DDoS 공격 탐지 기법인 IPCW-IDS 설계

정회원 정 은 희*, 이 병 관**

A IPCW-IDS(IP Count and WLC based Intrusion Detection System) Design of DDoS attack detection scheme

Eun-Hee Jeong*, Byung-Kwan Lee** *Regular Members*

요 약

본 논문은 목적지 주소를 이용해 DDoS 공격을 탐지하는 IPCW-IDS(IP Count and WLC based Intrusion Detection System)를 설계하였다. IPCW-IDS는 패킷을 캡쳐하는 PCM(Packet Capture Module), 로드 밸런싱 기법인 WLC를 이용해 패킷을 분산시키는 WLCM(WLC Module), 패킷을 분석하는 에이전트인 PAA(Packet Analysis Agent), 패킷의 목적지 IP 정보를 카운트하는 IPCM(IP Count Module), 그리고 DoS공격, DDoS 공격을 탐지하는 IDM(Intrusion Detection Module)로 구성된다. 본 논문에서 제안한 IPCW-IDS는 3단계 DDoS 공격 탐지를 수행하여 False Positive를 줄였다. 1단계는 목적지 주소로 DDoS 공격을 탐지하고, 2단계는 목적지 주소의 패턴으로 DDoS 공격을 탐지하고, 마지막 3단계는, 임계치 이상으로 카운트된 목적지 IP 주소에 대한 패턴으로 DDoS 공격으로 탐지한다. 그리하여 IPCW-IDS는 기존의 고정 임계치에 대한 DoS 공격 오탐지율(TCP)이 20.83%에서 제안한 수식에 의해 8.33%로 감소하였고, DDoS의 False Positive는 기존의 CFB의 8개에서 1개로 감소하였다. 또한, 패킷 분석 에이전트에 패킷을 분산 처리함으로써 병목현상을 줄여 패킷처리속도를 향상시켜 IDS을 성능을 향상시켰다.

Key Words : IPCW-IDS, WLC, CBF, DoS, DDoS, IDS

ABSTRACT

This paper proposes IPCW-IDS(IP Count and WLC based Intrusion Detection System) which detects DDoS attack using destination IP address. IPCW-IDS consists of PCM(Packet Capture Module) capturing packets, WLCM(WLC Module) distributing packets by using load balancing WLC, PAA(Packet Analysis Agent) analyzing packets, IPCM(IP Count Module) counting destination IP address information, and IDM(Intrusion Detection Module) detecting DoS and DDoS attack. The IPCW-IDS proposed in this paper reduces the False Positive by using the DDoS attack detection of the following three steps. The DDoS attack is detected with destination IP address in the first step, the DDoS attack is detected with the patterns of destination IP address in the second step, and the DDoS attack is detected with the patterns of destination IP address which is counted over a critical value. Therefore, IPCW-IDS reduce the 20.83% of respective DoS attacke error detection rate(TCP) about the fixed ciritical value to 8.33% with the proposed expression, and reduce the 8 tif s of the False positive about the existing CFB to 1 tif s. In addition, IPCW-IDS difinish s some bottleneck by distributing packets to a packet analysis agent, which increases the processing speed of packets and improves the performance of IDS.

* 강원대학교 지역경제학과(jeongeh@kangwon.ac.kr), ** 관동대학교 컴퓨터학과(bklee@kwandong.ac.kr)
논문번호 : #KICS2010-04-186, 접수일자 : 2010년 4월 26일, 최종논문접수일자 : 2010년 6월 18일

Ⅰ. 서 론

최근 네트워크 주요 위협 요소로 부각되고 있는 DDoS (Distributed Denial of Servie)는 2000년 2월 Yahoo, Amazon,com, Buy.com, eBay, CNN, E*TRADE, ZDNet 등 미국의 대기업 Web사이트가 차례차례 DDoS의 피해를 받은 후에 주목을 끌게 된 공격 수법이다. DDoS는 취약성이 노출된 여러 호스트에 악성 코드나 바이러스 등의 악의적인 프로그램을 몰래 설치하여 일반 사용자의 PC를 감염시켜 좀비 PC로 만든 후에 C&C(Command & Control)서버를 통해 공격을 개시한다. C&C 서버는 좀비 PC에 패킷을 송출하도록 원격으로 조정하여 명령을 실행하므로, 표적이 된 서버에는 좀비 PC로부터 패킷을 전송받기 때문에 공격을 당하는 서버는 실제의 공격원인 배후인물에 해당하는 컴퓨터인 C&C서버를 찾아내는 것이 어렵다[1].

