한국시뮬레이션학회 논문지
Vol. 19, No. 4, pp. 151-159 (2010. 12)

패킷 카운팅을 이용한 DoS/DDoS 공격 탐지 알고리즘 및 이를 이용한 시스템

김태원[1] · 정재일[1] · 이주영[2†]

DoS/DDoS attacks Detection Algorithm and System using Packet Counting

Tae-Won Kim · Jae-Il Jung · Joo-Young Lee

ABSTRACT

Currently, by using the Internet, We can do varius things such as Web surfing, email, on-line shopping, stock trading on your home or office. However, as being out of the concept of security from the beginning, it is the big social issues that malicious user intrudes into the system through the network, on purpose to steal personal information or to paralyze system. In addition, network intrusion by ordinary people using network attack tools is bringing about big worries, so that the need for effective and powerful intrusion detection system becomes very important issue in our Internet environment. However, it is very difficult to prevent this attack perfectly. In this paper we proposed the algorithm for the detection of DoS attacks, and developed attack detection tools. Through learning in a normal state on Step 1, we calculate thresholds, the number of packets that are coming to each port, the median and the average utilization of each port on Step 2. And we propose values to determine how to attack detection on Step 3. By programing proposed attack detection algorithm and by testing the results, we can see that the difference between the median of packet mounts for unit interval and the average utilization of each port number is effective in detecting attacks. Also, without the need to look into the network data, we can easily be implemented by only using the number of packets to detect attacks.

Key words : DDoS Detection, IDS, IPS, Packet monitering

요 약

인터넷은 이제 일상생활에서 떼어놓을 수 없는 생활의 일부가 되었다. 그러나 인터넷은 애초에 보안의 개념 없이 만들어졌기 때문에 악의적인 사용자가 네트워크를 통해 시스템에 침투하여 시스템을 마비시키거나 개인정보를 탈취하는 문제들이 커다란 사회적 이슈가 되고 있다. 또한 최근 평범한 일반 사람들도 네트워크 공격 툴 사용으로 인한 DoS 공격이 가능해짐에 따라 인터넷 환경에서 큰 위협을 주고 있다. 그러므로 효율적이고 강력한 공격 탐지 시스템이 인터넷 환경에서 매우 중요하게 되었다. 그러나 이러한 공격을 완벽하게 막아내는 것은 매우 어려운 일이다. 본 논문에서는 DoS 공격의 탐지를 위한 알고리즘을 제안하고, 이를 이용한 공격탐지도구를 제시한다. 먼저 정상상태에서의 학습단계를 거쳐서, 학습된 임계치 허용량, 각 포트로 유입되는 패킷의 개수, 중간값 그리고 각 포트별 평균사용률을 계산하고, 이 값을 바탕으로 공격탐지가 이루어지는 3단계 판별 방법을 제안하였다. 제안한 방법에 맞는 공격 탐지 도구를 제작하여 실험을 하였으며, 그 결과 각 포트별 평균사용률과 단위 시간당 패킷량 중간값의 차이와 학습된 임계치 허용량의 비교는 공격 탐지에 효율적임을 알 수 있다. 또한 네트워크 데이터를 들여다 볼 필요 없이, 패킷의 개수만을 이용하여 공격을 탐지함으로써 간단히 구현할 수 있음을 알 수 있다.

주요어 : DDoS 공격탐지, 공격탐지시스템, 공격차단시스템, 패킷 모니터링

* 본 연구는 지식경제부 및 정보통신산업진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음. (NIPA-2010-(C1090-1031-0005))
접수일(2010년 10월 11일), 심사일(1차 : 2010년 12월 2일), 게재 확정일(2010년 12월 12일)
[1] 한양대학교 전자컴퓨터통신공학과
[2] 서경대학교 전자공학과
주 저 자 : 김태원
교신저자 : 이주영
E-mail; jylee@skuniv.ac.kr

1. 서 론

인터넷은 이제 일상생활에서 떼어놓을 수 없는 생활의 일부가 되었다. 집이나 사무실에서 웹서핑, 이메일, 쇼핑, 증권거래 등 인터넷을 이용한 수없이 많은 일들을 하고 있다. 그러나 인터넷은 애초에 보안의 개념 없이 만들어 졌기 때문에 악의적인 사용자가 네트워크를 통해 시스템에 침투하여 시스템을 마비시키거나 개인정보를 탈취하는 문제들이 커다란 사회적 이슈가 되고 있다. 오늘날 네트워크 침해들은 점점 더 지능적이고 복잡해지고 있고, 이에 따라 이를 방지하려는 보안 기술들도 발전을 거듭하고 있다. 침입탐지 시스템은 수많은 패킷들 중 공격 패킷을 찾아내어 차단할 수 있도록 하는 1차 저지선 역할을 하므로 가장 기본적이면서 중요한 기술이라고 할 수 있다[1].

지금까지 다양한 침입탐지 시스템 기술들이 개발되어 왔고 이들을 분류하는 몇 가지 방법이 있지만 일반적으로 침입을 판단하기 위해 정보를 모으는 위치에 따라 호스트 기반과 네트워크 기반의 침입탐지 시스템으로 분류하는 방법이 사용된다[2]. 호스트 기반 침입탐지 시스템은 침입 여부를 호스트 내부에서 정보를 얻어 분석하여 결정한다. 네트워크 기반 침입탐지 시스템은 호스트 외부의 네트워크 세그먼트에서 지나가는 패킷의 트래픽량이나 패킷 헤더 또는 내용을 분석하여 결정한다. 네트워크 기반 탐지 기술은 하나의 네트워크 세그먼트에서 하나의 침입탐지 시스템만 있으면 되고 호스트의 처리능력을 방해하지 않기 때문에 많이 사용되고 있다.

