않는 형태의 공격이다. 호스트는 응답이 올 것을 기대하고 반 오픈 상태가 되어 대기 상태에 머무른 후 일정시

간(75초) 후에 다음 요청이 오지 않으면 해당 연결을 초기화하게 된다[8]. 이와 같이 지속적인 연결 요청을 수행한 후 다음 요청을 수락하였을 때 확인 메시지를 보내지 않는다면 시스템에서 초기화 전까지 메모리 공간인 백로그 큐에 계속 쌓이게 된다. 따라서 초기화하기 전에 계속적으로 새로운 요청이 오게 되면 백로그 큐가 꽉 차게 되어 더 이상의 연결을 받아들일 수 없는 서비스 거부 상태가 된다. TCP SYN 플러딩 공격은 Next Header의 값을 6으로 설정한 후 근원지 주소를 위조하고, TCP 헤더의 플랙 필드에서 SYN 비트를 1로 세팅하여 지속적으로 전송하면 목표 시스템은 과부하로 인해 정상적인 서비스를 제공할 수 없게 된다[9]. [그림 3]은 TCP SYN 플러딩 공격에 사용되는 헤더이다.

<table>
<tr><td colspan="2">version(6)</td><td colspan="2">Traffic Class(0)</td><td colspan="3">Flow Label(0)</td></tr>
<tr><td colspan="4">Payload Length</td><td colspan="2">NextHeader(58)</td><td>HopLimit(255)</td></tr>
<tr><td colspan="7">Source Address</td></tr>
<tr><td colspan="7">Destination Address</td></tr>
<tr><td colspan="4">Source port</td><td colspan="3">Destination port</td></tr>
<tr><td colspan="7">순서번호</td></tr>
<tr><td colspan="7">확인번호</td></tr>
<tr><td>헤더 길이</td><td colspan="2">예약</td><td>1</td><td></td><td></td><td>확인번호</td></tr>
<tr><td colspan="4">확인번호</td><td colspan="3">확인번호</td></tr>
</table>

그림 3. TCP SYN 플러딩 공격의 헤더

UDP 플러딩 공격은 목적지의 포트번호 필드를 7, 31335, 19 등 특정 포트 번호로 세팅하고 서브넷의 브로드캐스트 주소값을 목적지 주소로 하여 전송하는 형태의 공격이다. [그림 4]는 UDP 플러딩 공격에 사용 되는 헤더이다.

<table>
<tr><td colspan="2">version(6)</td><td colspan="2">Traffic Class(0)</td><td colspan="3">Flow Label(0)</td></tr>
<tr><td colspan="4">Payload Length</td><td colspan="2">NextHeader(17)</td><td>HopLimit(255)</td></tr>
<tr><td colspan="7">Source Address</td></tr>
<tr><td colspan="7">Destination Address</td></tr>
<tr><td colspan="4">Source port</td><td colspan="3">Destination port
(31335,7,19)</td></tr>
<tr><td colspan="4">체크섬</td><td colspan="3">긴급포인터</td></tr>
</table>

그림 4. UDP 플러딩 공격의 헤더

ICMP 플러딩 공격은 echo request 메시지를 보내서 목표 시스템을 정지시키는 공격으로 수법이 매우 간단하며, 목표 시스템에 대해 IP 주소 이외에는 어떠한 정보도알 필요가 없다. 또한 ICMP 요청 메시지를 브로드캐스트 주소로 보내게 되면 모든 시스템이 echo reply 메시지를 근원지 주소로 보내게 되어 시스템이 다운되는 공격이다. [그림 5]는 ICMP 플러딩 공격에 사용되는 헤더이다.

<table>
<tr><td colspan="2">version(6)</td><td colspan="2">Traffic Class(0)</td><td colspan="3">Flow Label(0)</td></tr>
<tr><td colspan="4">Payload Length</td><td colspan="2">NextHeader(58)</td><td>HopLimit(255)</td></tr>
<tr><td colspan="7">Source Address</td></tr>
<tr><td colspan="7">Destination Address</td></tr>
<tr><td colspan="2">Type(128)</td><td colspan="2">Code(0)</td><td colspan="3">Checksum</td></tr>
<tr><td colspan="7">Reserved</td></tr>
<tr><td colspan="7">Target link-later Address</td></tr>
</table>

그림 5. ICMP 플러딩 공격의 헤더

III. IPv6 기반 트래픽 분석 도구 설계

본 논문에서 제안한 IPv6 기반 트래픽 분석 도구는 다음과 같은 기능을 하며, 이를 [그림 6]에 도시하였다.