기존의 네트워크 보안 기법들은 DoS 공격에 대한 보안 방식만을 수행하고 있어 분산 공격 상황을 실시간으로 감지하기 어렵다. 또한 공격에 대응하기 위해 라우팅 프로토콜에 의존하므로 대응시간이 느리며 복잡도가 증가하는 문제점을 가진다. 따라서 이러한 문제점을 해결할 수 있는 효율적인 탐지 기법이 요구되고 있다[1].

본 논문에서는 목적지 주소와 로드밸런싱 기법인 WLC(Weight Least Connection)을 이용하여 DDoS 공격을 탐지 및 차단할 수 있는 소프트웨어 방화벽인 IPCW-IDS(IP Count and WLC based Intrusion Detection System)를 설계하였다. 기존의 CBF (Counting Bloom Filter)는 해시함수를 이용한 인덱스 값을 계산하고 카운트해 임계치 이상으로 카운트된 목적지 IP를 DDoS 공격으로 탐지함으로써 높은 False Positive 문제가 발생하는데, 본 논문에서 제안한 IPCW-IDS는 목적지 주소 자체를 인덱스 값으로 이용해 배열에 카운트하고, 목적지 주소에 대한 패턴을 생성해 3단계 DDoS 공격 탐지에 이용함으로써 False Positive 발생률을 감소시키고자 한다. 또한, 트래픽 임계치를 이용해 정상 트래픽과 비정상 트래픽으로 구분하도록 하여 DoS 공격을 탐지하도록 하였으며, 로드 밸런싱을 이용해 패킷 전송지연을 방지하고 병목현상을 줄여 패킷 처리 속도를 향상시킴으로써 방화벽의 성능을 향상시키고자 한다.

Ⅱ. 관련연구

2.1 DDoS 공격 유형

DDoS 공격 유형은 여러 가지로 구분되지만 크게 Flooding 공격, Connection 공격, Application 공격으로 구분할 수 있다.

Flooding 공격은 정상 패킷과 동일한 패킷을 무작위로 전송하여 타겟 시스템의 CPU, 메모리 등을 고갈시키고 네트워크의 병목을 야기시켜 정상적인 서비스 제공을 방해하는 형태의 공격방법이다.

Connection 공격은 인 HTTP 공격은 아파치 서버의 경우 일반적으로 한 개의 데몬이 1,024개의 연결만 지원하는데 Connection 형태의 공격인 HTTP 공격은 공격자가 임의로 특정 PC에서 수십 개의 연결을 설정하여 여러 대의 PC에게 동일하게 접속을 요청하여 서버의 HTTP 처리 커넥션 용량을 초과시켜 정상적인 HTTP 연결을 방해하는 형태를 말한다.

Application 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, email 스팸, DNS 공격, DHCP 리퀘스트 공격, SQL 공격, Netbios 공격, RPC 공격 등이 각종 프로토콜의 취약점을 활용한 다양한 형태의 애플리케이션 공격이 존재한다.

표 1은 DDoS 공격 유형을 설명한 것이다[2-4].

이러한 DDoS 공격을 탐지할 수 있는 방법은 기존

표 1. DDoS 공격 유형
Table 1. DDoS attack pattern

공격분류	특징	공격유형
Flooding 공격	non-Spoofing 공격	SYN Flooding, ACK Flooding, SYN/ACK Flooding, FIN Flooding, RST Flooding, UDP Flooding, ICMP Flooding, TCP/UDP/ICMP 혼합형 공격
	Spoofing 공격	SYN Flooding, ACK Flooding, SYN/ACK Flooding, FIN Flooding, RST Flooding, UDP Flooding, ICMP Flooding, TCP/UDP/ICMP 혼합형 공격, TCP/IP Null 공격
Connection 공격	HTTP공격	HTTP Daemon 개수 이상을 초과시킴
	과다 TCP connection 공격	Application의 input queue 마비
Application 공격	Application 특성을 이용	FTP 공격, Time 공격, VoIP 공격, Email 공격, DNS 공격, DHCP 공격, SQL 공격, Netbios 공격, RPC 공격 등 Cache Control 공격

의 IDS, IPS, Firewall 등의 보안 장비를 활용하는 방법이나 DDoS 전용 대응시스템이나 망 차원의 Netflow, MRTG(Multi Router Traffic Grapher) 정보를 활동하는 방법 등이 있으며, DDoS 공격 차단은 크게 URL 차단, IP 차단, Port/Protocol 차단 등이 있다.

2.2 Counting Bloom Filter

Bloom Filter는 1bit의 bucket 크기를 갖는 CBF (Counting Bloom Filter)로, 엘리먼트의 삽입만 가능할 뿐 엘리먼트의 삭제는 불가능하다. 왜냐하면, 특정 엘리먼트를 삭제한다는 것은 해쉬 함수들에 의해 정해진 위치들의 비트 값을 "0"으로 설정해야한다는 것인데, 이것은 다른 엘리먼트들의 비트 값을 "0"으로 설정할 수도 있게 된다. 이로 인해 다른 엘리먼트가 그 집합에 속하지 않는다는 부정오류(False Negative)를 발생시키는 문제점이 발생하게 된다. 이 문제점을 해결하기 위해 제안된 것이 CBF이다[5-8].