한편 네트워크 침해는 매우 다양한 방법으로 이루어지고 있는데, 바이러스, 웜과 같이 네트워크를 통해 타겟 시스템에 해킹 코드가 침투하여 시스템을 무력화시키거나 개인 정보를 탈취하는 방법, DoS, DDoS와 같이 인터넷의 보안 취약점을 이용하여 타겟 시스템의 네트워크나 시스템 자체를 무력화시키는 방법, 패킷 스니핑, 세션 하이잭킹과 같이 호스트간 통신을 중간에서 끼어들어 거짓 정보를 흘리거나 개인정보를 취득하는 방법 등으로 나눌 수 있다. 이들 중 현재 가장 큰 피해를 입히고 탐지나 추적이 어려운 공격은 DoS 공격이라고 할 수 있다. DoS 공격은 시스템 또는 네트워크 자원을 공격 대상으로 하여 사용가능한 자원을 모두 소비하여 사용자가 실제 사용하야 하는 자원을 사용할 수 없게 만드는 서비스 거부 공격이다. DoS 공격은 대역폭, 프로세스 처리 능력 및 시스템 자원을 고갈시킴으로써 정상적인 서비스를 제공하지 못하게 만드는 모든 행위를 발하기 때문에 그 방법 또한 다양하다. 최근에는 많은 수의 시스템에 몰래 Agent를 설치하여 Zombie로 만든 뒤 이 Zombie 시스템들이 하나의 타겟 시스템을 한꺼번에 집중 공격하는 분산 서비스 거부 공격(DDoS) 이 대부분을 이루고 있다[3]. 최근 빈번하게 발생하는 웜바이러스에도 DoS 공격 방식이 내장되고 있는 현실이다. DoS 공격은 공격이 여러 개의 소스에서 이루어지고 특정 소스에서는 매우 적은 수의 패킷을 사용하고 또 TCP, UDP, ICMP 등 다양한 형태의 패킷을 공격에 이용하기 때문에 공격자의 추적은 물론, 탐지와 방어에 어려움이 있다.

본 논문에서는 이러한 DoS 공격을 유형에 따라 분류하고, 효과적으로 대처할 수 있는 새로운 탐지 기법을 제시한다. 또한 이러한 탐지 기법을 이용하여 DoS 공격을 효과적으로 탐지하고 차단하는 시스템의 구조에 대하여 제안한다. 본 논문의 구성은 다음과 같다. 제2장에서는 DoS 공격의 유형에 대하여 분석한다. 제3장에서는 제안하는 공격 탐지 기법에 대하여 설명한다. 제4장에서는 이 시스템을 구현하여 실제의 패킷에 대하여 공격 탐지 여부의 실험에 대하여 설명한다. 마지막으로 제5장에서는 본 연구의 의의와 향후 연구 과제에 대하여 기술한다.

2. 관련연구

2.1 DoS 공격 유형 분류

DoS 공격은 현재 여러 대의 컴퓨터에 Agent를 감염시켜 Zombie PC로 만든 뒤 이 Zombie PC들을 이용하여 타겟 시스템에 집중 공격하는 DDoS 공격이 대부분을 이루고 있으므로 본 논문에서 DoS 공격의 유형에 대하여 설명하는 것은 DDoS 공격을 설명하는 것과 같은 의미로 볼 수 있다. DDoS 공격은 대량의 트래픽을 유발하는 플러딩(Flooding) 공격, 과도한 세션을 요구하는 커넥션(Connection) 공격, 기타 애플리케이션(Application) 특성을 활용한 공격으로 구분할 수 있다.

2.1.1 Flooding 공격

Flooding 공격은 정상 패킷을 무작위로 전송하여 Target 시스템 및 네트워크의 자원을 고갈시켜서 정상적인 서비스 제공을 방해하는 형태의 공격방법이다.

SYN 플러딩 공격은 공격자가 TCP SYN 패킷을 무작위로 전송하여 착신측의 시스템은 무차별적으로 들어오는 TCP 세션으로 인해 시스템이 마비되는 공격으로, 플러딩 공격의 대표적인 공격 중의 하나라고 할 수 있다. RST 플러딩 공격은 공격자가 TCP RST 패킷을 무작위로 전송하여 실제 액티브 세션을 단절시키는 공격이다. ACK Flood-

