실시간 트래픽 분석을 통한 분산 서비스 거부 공격 대응 시스템의 설계 및 구현

한재성[1] 김효곤[2]
[1]고려대학교 디지털정보미디어공학과
[2]고려대학교 컴퓨터학과
[1]js_han@korea.ac.kr, [2]hyogon@korea.ac.kr

Design and Implementation of DDoS Response System with the Real-time Traffic Analysis

Jae-Sung Han[1] Hyo-Gon Kim[2]
[1]Department of Digital Information and Media Engineering, Korea University
[2]Department of Computer Science and Engineering, Korea University

요 약

분산 서비스 거부 공격 탐지를 위한 많은 연구와 개발이 진행 되고 있다. 하지만 분산 서비스 거부 공격의 유형은 계속 변화되어 가고 있어서 새로운 유형의 분산 서비스 거부 공격의 완벽한 탐지는 현실적으로 불가능하다. 본 논문에서는 알려진 유형의 분산 서비스 거부 공격의 탐지뿐만 아니라 새로운 유형의 분산 서비스 거부 공격 탐지를 위하여 실시간으로 트래픽을 모니터링 하고 분산 서비스 거부 공격으로 의심 되는 트래픽을 조기에 탐지하고 신속하게 대응이 가능 한 시스템의 설계와 구현에 관하여 기술 한다.

1. 서 론

초고속 인터넷 인프라가 구축 되고 인터넷 사용자가 늘어나면서 해킹 및 인터넷 침해에 대한 사고 사례가 매년 증가하고 있다. 특히 분산 서비스 거부(이하 DDoS) 공격은 오래 전 부터 발생 해온 공격 유형 이지만 단순한 공격 기법과 어디서나 쉽게 구할 수 있는 툴로 인해 인터넷 상에서 발생하는 공격 유형 중에서 가장 심각하고 그 발생 횟수도 잦으며 효과적으로 차단하기도 쉽지 않다. 최근 DDoS 공격의 주요 목적은 웹사이트나 서버에 네트워크 장애를 발생시켜 해당 업체에 정치적 또는 금전적인 요구를 하며 주로 실시간 서비스를 제공하는 게임거래사이트나 증권사이트, 인터넷 포탈 사이트 등의 다양한 업체들을 대상으로 공격 목표가 다양화 되고 있다. 또한 최근 발생 하는 분산 서비스 거부 공격의 특성은 여러 대의 Zombie(botnet) 시스템으로부터 동시에 많은 트래픽을 발생시키는 형태를 띄고 있고 트래픽의 규모도 Gbps 급으로 증가했으며 네트워크 대역폭을 고갈시켜 서비스를 불가능 하게 하는 형태가 주를 이루고 있다.

위와 같은 DDoS 공격으로 인한 서비스의 중단 및 인터넷 사용의 불가는 개인이나 단체에 심각한 금전적 손해를 입힐 수 있다.

DDoS 공격 탐지와 방어를 위한 연구로는 DDoS 공격의 특성을 이용하여 패킷들의 목적지 주소를 기반으로 공격 트래픽을 모니터링 하는 여러 가지 기법들[1-2]과 통계적 기법을 이용한 연구[3], 공격 트래픽으로 의심되는 패킷들을 우회 시켜 공격 패킷들을 제거하고 정상 패킷들만을 통과 시켜주는 방법[4] 등이 있다. 하지만 위와 같은 기법을 이용한 DDoS 공격의 탐지와 기존 시그니처 위주의 보안 장비에서의 DDoS 공격의 탐지는 공격 상황의 정보 제공 및 실시간 모니터링 기능이 미흡하므로 변화하는 새로운 DDoS 공격 대응에 취약한 면이 존재한다. DDoS 공격을 효과적으로 방어 하기 위해서는 보안 장비에서 탐지 하고 차단 하는 것도 중요하지만 시스템으로 유입되는 트래픽 상황을 실시간으로 모니터링 할 수 있어야 한다. 이를 위해서 트래픽을 수집 하고 이를 분석하여 평상 시 트래픽의 기본 임계치 값을 산출 한다. 이를 이용하여 평상 시 트래픽 유형과 다른 트래픽이 유입 될 경우 DDoS 공격 여부를 신속하게 탐지 한다. 만약 DDoS 공격 일 경우 관리자가 신속하게 대응 할 수 있게 해야 한다. 본 논문에서는 위와 같은 시스템의 설계와 구현에 관하여 기술 한다.