CBF는 엘리먼트가 삽입되거나 삭제될 때 해쉬 함수들에 의해 정해진 위치의 카운터를 증가시키거나 감소시킨다. 이때 카운터를 저장하는 단일비트를 배열(buckets)로 확장할 수 있으며, n비트 카운터라 한다.

$C(i)$는 i번째 카운터를 가리킬 때, i번째 카운터가 j만큼 증가할 확률은 다음과 같다.(여기서 k번째 해쉬 함수, m 카운터를 갖는 n번째 항목에 대한 블룸 필터를 생각해보자)[6,8,9].

$$p(C(i)=j)=\binom{nk}{j}\left(\frac{1}{m}\right)^{j}\left(1-\frac{1}{m}\right)^{nk-j} \quad (1)$$

n비트 카운터가 2^n값이 된다면 overflow가 될 것이다. 대부분의 응용분야에서 4비트 카운터가 적합하다고 하며, 4비트 카운터일 경우, overflow가 될 확률은 다음과 같다[5-9].

$$p(\max_i(C(i)\geq 16)\geq 1.37\times 10^{-15}.m \quad (2)$$

CBF 기반의 공격 탐지 기법은 세부 주소 필드를 독립적으로 관리함으로써 유일한 IP 주소에 의해 카운트가 증가하는 것이 아니라 서로 다른 IP 주소이지만 같은 인덱스 값에 의해 카운트가 증가되는 경우가 발생한다. 예를 들어, 목적지 주소가 121.x.x.x, x.187.x.x, x.x.85.x, x.x.x.115인 경우일 때, 실제적으로 목적지 주소 121.187.85.115가 발생하지는 않았지만 각각의 인덱스 값에 의해 카운트가 증가하여 임계치를 초과한다면, 목적지 주소 121.187.85.115는 공격 트래픽으로 오탐지 될 수 있다.

이 오탐지가 CBF 기반의 공격 탐지 기법에서 가장 흔하게 발생하는 문제점이라고 할 수 있다. 본 논문에서는 목적지 주소 IP를 4×255 배열에 저장하고, 카운트 값이 임계치를 초과하는 것을 DDoS 공격으로 탐지하도록 하였으며, DDoS 공격 목적지 IP 주소에 대한 패턴인 SubIPList를 이용해 CBF 기반 공격 탐지 기법의 문제점인 False Positive를 줄이고자 한다.

그림 1은 CBF의 동작과정을 설명하고 있다.

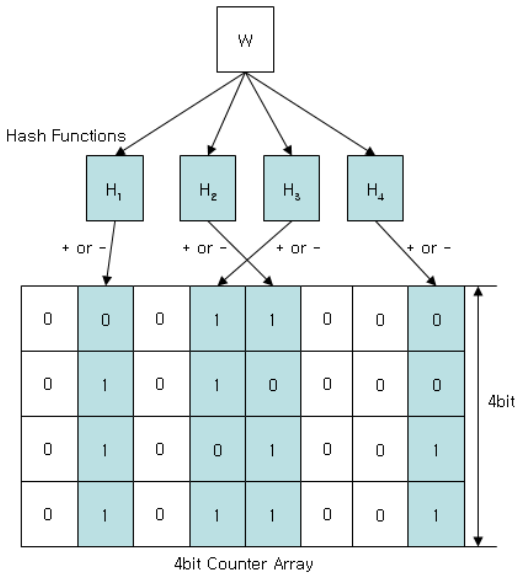

그림 1. Counting Bloom Filter(4bit)
Fig. 1. Counting Bloom Filter(4bit)

2.3 WLC(Weight Least Connection)

WLC는 로드밸런싱 기법 중의 하나로서 작업을 여러 대의 컴퓨터에 균등하게 분산시킴으로서 한 대의 컴퓨터를 사용하는 것보다 짧은 시간에 사용자가 원하는 작업을 수행할 수 있도록 한다.

WLC는 최소 접속 스케쥴링의 한 부분으로 실제 서버에 가중치를 부여하여 가중치에 따라 실제 접속 수가 적은 서버에 요청을 할당한다.

즉, WLC의 기본 가중치는 1이고, 성능이 높은 서버가 더 많은 요청에 응답하도록 설계한 방법으로서 최소 접속 스케쥴링에 비해 가중치를 계산하는 부가적인 배분 작업이 필요하며, 실제 서버의 실제 접속 수를 가중치로 나눈 값이 최소인 실제 서버에 요청을 할당한다[2,11-14].