표 1. DDoS 공격 탐지 기법

탐지 기법명	탐지 방법
IDS/IPS	- 특정 signature를 등록하여 탐지
DDoS 대응시스템	- L3 기반으로 고속으로 DDoS 공격
Netflow	- 트래픽 패턴 분석 및 불규칙적 트래픽에 대해 식별 가능 - source/destination IP 별, protocol 별, port 별, AS 별 등으로 분석 가능
ACL	- 라우터에서 Access-list를 이용하여 실시간 source/destination IP, port, protocol 만 확인 가능
MRTG/RRD	- 서버에서 라우터를 대상으로 SNMP get 으로 수집한 MIB 데이터를 분석 - 트래픽 급증, 급감여부를 보고 징후 판단
DNS 서버	- DNS 서버로 들어오는 DNS query 패킷을 분석하여 과도한 query 패킷을 탐지 - DNS 서버에 저장되는 log를 실시간으로 콘솔에서 모니터링
L7 스위치 (IPS)	- query 수 임계치를 미리 설정해 놓고 초과하는 query가 발생시 알림

ing 공격은 공격자가 TCP 세션이 없는 상태에서 TCP ACK 패킷을 무작위로 보내면 착신측에서 변조된 발신 IP로 RST 패킷을 무작위로 보내게 되고, 동시에 ICMP host unreachable 패킷을 보내면서 착신측 시스템의 과부하를 초래하는 공격이다. UDP/ICMP 플러딩 공격은 각각 UDP/ICMP 패킷을 다량으로 발생시켜서 네트워크의 병목현상 및 시스템의 과부하를 유발시키는 공격방법이다[4].

2.1.2 커넥션 기반 공격

커넥션 기반 공격 중에 HTTP 공격의 경우에는 여러 대의 PC에게 동일하게 접속을 요청하여 서버의 HTTP 처리 커넥션 용량을 초과시켜서 정상적인 HTTP 연결을 방해하는 형태의 공격이라고 할 수 있다. 마찬가지로 과다 TCP 커넥션 형태의 공격도 정상적인 TCP 연결 가능 수치를 초과하는 연결을 시도하도록 하여 서버의 정상적인 연결 시도를 방해하는 형태의 공격이라고 할 수 있다[5].

2.1.3 애플리케이션 기반 공격

애플리케이션 기반 공격은 VoIP의 경우 SIP 단말의 등록을 위한 REGISTER 패킷을 과도하게 요청하는 REGISTER storm 공격, 통화 시도를 과도하게 요청하는 INVITE 공격, BYE 공격 등이 있으며 기타 FTP 공격, DNS 공격, DHCP 리퀘스트 공격, RPC 공격 등의 각종 프로토콜의 취약점을 활용한 다양한 형태의 애플리케이션 공격이 존재한다[6].

표 2. DoS 공격 차단 방법

구분	기법명	차단 방법
URL 차단	DNS 싱크홀	- DNS 캐싱 서버에서 차단하고자 하는 특정 URL에 대해 loopback IP (127.0.0.1) 선언을 하거나, 임의의 서버 IP를 설정 - 해당 사업자에 할당되지 않은 IP에서 DNS query를 받을시 차단하도록 캐싱서버에 차단설정(IP 스푸핑 등 차단 효과)
	L7 스위치	- DNS 앞단에서 특정 URL에 대한 DNS query 패킷 차단설정
IP 차단	Blackhole 라우팅	- 네트워크에서 차단하고자 하는 Destinatin IP를 blackhole 라우팅으로 처리하여 차단 - 등록된 IP는 Null 0 라는 가상 인터페이스로 패킷을 포워딩하여 drop 시킴
	ACL 처리	- Source IP, Destination IP, port 별로 차단이 가능
	uRPF	- G/W 라우터나 가입자접속용 라우터에 uRPF를 적용하여 차단
	CAR (Rate-limit)	- 특정 패턴 (예: sync flooding 등)의 bandwidth를 제한하여 차단효과 발휘
	PBR (Policy Base Routing)	- 특정 사이즈별로 패킷을 ACL 처리, Null 0 로 차단
Port, Protocol 차단	L7 스위치	- 포트, 프로토콜 별 및 TCP/UDP flooding, payload 패턴 등을 설정하여 차단
	ACL 처리	- 라우터에서 포트, 프로토콜 등을 ACL로 설정하여 차단

2.2 DoS 공격 탐지 및 차단 기술

2.2.1 DoS 공격 탐지 기법

DoS 공격을 탐지할 수 있는 방법은 기존의 IDS/IPS, 방화벽 등을 활용하는 방법이나 DoS 전용 대응시스템이나 망 차원의 Netflow, MRTG 등을 이용하는 방법 등이 있다.

2.2.2 DoS 공격 차단 방법

(a) DNS 싱크홀

DNS 캐싱 서버의 DB에 Bot C&C 서버의 IP를 127.0.0.1 이나 특정 분석용 서버의 IP로 설정하여 감염된 Zom

bie PC 등이 DNS 쿼리를 요청할 때 DNS 서버에서 원천적으로 접속을 차단하는 형태의 차단 방법으로서 현재 대형 ISP들의 서버에는 해당 기능이 적용되어 많은 유해접속을 근본적으로 차단하고 있다.

(b) 블랙홀 라우팅(Blackhole Routing)

기존의 라우터에서 ACL을 수동으로 설정하는 것은 일정 규모가 넘어가는 망에서는 효용성이 많이 떨어질 수 밖에 없는 방법이다. 특히 네트워크 장비가 수천대 이상되는 대형 ISP에서는 모든 라우터에 ACL을 동시에 거는 것도 어렵지만 이미 설정되어 있는 ACL을 변경하거나 삭제하는 것 그리고 전체 라우터의 ACL을 동기화 하는 것은 매우 어렵다고 할 수 있다. 따라서 쉬게 ACL 같은 기능을 전체 라우터에 enable 하기 위해서는 BGP 라우팅 프로토콜을 활용하여 블랙홀 서버와 각 라우터간 iBGP를 설정하여 특정 목적지로 가는 트래픽을 차단할 필요성이 발생할 경우 BGP routing table에 목적지를 라우터의 192.168.0.1 같은 특정 IP로 포워딩 처리하고 해당 라우터에는 사전에 해당 IP를 null 0 으로 설정해 놓으면 결과적으로 해당 목적지로 가는 트래픽이 drop 되는 효과를 가질 수 있다. 동시에 블랙홀 서버와 연동되어 있는 모든 라우터에 동시에 적용할 수 있으므로 운영하기 편리한 장점이 있다.