- 공격자가 IPv6 환경에서 예상 가능한 유해 트래픽을 전송.
- 패킷이 경유하는 라우터에서 트래픽을 수집.
- 헤더 정보를 분석하여 추정 공격 시나리오와 비교.
- 추정 공격과 같으면 2차 판별.
- 공격으로 판별되면 경고 메시지를 콘솔에 보내고, 근원지 주소를 차단.

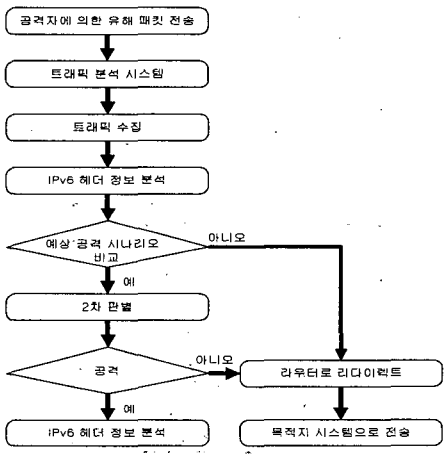


그림 6. IPv6 기반 트래픽 분석 도구의 흐름도

제안한 트래픽 분석 도구는 패킷 생성 모듈, 패킷 수집모듈, 판별 모듈, X 윈도우 기반 디스플레이 모듈로 구성되어 있다. 패킷 생성 모듈은 2장에서 기술한 헤더를 갖는 공격 패킷을 생성하여 전송하는 공격자 역할의 모듈이며, 임의의 패킷을 생성하여 목표 시스템으로 유해 트래픽을 전송하는 기능을 수행한다. [그림 7]은 패킷 생성 모듈의 흐름도이다.

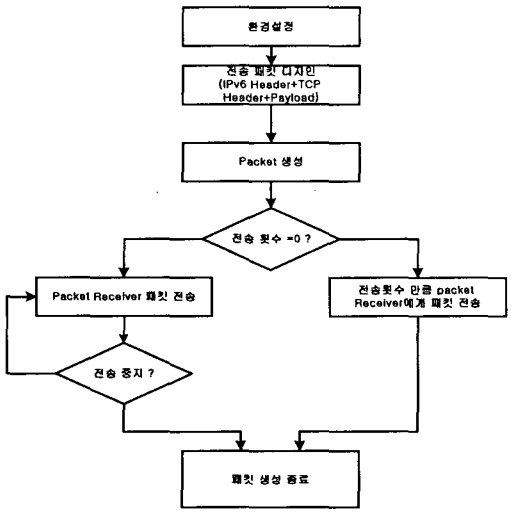


그림 7. 패킷 생성 모듈의 흐름도

패킷 수집 모듈은 패킷 생성 모듈로부터 전송된 패킷 및 지나가는 모든 패킷을 수집한다. 패킷 수집 모듈은 패킷을 수집하기 위한 환경 설정 및 패킷 필터링을 위한 설정 후 패킷 수신을 대기한다. 패킷 수집 모듈은 대기 모드에 있다가 패킷이 수집되면 수집된 패킷의 시간, 프로토콜, 근원지 IP 주소, 목적지 IP 주소, 필드값을 구분하여 저장한다. [그림 8]은 패킷 수집 모듈의 흐름도이다.