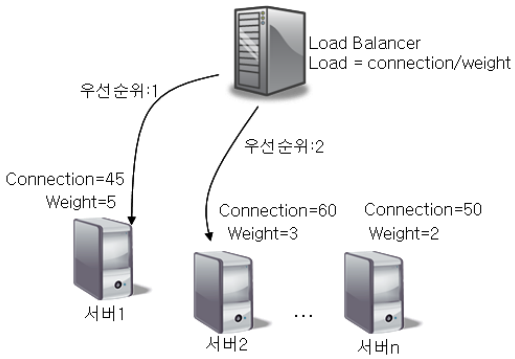

그림 2. WLC(Weight Least Connection)
Fig. 2. WLC(Weight Least Connection)

Ⅲ. IPCW-IDS 설계

본 논문에서 설계한 IPCW-IDS(IP Count and WLC based Intrusion Detection Scheme)는 패킷을 캡쳐하는 PCM, WLC 로드밸런싱 기법을 이용해 패킷을 패킷 분석 에이전트인 PAA(Packet Analysis Agent)에 분산시키는 WLCM과 패킷의 목적지 IP 정보를 카운트하는 IPCM(IP Count Module), PAA에서 분석한 패킷 트래픽으로 DoS공격을 탐지하고, IPCM에 의해 카운팅된 목적지 IP로 DDoS 공격을 탐지하는 IDM(Intrusion Detection Module)로 구성된다.

그림 3은 IPCW-IDS의 전체적인 흐름과 구조를 설명한 것이다.

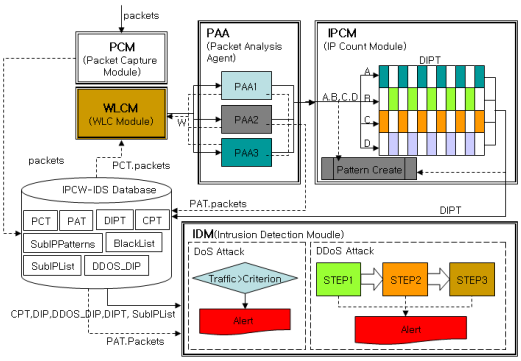

그림 3. IPCW-IDS 구조
Fig. 3. IPCW-IDS structure

3.1 PCM 설계

Ethernet 환경에서 내부 네트워크로 향하는 패킷들을 Broadcasting하게 되고 각 시스템은 자신의 주소가 목적지인 패킷만을 받아들여 운영체제가 처리하게 된다. 이때 인터페이스의 수선 Mode가 Promiscuous로 설정이 되면 목적지가 어디든 상관없이 네트워크상의 모든 패킷을 수신할 수 있게 된다.

본 논문에서 설계한 PCM(Packet Capture Module)은 패킷 캡쳐 모듈로서 WinPcap 라이브러리를 이용하였다. 캡쳐된 패킷은 Source IP, Destination IP, Source Port 번호, Destination Port 번호, TCP, IP, UDP 등 패킷 유형, 패킷 길이 등의 정보를 데이터베이스에 저장한다[1,2,14].

3.2 WLCM 설계

WLCM(Weight Least Connection Module)는 가중치 최소 연결 알고리즘인 WLC를 사용하여 가중치가 높은 Agent를 선택하도록 한 것으로, WLC 알고리즘의 기본 가중치는 1이고, 가중치가 주어진 3개의 각 Agent 서브 모듈의 가중치가 $W_i(i=1,2,3)$일 때, i의 패킷 처리량은 $Packet_i(i=1,2,3)$이고 전체 패킷 처리량은 $Packet_i(i=1,2,3)$의 합이다. 이때, WLCM은 각 Agent의 가중치 W_i와 처리중인 패킷 처리량 $Packet_i$를 전달받아 $\min(Packet_i/W_i)$를 찾아 최소값을 갖는 Agent에 Packet을 전송한다.

WLCM의 결과에 따라 패킷을 수신한 Agent는 수신받은 모든 패킷을 TCP, UDP, ICMP로 구분하여 정리한다[1,2,14].

그림 4는 WLCM에서 가중치에 따라 PAA의 Agent를 선택하는 흐름을 설명한 것이다.