(c) uRPF

Source IP 주소를 위장(IP Spoofing) 한 공격을 차단해 줄 수 있는 기술로서, 라우터가 패킷을 받으면 source IP 주소를 확인하여 해당 IP로 갈 수 있는 역경로(Reverse Path)가 존재하는지 확인함으로써 출발지 IP 주소를 신뢰한다. DoS 또는 DDoS 공격이 자신의 출발지 주소를 위장하므로 uRPF는 상당히 효과적인 서비스 거부 공격 차단 방법이 될 수 있다. 하지만 이 기술 역시 다수의 라우팅 경로가 존재하는 비대칭 망구조를 가지고 있을 경우 적용의 한계가 있으며, Spoofing을 방지하는 것 이외에 다양한 서비스 거부 공격에 대한 대응 기능이 없다는 단점이 있다.

(d) Rate-Limit

특정 서비스 또는 패턴을 가진 패킷이 단위시간 동안 일정량 이상 초과할 경우 그 이상의 패킷을 통과하지 않도록 하는 기술을 Rate-Limit 기술이라 한다.

3. 공격탐지기법

3.1 제안하는 공격 탐지 알고리즘

DoS(Denial-of-Service) 및 DDoS(Distributed DoS) 공격은 피해 호스트가 인터넷에 정상적인 서비스를 제공하거나 서비스를 받는 것을 방해하는 공격이다. 이러한 공격은 다수의 감염된 호스트가 피해 호스트에게 다량의 무의미한 패킷을 전송하여, 피해 호스트와 인터넷 사이의 자원 불균형을 초래하고, 감염된 호스트로부터 전송되는 막대한 트래픽은 피해 호스트의 연결을 방해한다.

공격이 발생했을 경우, 네트워크에서 전달되는 패킷을 살펴보면 다음과 같은 특성을 가진다. 근원지 주소의 경우 매우 폭넓게 분포하게 된다. 그러나 많은 양의 패킷이, 공격 도구에 따라 포트는 달라질 수 있지만, 특정한 피해 호스트를 향하게 되어, 목적지 주소의 분포는 집중된다.

이러한 DoS 공격을 탐지하기 위해서는 먼저 네트워크가 정상상태(normal state)에 어느 정도의 부하를 처리하고 있는지 알아야 한다. 그리고 네트워크 공격 분석에 대한 특정한 parameter를 정의하고, 정상상태의 parameter 값 등에 대한 임계치를 정하는 것이 무엇보다 중요하다. 일반적으로 잘 알려진 parameter는 CPU 사용량 및 Load 양, 패킷의 크기와 패킷 header의 정보 분포, 네트워크 서비스의 종류별 분포를 알 수 있는 프로토콜의 분포와 전체적인 트래픽양에 대한 최대치 및 평균치와 특정 호스트에 대한 집중현상, spoofing 주소를 이용하는 플로우에 대한 모니터링, 네트워크 상에서 플로우 급증 현상을 파악하는데 이용하는 네트워크 플로우 정보 등이 있다. 이러한 parameter를 서로 조합하여 트래픽을 분석함으로써 트래픽 특성에 대한 신뢰도를 높일 수 있다. 그러나 많은 parameter의 조합과정과 유입되는 네트워크 패킷의 데이터를 분석해야하기 때문에, 실제 구현 복잡도가 높아지고 시스템의 자원을 소모하게 된다. 따라서 본 논문에서는 네트워크 패킷의 데이터를 볼 필요가 없으면서, 구현 복잡도를 최소화하고 또한 오탐률을 줄이기 위해 적용 시스템의 특성에 맞게 자동 임계치를 설정하는 Detecting Early DoS/DDoS attacks through Packet Counting 알고리즘을 제안한다.

제안된 알고리즘은 다음의 3단계로 동작한다.

a. 정상 상태의 네트워크에서의 학습단계
b. 학습단계에서 얻어진 임계치 허용량과 실시간 패킷의 개수와의 비교
c. 공격 판단

본 논문에서 제안한 알고리즘의 동작을 위해서는 네트워크의 정상상태와 공격상태의 비교를 위한 parameter로 각 포트별 평균 이용률, 순간 이용률, 임계치, 중간값이 필요하며, 구하는 과정은 다음과 같다.

임의의 단위 시간을 t라고 하면, 임의의 단위 시간 t동안의 유입되는 패킷의 개수를 각각의 포트번호별 계산하여 P_t를 구한다. 이 P_t를 사용하여 식 (1)과 같이 각 포트별 평균 이용률을 구할 수 있다.

각 포트별 평균 이용률

$$P_a = \frac{\sum_{t=0}^{T} P_t}{T} \tag{1}$$

또한 각 포트별 순간 이용률을 식 (2)와 같이 구할 수 있다.