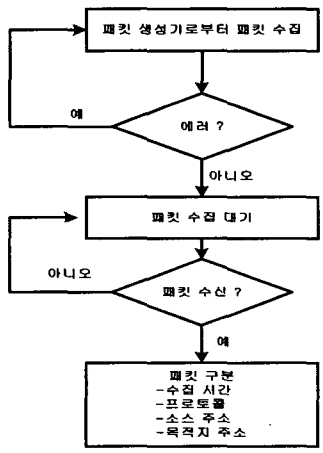


그림 8. 패킷 수집 모듈의 흐름도

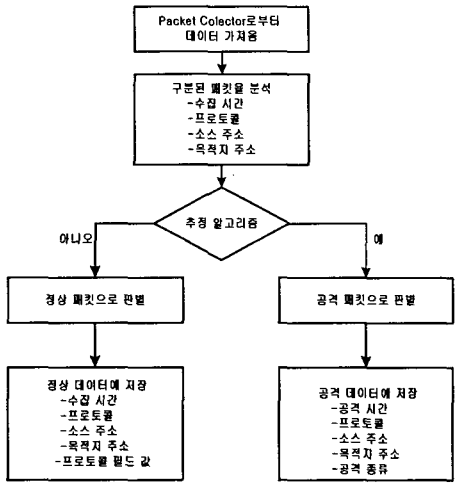


그림 9. 판별 모듈의 흐름도

판별 모듈은 패킷 수집 모듈에 의해 구분된 데이터를 근거로 공격 여부를 판정한다. 추정한 공격들과 비교하여 일치하면 공격으로 간주하고, 일치하지 않으면 다시 한번 패킷을 검사한 후 정상으로 판정한다. 판별 데이터를 정상 패킷과 공격 패킷으로 구분하여 수집 시간, 프로토콜, 공격 유형, 근원지 주소를 저장한다. [그림 9]는 판별 모듈의 흐름도이다.

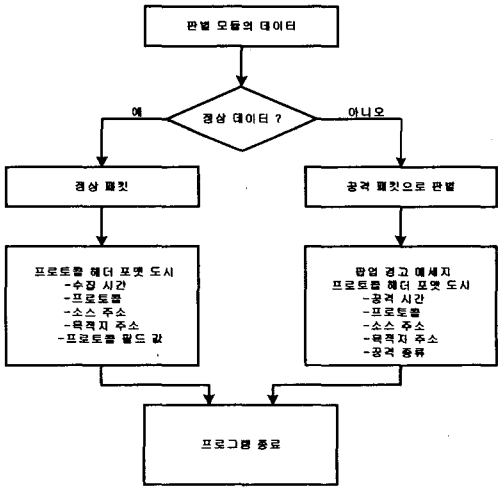


그림 10. X 윈도우 기반 디스플레이 모듈의 흐름도

X 윈도우 기반 디스플레이 모듈은 판별 모듈이 판정한 데이터를 이용하여 리눅스 시스템에서 GUI로 나타내는 모듈이다. 공격이 검출되면 시스템 관리자에게 공격 알람 통보를 하고, 공격 헤더를 화면에 나타내며, 정상 패킷인 경우에는 단순히 프로토콜의 헤더만 나타낸다. [그림 10]은 X 윈도우 기반 디스플레이 모듈의 흐름도이다.

IV. 실험 및 결과 고찰

본 논문에서 제안한 IPv6 기반 트래픽 분석 도구의 성능을 평가하기 위한 실험망은 [그림 11]과 같다. 각 호스트는 정상 패킷과 공격 패킷을 생성하여 목표 시스템으로 전송하며, 라우터에서는 IPv6 기반 트래픽 분석 도구가 실행되어 외부에서 들어오는 패킷과 내부에서 발생되는 패킷을 분석한다[3]. DAD-NA 메시지 공격, TCP 플러딩 공격, UDP 플러딩 공격, ICMP 플러딩 공격을 수행한 다음 공격 검출 능력을 실험하였다.

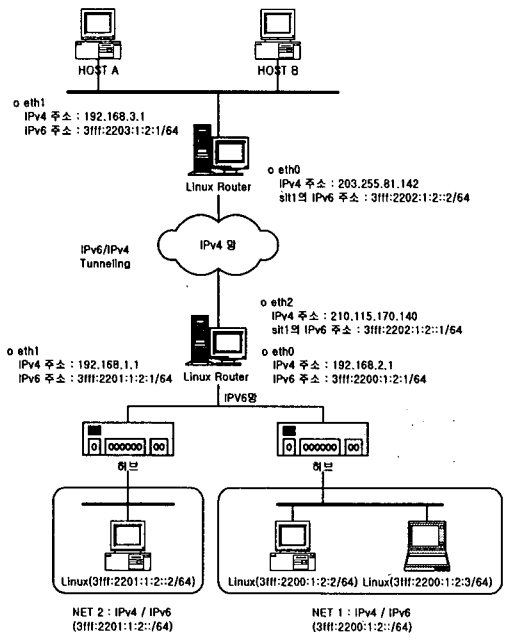
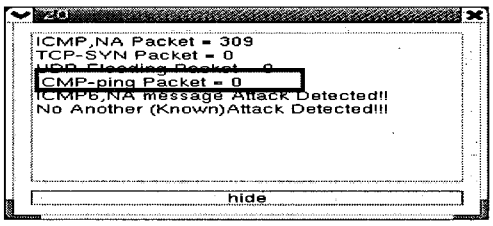