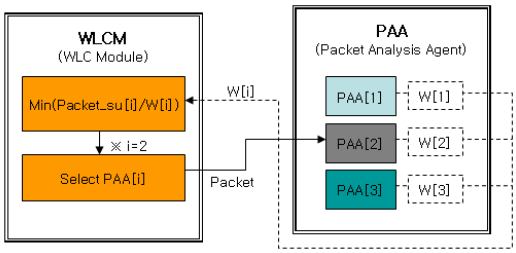

그림 4. WLCM 흐름도
Fig. 4. WLCM flowchart

3.3 PAA 설계

PCM에 의해 캡쳐된 패킷들은 이더넷 프레임 전체를 받기 때문에 수집된 패킷을 유형별로 분류해야 한다. PAA(Packet Analysis Agent)는 패킷을 유형별로 분석하는 에이전트로 PCM에 의해 캡쳐된 패킷들을 TCP, IP, UDP 등으로 분류한 후 데이터베이스에 저장한다. 본 논문에서 제안한 IPCW-IDS는 세 개의 PAA를 가지고 있으며, WLCM에 의해 가중치에 따라 각각의 PAA가 패킷을 할당받아 처리함으로써

PAA의 유휴시간을 줄여 패킷 분석 시간을 줄이고자 하였다[14].

그림 5는 패킷 분석 에이전트의 흐름도를 설명한 것으로 패킷 헤더의 타입 필드를 확인하고 IP, ARP, RARP 로 구분하고 IP 패킷에 대해서는 헤더의 프로토콜을 확인하여 TCP, UDP, ICMP의 패킷으로 구분하여 각 정보는 데이터베이스에 저장한다. 이때 TCP, UDP, ICMP의 트래픽을 체크하여 실시간 트래픽 검사에 이용할 수 있도록 데이터베이스에 저장한다.

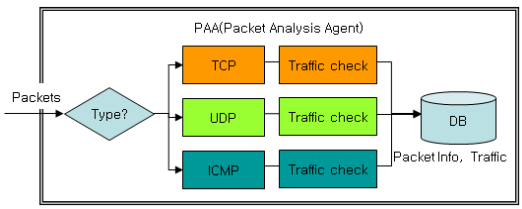

그림 5. Packet Analysis Agent 흐름도
Fig. 5. Packet Analysis Agent flowchart

3.4 IPCM 설계

IPCM(IP Count Module)은 캡쳐된 패킷의 정보 중에서 목적지 IP는 4×255의 2차원 배열의 DIP 테이블의 해당 인덱스를 찾아 인덱스의 카운트를 1씩 증가시킨다. 이렇게 증가된 카운트를 이용해 IDM(Intrusion Detection Module)에서 임계값을 초과할 경우에 침입으로 간주하여 관리자에게 경고를 하게 된다.

본 논문에서 제안한 IPCM은 목적지 IP를 4×255배열에 카운트하고, 임계치보다 큰 목적지 IP를 단순히 DDoS 공격으로 결정하기 전에 목적지 IP에 대한 패턴을 생성해 DDoS 공격 탐지에 이용함으로써 False Positive 오류의 발생 가능성을 감소시켰다.

그림 6은 IPCM의 목적지 IP를 카운트하는 과정을

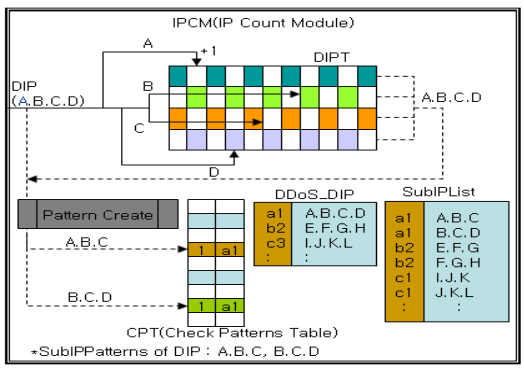

그림 6. IPCM 흐름도
Fig. 6. IPCM flowchart

설명한 것이다. 목적지 주소 A.B.C.D의 A는 목적지 IP 테이블인 DIPT의 1행 A열, B는 2행 B열, C는 3행 C열 그리고 D는 4행 D열에 각각 카운트 된다. 또한, IPCM은 목적지 IP에 대한 패턴을 생성한다. 이렇게 카운트된 결과와 목적지 IP에 대한 패턴은 IDM에서 DDoS 공격을 탐지하는데 사용한다.

3.5 IDM 설계

IDM(Intrusion Detection Module)은 PAA의 모듈에 의해 분석된 패킷의 트래픽으로 DoS 공격을 탐지하고, IPCM 모듈에 의해 동일한 목적지 IP의 방문 횟수를 카운트한 결과를 이용해 DDoS 공격을 탐지하는 역할을 담당하는 모듈이다.

DoS 공격 트래픽의 기준값은 고정임계치를 이용한 유동임계치를 계산하여 유동임계치를 초과하는 트래픽을 DoS 공격으로 탐지하도록 하였으며, 트래픽 분석 절차는 다음과 같다.