각 포트별 순간 이용률

$$P_i = \frac{P_{t-1} + P_t}{2} \tag{2}$$

이렇게 구해진 평균 이용률과 순간 이용률의 차이를 이용해 식 (3) 같이 공격 받는 포트번호의 순간적 패킷 증가를 알 수 있다.

$$P_c'' = P_a - P_i \tag{3}$$

하지만 식 (3)의 값을 이용하여 공격을 탐지한다면, 서서히 패킷량을 증대시켜 이러한 값의 비교 자체를 할 수 없게 하여 공격을 탐지하지 못하게 하는 지능화된 DoS 공격은 이러한 순간적인 변화값으로는 알아차리지 못하는 경우가 생긴다. 따라서 본 논문에서는 공격탐지의 기준이 될 수 있는 패킷량의 중간값을 구하는 방법을 제안한다. 중간값을 구하는 방법은 다음 식 (4)와 같다.

$$\begin{aligned} \text{중간값 } M_1 &= \frac{P_1 + P_2}{2} \\ M_2 &= \frac{M_1 + P_3}{2} \\ M_3 &= \frac{M_2 + P_4}{2} \\ &\vdots \\ M_{t-1} &= \frac{M_{t-2} + P_t}{2} \end{aligned} \tag{4}$$

이렇게 구해진 중간값과 각 포트별 평균 이용률의 차를 통해 식 (5)와 같이 본 논문의 공격 탐지 알고리즘의 임계치를 구한다.

$$\begin{aligned} &\text{임계치} \\ &P_c = P_a - M_t \end{aligned} \tag{5}$$

이 임계치(P_c)로부터 공격을 탐지하기 위해서는 적정 범위의 허용량이 필요로 하는데, 이 허용량과 식 (5)의 값을 비교하여 공격임을 판단한다. 임계치(P_c)의 허용량을 특정한 값으로 정할 경우 각 각의 시스템별 포트 이용률에 유연하게 대처할 수 없다. 따라서 본 알고리즘에서는 일정 기간의 학습단계를 가진다. 학습기간에서 시스템은 각각의 포트별 임계치의 허용량을 점차적으로 증가시켜 일정기간의 학습을 거친 후 이 임계치의 허용량은 시스템에 특화된 각각의 포트 별 임계치 허용량을 가질 수 있다. 이 학습된 임계치 허용량을 바탕으로 식 (6)과 같이 DoS 공격을 탐지할 수 있으며, 사용자의 정상 트래픽에 대한 오탐율을 줄일 수 있다.

$$\text{if} \left[\begin{array}{l} \text{학습된 임계치 허용량 } P_c' < \\ \left| \begin{array}{l} (\text{특정 포트의 평균 이용률 } P_A) - \\ (\text{특정 포트의 단위 시간당 패킷수의 중간값 } M_t) \end{array} \right| \end{array} \right], \tag{6}$$

$then\ DoS$ 공격 판정

4. 시스템 구현 및 실험

4.1 공격 탐지 도구 개발

본 논문에서 제안한 DoS 공격 탐지 알고리즘을 이용하여, C#을 이용하여 공격탐지 도구를 구현하였다. 개발하면서 구현 복잡도를 줄이기 위해 단위 시간당 패킷량은 이전 값과 비교하여 최대 값만을 고려하여 구현하였다. 구현에 필요한 순서도는 다음 그림과 같다.

공격탐지 도구는 사용자 호스트에 위치하여 IP View, Port View, Session View, Packet View별로 나누며, 들어오는 패킷들을 실시간으로 모니터링한다. 모듈에서 사용되는 로컬 호스트(Local Host)는 현재 모니터링 중인 에이전트를 말하며, 원격 호스트(Remote Host)는 현재 모니터링 중인 에이전트들과 세션을 맺은 호스트를 말한다. 그림 2는 로컬 호스트와 원격 호스트의 end-to-end 연결 상태를 보여주는 매핑도이다.

그림 3은 각 패킷의 최소한의 정보를 분석하기 위한 것이며, 로컬 호스트에서 송수신되는 모든 패킷의 발신지와 목적지의 주소 및 포트, 사용 프로토콜, TCP State, TTL, 패킷의 전송 및 수신 시간을 누적하여 실시간으로 보여준다. 분석된 정보를 바탕으로 하여 송신지 주소와 수신지 주소를 알 수 있으며(그림 4), 또한 사용되는 포트 번호를 알 수 있다(그림 5). 또한 사용되고 있는 프로토콜을 알 수 있다(그림 6).

그림 4는 로컬 호스트와 연결된 원격 호스트의 IP를 보여주는 화면으로, 그림 4(b)는 DoS공격을 하였을 경우의 모니터링 화면이다. 로컬 호스트의 NIC(Network Interface Card)는 가상의 NIC를 포함하여 2개 이상이 될 수 있다. 또한, 로컬 호스트의 각 NIC 별 통신 현황을 한눈에 파악할 수 있다.

그림 5는 로컬 호스트와 원격 호스트의 포트 간의 연결 상태를 보여주는 화면이다. TCP와 UDP를 구분하여 전송계층에서 사용 중인 프로토콜 현황 파악이 가능하다.

그림 6은 로컬 호스트와 원격 호스트 간의 응용 서비스 이용 현황을 보여주는 화면으로, 로컬 호스트에서 이용 중인 응용 서비스를 파악할 수 있다. HTTP, FTP, DNS, telnet 등의 잘 알려진 서비스뿐만 아니라 멀티미디어 관련 프로토콜인 SIP, RTP, RTCP의 세션 상태도 파악이 가능하다. 정의가 되지 않은 응용서비스는 Unidentified로 하였다.