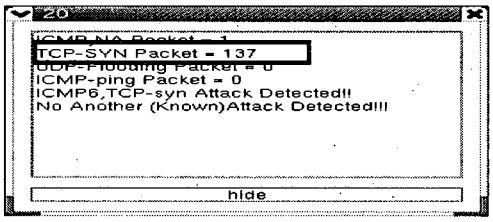
그림 11. 실험망 구성도

DAD-NA 메시지 공격을 수행한 결과, [그림 12(a)]에서 보는 바와 같이 공격을 검출하였다. TCP SYN 플러딩 공격을 수행한 결과, [그림 12(b)]에서 보는 바와 같이 공격을 검출할 수 있었으며, IPv4와 마찬가지로 IPv6 환경에서도 TCP SYN 플러딩 공격이 가능함을 확인하였다. UDP 플러딩 공격도 [그림 12(c)]에서 보는 바와 같이 검출할 수 있었으며, 헤더 정보를 분석하여 특정 포트로 대량의 패킷이 전송되고 있음을 알 수 있었다. ICMP 플러딩 공격은 패킷 생성기로 IPv4 환경에서 사용되고 있는 ping을 사용하였다. ICMP 플러딩 공격이 수행한 결과, [그림 12(d)]에서 보는 바와 같이 공격을 검출할 수 있었으며, 트래픽 분석기를 통해 ICMP echo request 메시지가 지속적으로 수신되는 것을 확인할 수 있었다.

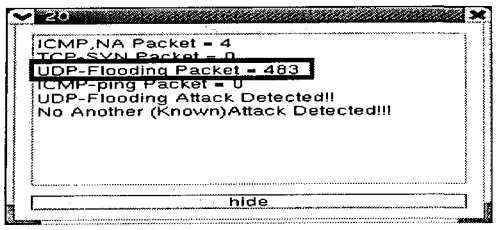
IPv6 환경에서도 한 종류의 트래픽 폭주 공격만 수행되지는 않을 것이다. 본 논문에서도 이러한 상황을 가정하여 여러 형태의 공격 패킷을 생성한 후 목표 시스템을 공격하는 실험을 수행하였다. 실험 결과, 제안한 트래픽 분석 도구로 다양한 공격을 검출할 수 있었다. [그림 13]은 여러 공격이 동시에 수행되었을 때 트래픽 분석 도구가 공격을 검출하고 경고하는 화면이다.



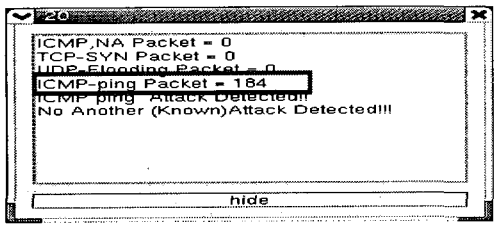
(a) DAD-NA 메시지 공격



(b) TCP SYN 플러딩 공격



(c) UDP 플러딩 공격



(d) ICMP 플러딩 공경

그림 12. 트래픽 폭주 공격 경고 화면

IPv6 환경의 실험에 사용된 가상의 공격들은 TCP와 UDP, ICMP 프로토콜의 버그를 이용한 트래픽 폭주 공격의 일종이며, 현재의 IPv4 환경에서 심각한 피해를 주고 있는 공격이다. 실험 결과, IPv4 환경에서 자행되고 있는 트래픽 폭주 공격들이 IPv6 환경에서도 IPv6 헤더의 단순한 조작만으로 가능할 것으로 판명되었다.