1단계 : 트래픽과 고정임계치를 비교해 트래픽이 고정임계치보다 작으면 정상 트래픽으로 판정한다.
2단계 : 트래픽이 고정임계치보다 크면 유동임계치를 계산한다.
유동임계치 = (트래픽 + 이전유동임계치)/2 + 고정임계치×0.01
3단계 : 트래픽이 유동임계치보다 크면 DoS공격으로 간주하고 관리자에게 통보한다.

IPCW-IDS의 DDoS 공격 탐지는 3단계로 이루어지는데, 그 절차는 다음과 같다.

1단계 : 목적지 IP가 DDoS_DIP(DDoS 공격 리스트)에 존재하면 DDoS 공격으로 관리자에게 통보한다.
2단계 : 목적지 IP의 패턴이 SubIPList에 존재하면 DDoS 공격으로 관리자에게 통보한다.
3단계 : 카운트된 DIPT의 목적지 IP가 임계치 이상인 목적지 IP에 대한 패턴이 CPT(패턴 검사 테이블)에 존재하는지 검사하여, 패턴이 CPT에 존재하지 않으면, 목적지 IP를 Black List에 등록하고, 패턴이 CPT 테이블에 존재하면, DDoS 공격으로 간주하여 목적지 IP를 차단 및 DDoS_DIP, SubIPList에 등록 및 하고 관리자에게 통보한다.

그림 7는 IDM이 DoS 공격 및 DDoS 공격을 탐지

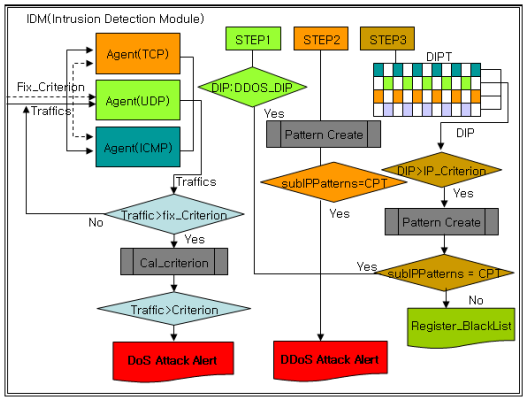

그림 7. DoS 공격 및 DDoS 공격 탐지 절차
Fig. 7. DoS attack and DDoS attack detection flowchart

하는 절차를 설명한 것이다.

Ⅳ. IPCW-IDS 시뮬레이션

본 논문에서 제안한 IPCW-IDS의 시뮬레이션은 Windows XP 운영체제, Visual C++, MySQL 데이터베이스, winpcap 라이브러리를 이용해 실험하였고, 패킷생성기를 이용해 TCP, UDP, ICMP 패킷을 총 16,000개 생성하였으며, 실험기간동안 DoS 공격은 3회 시행하였으며, DDoS 공격은 2회 시행하였다.

4.1 트래픽 분석

4.1.1 TCP 트래픽 분석

그림 8은 TCP 트래픽 분석 결과를 설명한 그래프이다. 고정 임계치를 700(KB)으로 사용하였을 경우에 DoS 공격의 탐지율이 100%이지만 DoS 공격 오탐지율이 20.83%(=(5/24)×100)이다.

하지만, IPCW-IDS에서 유동임계치를 사용하여 DoS 공격 탐지율을 100%, DoS 공격 오탐지율을 8.33%(=(2/24)×100)으로 감소시켰다.

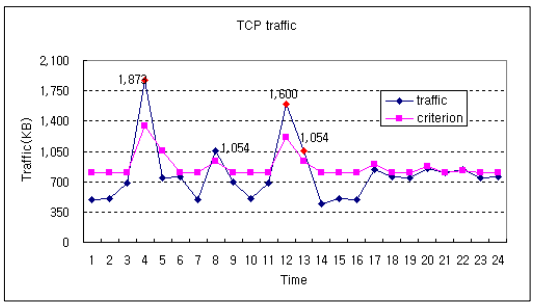

그림 8. TCP 트래픽 분석결과
Fig. 8. The result of TCP traffic analysis

4.1.2 UDP 트래픽 분석

그림 9는 UDP 트래픽 분석 결과를 설명한 그래프이다. 고정 임계치를 4(KB)으로 사용하였을 경우에 DoS 공격의 탐지율이 100%이지만 DoS 공격 오탐지율이 12.50%(=(3/24)×100)이다.

하지만, IPCW-IDS에서 유동임계치를 사용하여 DoS 공격 탐지율을 100%이고, DoS 공격 오탐지율을 4.17%(=(1/24)×100)로 감소시켰다.