그림 6은 제안된 공격 탐지 알고리즘을 분석하기위해서, 구현된 프로그램으로부터 얻어진 값들의 데이터베이스이다. 값들은 ①의 화살표 방향으로 분석되며 단위시간은 3초로 설정하였다. ②는 매 단위시간 3초 동안의 실제 패킷의 수를 계산하였으며, 구현 복잡도를 줄이기 위해 과거의 패킷량보다 현재의 패킷량이 적다면, 계산의 편의

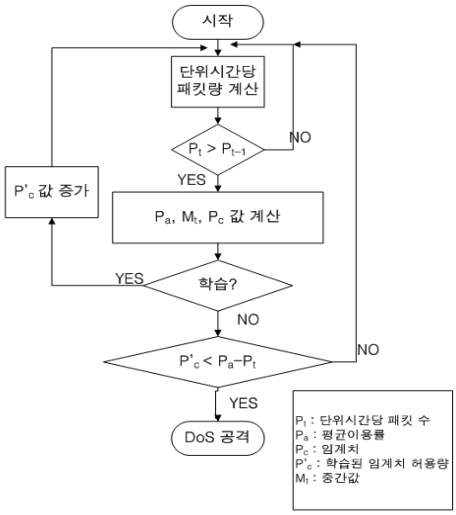


그림 1. 공격 탐지 순서도

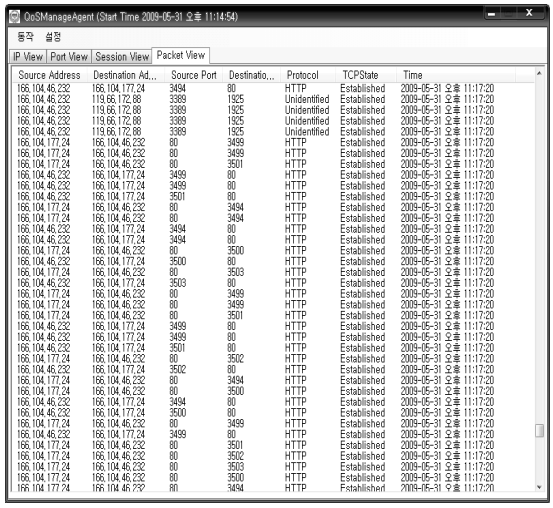


그림 3. Packet View

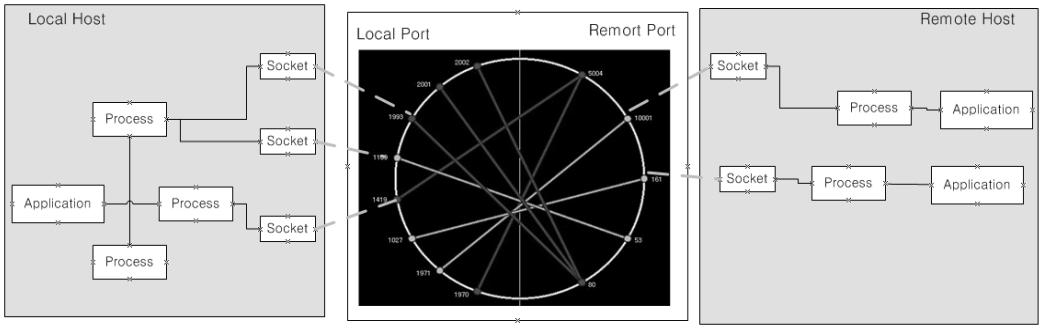
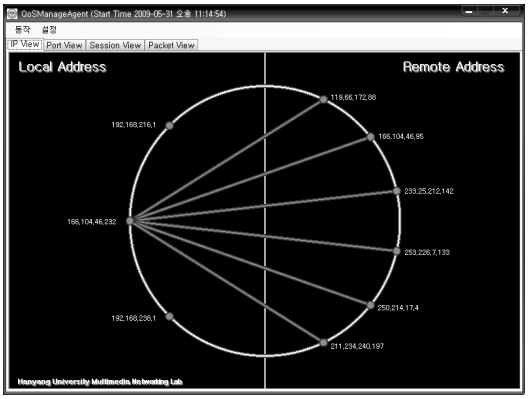
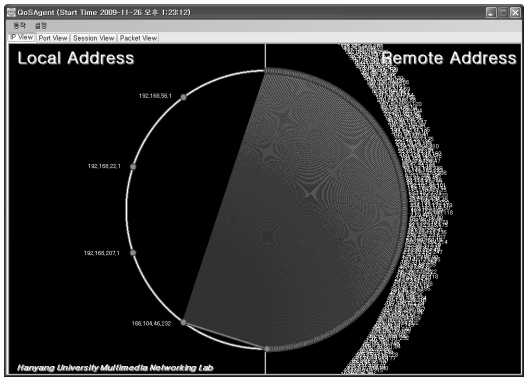