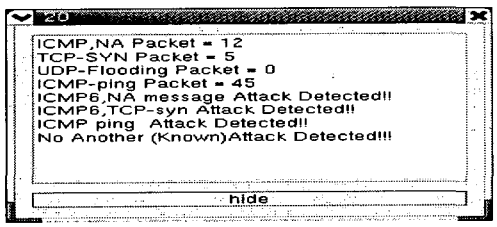


그림 13. 여러 가지 공격이 검출되었을 때의 경고 화면

V. 결 론

본 논문에서는 IPv6 환경에서 유해 트래픽과 정상 트래픽을 분석할 수 있는 트래픽 분석 도구를 설계하였다. 제안한 트래픽 분석 도구를 이용하여 DAD-NA 메시지 공격, TCP SYN 플러딩 공격, UDP 플러딩 공격, ICMP 플러딩 공격 등 다양한 IPv6 기반의 트래픽 폭주 공격을 탐지할 수 있었다. 향후, 보다 많은 공격 탐지 알고리즘을 추가한다면 IPv6 환경에서도 효과적으로 트래픽 폭주 공격을 탐지할 수 있을 것이다.

참 고 문 헌

[1] 오창석, 생동하는 TCP/IP 인터넷, 내하출판사, 2004.

[2] 유대성, 오승희, 김선영, 서동일, 오창석, "SNMP MIB를 이용한 트래픽 분석, 한국통신학회 COMSW2004, pp.113~117. 2004.

[3] 김용진외, 차세대 인터넷 프로토콜 IPv6, 다성출판사, 2002.

[4] 이용락외, IPv6 네트워크구축, 성안당, 2003.

[5] Neighbor Discovery for IPv6, RFC 2461, 1998.

[6] Transition Mechanism for IPv6 Hosts and Routers, RFC 2993, 2003.

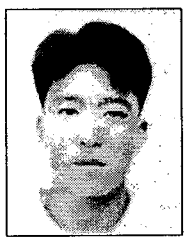
[7] Connection of IPv6 Domains via Clouds, RFC 3056, 2001.

[8] W. Stevens, TCP/IP Illustrated, Addison-Wesley, 1994.

[9] W. Stevens, Unix Network Programming, Prentice Hall, 1999.

저 자 소 개

김 선 영(Sun-Young Kim) 정회원



- 2001년 2월 : 한밭대학교 전자공학과(공학사)
- 2003년 2월 : 충북대학교 컴퓨터공학과(공학석사)
- 2003~현재 : 충북대학교 컴퓨터공학과 박사과정

<관심분야> : 정보보호, 컴퓨터네트워크,

이 홍 규(Hong-Kyu Lee) 준회원

- 2003년 2월 : 충북대학교 컴퓨터공학과(공학사)
- 2003년 8월~현재 : 충북대학교 컴퓨터공학과 석사과정

<관심분야> : 정보보호, 컴퓨터 네트워크

오 승 희(Seung-Hee Oh) 정회원

- 1999년 2월 : 전북대학교 컴퓨터과학과(이학사)
- 2001년 2월 : 이화여자대학교 컴퓨터학과(공학석사)
- 2001년~현재 : 한국전자통신연구원 정보보호연구단 네트워크보안구조연구팀 연구원

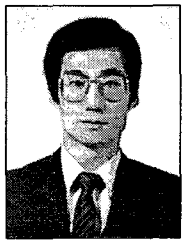
<관심분야> : 정보보호, 차세대 네트워크보안

서 동 일(Dong-Il Seo) 정회원

- 1989년 2월 : 경북대학교 전자공학과(공학사)
- 1994년 2월 : 포항공과대학교 정보통신공학과(공학석사)
- 2000년 3월~2004년 8월 : 충북대학교컴퓨터과학과(이학박사)
- 1994년~현재 : 한국전자통신연구원 정보보호연구단 네트워크보안구조연구팀장

<관심분야> : 인터넷 정보보호, 컴퓨터 통신, 네트워크

오 창 석(Chang-Suk Oh) 종신회원



- 1978년 2월 : 연세대학교 전자공학과(공학사)
- 1980년 2월 : 연세대학교 전자공학과(공학석사)
- 1988년 8월 : 연세대학교 전자공학과(공학박사)
- 1985년~현재 : 충북대학교 전기전자컴퓨터공학부 교수
- 1982년~1984년 : 한국전자통신연구원 연구원
- 1990년~1991년 : Stanford대학교 객원교수