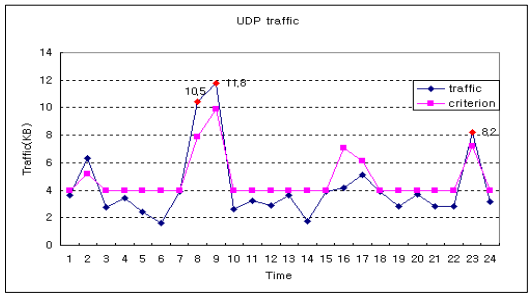

그림 9. UDP 트래픽 분석결과
Fig. 9. The result of UDP traffic analysis

4.1.3 ICMP Traffic 분석

그림 10은 ICMP traffic 분석 결과를 설명한 그래프이다. 고정 임계치를 3(KB)으로 사용하였을 경우에 DoS 공격의 탐지율이 100%이지만 DoS 공격 오탐지율이 37.50%(=(9/24)×100)이다. 하지만, IPCW-IDS에서 유동임계치를 사용하여 DoS 공격 탐지율을 100%이고, DoS 공격 오탐지율을 4.17%(=(1/24)×100)로 감소시켰다.

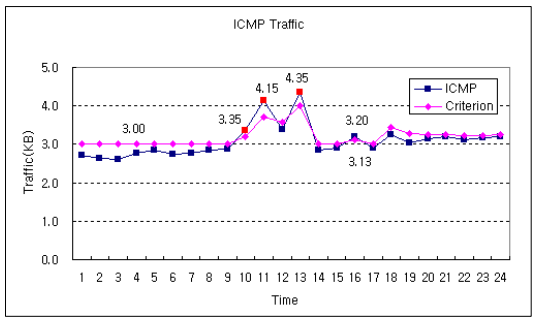

그림 10. ICMP 트래픽 분석결과
Fig. 10. The result of ICMP traffic analysis

4.2 DDoS 분석

IPCW-IDS는 목적지 IP 주소를 이용한 3단계 DDoS 공격 탐지기법으로 탐지과정은 다음과 같다. 1

단계, 캡처한 패킷의 목적지 IP 주소가 DDoS_DIP에 있는지 검사하고, 2단계, 목적지 IP의 패턴이 SubIPList에 있는지 검사한다. 그리고 3단계, DIPT에서 임계치를 초과한 목적지 IP주소의 패턴이 SubIPList에 있는지 검사하도록 하여 False Positive를 줄였다.

표 2는 DDoS 분석 결과를 설명한 것으로 기존의 CBF는 공격대상 목적지 IP를 100% 탐지하였으나, False Positive 발생이 8회 발생하였다. 그러나 본 논문에서 제안한 IPCW-IDS 는 공격대상 목적지 IP를 100% 탐지했을 뿐만 아니라 False Positive 또한 1회 발생하여 False Positive가 감소하였다.

표 2. DDoS 분석결과
Table. 2 The result of DDoS analysis

종류 / 내용	IPCW-IDS		CBF	
공격 대상 목적지 IP탐지 결과	공격 횟수	탐지 횟수	공격 횟수	탐지 횟수
	2	3	2	10
False Positive	1개 발생		8개 발생	

V. 결 론

본 논문에서는 목적지 주소와 로드밸런싱 기법인 WLC(Weight Least Connection)을 이용하여 DoS공격과 DDoS 공격을 탐지 및 차단할 수 있는 소프트웨어인 IPCW-IDS(IP Count and WLC base Intrusion Detection System)를 설계하였다.

IPCW-IDS는 패킷캡쳐를 담당하는 PCM와 패킷을 분석하는 PAA의 에이전트의 가중치에 따라 패킷을 PAA에 분배하는 WLCM, 패킷을 분석하는 에이전트인 PAA, 목적지 IP를 카운트하는 IPCM, 분석된 패킷의 트래픽으로 DoS 공격을 탐지하고 IPCM의 목적지 IP 카운트 값을 이용해 DDoS 공격을 탐지하는 IDM으로 구성된다.

기존 고정임계치와 IPCW-IDS의 유동임계치와 비교해 본 결과 DoS 공격 탐지율은 100%이고, DoS 공격 오탐지율은 TCP가 20.83%에서 8.33%로, UDP는 12.50%에서 4.17%로, ICMP는 37.5%에서 4.17%로 감소하였다. 또한 목적지 주소를 이용한 DDoS 공격 탐지는 기존의 CFB는 False Positive가 8개 발생하였는데, IPCW-IDS는 1개로 False Positive가 감소하였다.

즉, IPCW-IDS는 세 가지 측면에서 성능과 보안이 향상되었다고 볼 수 있다.

첫째, IPCW-IDS는 로드밸런싱기법인 WLC를 이용해 패킷 전송 지연을 방지하고 병목현상을 줄여 패킷 처리 속도를 향상시켰다.