그림 2. 로컬 호스트와 원격 호스트의 연결 상태 매핑



(a) 정상적인 모니터링 화면



(a) DoS 공격시의 모니터링 화면

그림 4. IP View 화면

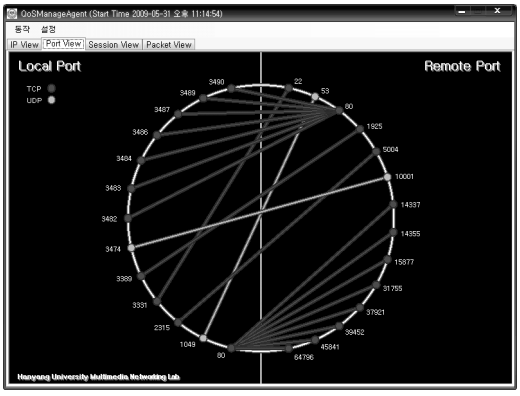


그림 5. Port View

성을 위해 0으로 하였다. ③은 학습을 통해 임계치의 허용량이 증가됨을 알 수 있다. 그림에서의 해당 포트(10035번)의 임계치 허용량은 700까지 증가되었음을 알 수 있다. 이 700은 평균 사용률과 중간값의 차이가 700이 넘어

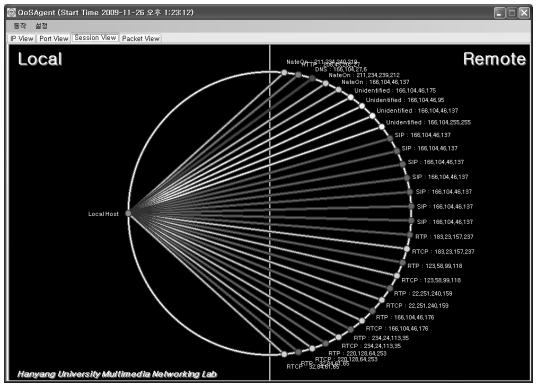
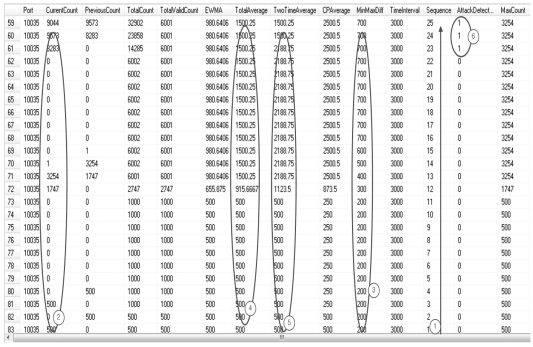


그림 6. Session View



	Port	CurentCount	PreviousCount	TotalCount	TotalValidCount	EWMA	TotalAverage	TwoTimeAverage	CPAverage	MinMaDiff	TimeInterval	Sequence	AttackDetect...	MaxCount
59	10035	9044	9573	32902	6001	980.6406	1502.25	1500.25	2500.5	700	3000	25	1	3254
60	10035	9570	9283	23958	6001	980.6406	1500.25	1500.25	2500.5	700	3000	24	1	3254
61	10035	9283	0	14295	6001	980.6406	1500.25	2188.75	2500.5	700	3000	23	0	3254
62	10035	0	0	6002	6001	980.6406	1500.25	2188.75	2500.5	700	3000	22	0	3254
63	10035	0	0	6002	6001	980.6406	1500.25	2188.75	2500.5	700	3000	21	0	3254
64	10035	0	0	6002	6001	980.6406	1500.25	2188.75	2500.5	700	3000	20	0	3254
65	10035	0	0	6002	6001	980.6406	1500.25	2188.75	2500.5	700	3000	19	0	3254
66	10035	0	0	6002	6001	980.6406	1500.25	2188.75	2500.5	700	3000	18	0	3254
67	10035	0	0	6002	6001	980.6406	1500.25	2188.75	2500.5	700	3000	17	0	3254
68	10035	0	0	6002	6001	980.6406	1500.25	2188.75	2500.5	700	3000	16	0	3254
69	10035	0	1	6002	6001	980.6406	1500.25	2188.75	2500.5	600	3000	15	0	3254
70	10035	1	3254	6002	6001	980.6406	1500.25	2188.75	2500.5	500	3000	14	0	3254
71	10035	3254	1747	6001	6001	980.6406	1500.25	2188.75	2500.5	400	3000	13	0	3254
72	10035	1747	0	2747	2747	655.675	915.6667	1123.5	673.5	300	3000	12	0	1747
73	10035	0	0	1000	1000	500	500	500	250	200	3000	11	0	500
74	10035	0	0	1000	1000	500	500	500	250	200	3000	10	0	500
75	10035	0	0	1000	1000	500	500	500	250	200	3000	9	0	500
76	10035	0	0	1000	1000	500	500	500	250	200	3000	8	0	500
77	10035	0	0	1000	1000	500	500	500	250	200	3000	7	0	500
78	10035	0	0	1000	1000	500	500	500	250	200	3000	6	0	500
79	10035	0	0	1000	1000	500	500	500	250	200	3000	5	0	500
80	10035	0	500	1000	1000	500	500	500	250	200	3000	4	0	500
81	10035	500	0	1000	1000	500	500	500	250	200	3000	3	0	500
82	10035	0	500	500	500	500	500	500	500	200	3000	2	0	500
83	10035	500	0	500	500	500	500	500	500	200	3000	1	0	500

그림 7. 공격탐지 DB

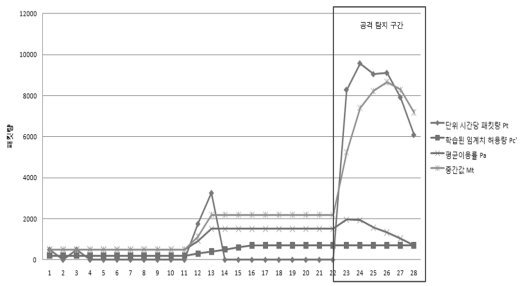


그림 8. 공격탐지 그래프

가면 DoS 공격을 받고 있다고 판단할 수 있는 기준이 되는 값이다. ④는 ②의 패킷량이 0이 아닌 값들로 계산된 해당 포트의 평균 사용률이 계산되고, ⑤는 ②의 패킷량이 0이 아닌 값들로 계산된 해당 포트의 중간값임을 알 수 있다. ⑥은 실제 DoS 공격을 탐지하였음을 알 수 있다.

그림 8은 구해진 값을 바탕으로 각각의 parameter의 그래프를 나타낸다. 그래프에서 알 수 있듯이 공격을 당했을 때 평균이용률의 변화량 보다 중간값의 변화량이 현저히 큼을 알 수 있고, 그로 인해 두 값들의 차는 순간적

으로 학습된 임계치 허용량보다 커짐을 알 수 있고, 공격에 대한 탐지는 정확히 수행됨을 알 수 있다.

5. 결 론

최근 평범한 일반 사람들도 네트워크 공격 툴 사용으로 인한 DoS 공격이 가능해짐에 따라 인터넷 환경에서 큰 위협을 주고 있다. 그러므로 효율적이고 강력한 공격 탐지 시스템이 인터넷 환경에서 매우 중요하게 되었다. 그러나 이러한 공격을 완벽하게 막아내는 것은 매우 어려운 일이다. 본 논문에서는 DoS 공격의 탐지를 위한 알고리즘을 제안하고, 공격탐지도구를 개발하였다. 먼저 정상상태에서의 학습단계를 거쳐서, 학습된 임계치 허용량, 각 포트로 유입되는 패킷의 개수, 중간값 그리고 각 포트별 평균사용률을 계산하고, 이 값을 바탕으로 공격탐지가 이루어지는 3단계 판별 방법을 제안하였다. 제안한 방법에 맞는 공격 탐지 도구를 제작하여 실험을 하였으며, 그 결과 각 포트별 평균사용률과 단위 시간당 패킷량 중간값의 차이와 학습된 임계치 허용량의 비교는 공격 탐지에 효율적임을 알 수 있다. 또한 네트워크 데이터를 들여다 볼 필요 없이, 패킷의 개수만을 이용하여 공격을 탐지함으로써 간단히 구현할 수 있었다. 각 시스템의 포트별 허용량을 학습시킴으로써 대용량 서버, 일반 개인용 PC에 상관없이 상황별 학습이 가능하여, 각 각의 시스템에 적합한 값을 사용하여 공격 탐지를 할 수 있음을 알 수 있다. 향 후 계획으로는 DoS 공격 탐지의 정확도를 높이기 위한 방안을 강구할 예정이다. 그중에서도 평균 사용량의 정확도를 높이고, 또한 중간값이 아닌 더 정밀한 비교값에 대해 연구할 예정이다. 본 논문의 결과는 DoS 공격에 대한 네트워크 보안 대책의 수립으로 네트워크의 가용성을 높여서 네트워크 사용자에게 보다 높은 QoS를 제공 할 수 있을 것이다.

참 고 문 헌

1. Xin Xu, Xuening Wang, “An adaptive network intrusion detection method based on PCA and support vector machines”, ADMA 2005, LNAI 3584, pp. 696-703, 2005.
2. Biswanath Mukherjee, L Todd Heberlein, Karl Levitt, “Network Intrusion Detection”, IEEE Network, Volume 8, Issue 3, pp. 26-41, May 1995.
3. Felix Lau, stuart H. Rubin, Michael H. Smith, Ljiljana Trajkovic, “Distributed Denial of Service Attacks”, 2000 IEEE International Conference on Systems, Man and Cybernetics, Volume:, pp. 2275-2280, 3, 2000.
4. G Carl, G Kesidis, RR Brooks, S Rai, “Denial of service attack detection techniques”, IEEE Internet Computing, pp. 82-89 January 2006.
5. J Charzinski “HTTP/TCP connection and flow characteristics”, Performance Evaluation, pp. 149–162, 2000.
6. H Sengar, D Wijesekera, H Wang, S Jajodia “VoIP Intrusion Detection Through Interacting Protocol State Machines” Dependable Systems and Networks, 2006. DSN 2006.

김 태 원 (taewon0609@gmail.com)

2007 한양대학교 전자전기컴퓨터공학부 학사
2009 한양대학교 전자통신컴퓨터공학과 석사
2009～현재 한양대학교 전자통신컴퓨터공학과 박사과정

관심분여 : 인터넷 QoS, VANET, Security

정 재 일 (jijung@hanyang.ac.kr)

1981 한양대학교 전자공학과 학사
1984 한국과학기술원 전기 및 전자공학과 석사
1993 프랑스 국립통신대학교 네트워크공학과 박사
1997～현재 한양대학교 정교수

관심분야 : 인터넷 QoS, VANET, Security

이 주 영 (jylee@skuniv.ac.kr)

1990 한양대학교 전자공학과 학사
1992 한양대학교 전자공학과 석사
2001 한양대학교 전자공학과 박사
2002～현재 서경대학교 전자공학과 조교수

관심분야 : 네트워크 토폴로지, 스위칭 및 라우팅 알고리듬, 통신시스템 설계