둘째, IPCW-IDS는 고정임계값과 유동임계값을 동시에 사용함으로써 기존의 고정임계값을 이용하는 DoS 공격 탐지 기법보다 DoS 공격에 대한 오탐지율을 감소시켰다.

셋째, IPCW-IDS는 1단계 목적지 주소로 DDoS 공격 탐지, 2단계 목적지 주소의 패턴으로 DDoS 공격 탐지, 3단계 임계치 이상으로 카운트된 목적지 IP 주소에 대한 패턴으로 DDoS 공격으로 탐지하는 3단계 탐지 기법을 사용함으로써 False Positive를 줄였다.

참 고 문 헌

〔1〕 정은희, 장재열, 이병관, “목적지 주소를 이용한 DDoS 공격 탐지 기법 설계”, *한국인터넷정보학회 추계학술발표대회논문집*, 제10권 제2호, pp. 241-244, 2009

〔2〕 정은희, 이병관, “Bloom Filter와 WLC 기법을 이용한 BFWbF(Bloom Filter and WLC based Firewall) 설계”, *한국정보전자통신기술학회 춘계학술발표대회논문집*, 제2권 제1호, pp.189-192, 2009

〔3〕 구자현, “서비스 거부 공격(Denial of Service)의 유형 및 대응”, *정보통신연구진흥원 주간기술동향*, 통권 제1377호, pp.1-12, 2008

〔4〕 전용희, 장종수, 오진태, “DDoS 공격 및 대응 기법 분류”, *정보보호학회지*, 제19권 제3호, pp.46-57, 2009

〔5〕 B. H. Bloom, “Space/Time Trade-offs in Hash Coding with Allowable Error,” *Communications of the ACM*, vol.40, No.7, 1970.

〔6〕 김익균, 오진태, 장종수, 손승헌, 한기준, “버퍼 오버플로우 웜 고속 필터링을 위한 네트워크 프로세서의 Bloom Filter 활동”, *전자공학회논문지*, 제43권 TC편 제7호, pp. 93-103, 2006

〔7〕 A. Broder, M. Mitzenmacher, “Network Applications of Bloom Filters : A Survey,” *Internet Mathmatics*, Vol.1, No.4, 2003

〔8〕 M. Mitzenmacher, “Compressed Bloom Filter,” *IEEE/ACM TRANSACTIONS ON NETWORKING*, Vol.10 No.5, 2002

〔9〕 L. Fan, P. Cao, J. Almedia, and A. Z. Broder, “Summary Cache:A Scalable WideArea web

Cache Sharing Protocol," *In Proceeding of the ACM SIGCOMM '98 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication, ACM Press*, pp.254-265, 1998

〔10〕 유경민, 심상헌, 한경은, 소원호, 김영선, 김영천, "DDoS 공격 탐지를 위한 확장된 블룸 필터 기반의 효율적인 목적지 주소 모니터링 기법", 한국통신학회논문지, 제33권 제3호, pp.152-158, 2008.

〔11〕 권은경, 서재우, 이필중, 박영만, 이해규, 김형현, 정학진, "서버에서 효율적인 메모리 사용을 제공하는 공개키 기반 검색 암호 시스템", *정보보호학회논문지*, 제18권 제4호, pp.3-15, 2008

〔12〕 W. Zhang, "Linux Virtual Server for Scalable Network Services," *Ottawa Linux Symposium*, 2002, http://www.linuxvirtual server.org/lvs.pdf

〔13〕 Y. M. Teo, R. Ayani, "Comparison of Load Balancing Strategies on Cluster-based Web Server," *Transaction of the Society for Modeling and Simulation,* 2001

〔14〕 정은희, 이병관, "병렬처리 HIT기법과 로드밸런싱 WLC 기법이 적용된 HWbF(hit and WLC based Firewall) 설계", *한국인터넷정보처리논문지*, 제10권 제2호, pp.15-27, 2009

정 은 희 (Eun-Hee Jeong) 정회원

1991년 2월 강릉대학교 통계학과

1998년 2월 관동대학교 전자계산공학과 석사

2003년 2월 관동대학교 전자계산공학과 박사

2003년 9월~현재 강원대학교 삼척캠퍼스 지역경제학과 부교수

<관심분야> 네트워크 보안, 전자상거래, 웹 프로그래밍

이 병 관 (Byung-Kwan Lee) 정회원

1975년 2월 부산대학교 기계설계학과

1986년 2월 중앙대학교 전자계산공학과 석사

1990년 2월 중앙대학교 전자계산공학과 박사

1988년 3월~현재 관동대학교 컴퓨터학과 교수

<관심분야> 네트워크 보안, 컴퓨터 네트워크, 전자상거래