2. 관련 연구

2.1 SNMP와 MRTG 를 이용한 탐지

일반적인 탐지 방법인 트래픽 수집 및 분석을 통한 DDoS 공격 탐지는 비교적 정확한 탐지와 상세한 분석이 가능하다. 하지만 비용과 운영의 확장 성이 부족하다는 단점도 있다. 이를 보완하기 위한 방법으로 SNMP를 이용한 탐지 방법[5]이 있다. SNMP를 이용한 탐지 기법은 TCP, UDP, ICMP 등 프로토콜 별로 MIB을 설정하고 트래픽을 수집 및 분석 하여 DDoS 공격을 탐지 하는 방법이다. SNMP MIB 데이터를 수집하는데 있어서 해당 시스템에 주는 부하가 적고, 표준화된 데이터를 얻을 수 있기 때문에 효과적인 탐지가 가능하다. 하지만 MIB 데이터를 수집하는 주기의 설정에 따라 시스템에 주는 부하가 증가 할 수 있으며 이로 인해 탐지 시간을 줄이는 데 한계가 있다.

2.2 통계적 방법을 이용한 탐지

DDoS 공격은 일반적으로 패킷 공격으로 이루어지는데, 정상적인 패킷과 비 정상 패킷을 구분하기 어려우며. 정확성과 복잡성을 동시에 고려해야 한다. 이런 사항을 반영한 또 하나의 방법이 통계적인 탐지 방법이다. 통계적 방법을 이용한 탐지는 다음과 같은 방식이 있다. 네트워크 속성 값에 대한 임의성을 계산하고, 그 값에 대한 평균 변화 량을 탐지하는 엔트로피(entropy)방식[6], 트래픽 볼륨(trafficvolume), 표준편차, 속성 값에 대한 분산 도를 측정하고 그 값에 비정상적인 값을 탐지하는 카이 제곱(Chi-Square) 통계가 있다. 통계적 방법은 정확한 탐지가 장점이지만 특정한 공격만을 고려하여 탐지하고 실시간성의 탐지가 어려우며, 새로운 공격 유형에 대한 대처가 어려워 실 환경에 적용하기 어려운 한계점을 가지고 있다.

2.3 MULTOPS (Multi-Level Tree for Online Packet Statistics)와 볼륨 필터 기반의 탐지 기법

MULTOPS와 볼륨 필터 기반의 탐지 기법은 목적지 주소를 기반으로 공격 트래픽을 감시한다.[1]

MULTOPS는 각 서브넷 프리픽스에 대한 입력과 출력 패킷 비율을 기록하는 노드의 트리 구조로 IPv4 전체 주소를 표현하기 위해 4-레벨 256-배열로 운영된다. In IP 어드레스와 Out IP 어드레스에 대한 모든 패킷 비율을 테이블에 저장하여, 트리 레벨이 높아질수록 패킷 비율이 긴 선행 구조를 가지게 된다. 해당 기법의 경우 새로운 목적지 주소가 발생할 때마다 동적으로 메모리가 증가하며, 목적지 IP 별로 트리 분할이 발생하여 처리의 복잡성이 증가하는 문제점이 있다.

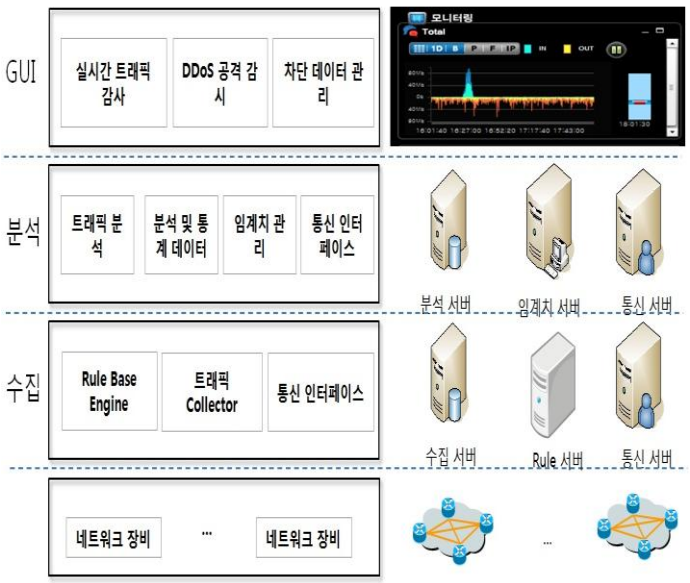
볼륨 필터기반의 탐지 기법은 2차원 배열 구조를 이용 하여, 목적지 IP 주소의 세부 값을 테이블 인덱스 값으로 변환하고 해당 값을 카운트하여 1씩 증가시킨다. 카운트 한 값이 임계 치를 초과 할 경우 그 목적지 IP를 공격 트래픽으로 간주한다. 각 세부 값을 독립적으로 관리함으로써, 하나의 값이 유일한 IP 주소에 의해서 증가되는 것이 아니라, 다른 IP이지만 같은 위치에 동일한 세부 값을 가지는 경우도 있다. 이럴 경우 여러 IP에 의해서 특정 값이 카운트 되는 문제점을 가지고 있다.

2.4 데이터 마이닝 기법

데이타 마이닝 기술은 대량의 데이터 상호간의 의미 있고 관련성이 잇는 유용한 정보를 추출하기 위해서 데이터베이스, 기계학습(Machine Learning), 정보이론(Information Theory), 통계, 가시화(Visualization) 기법 등을 통합한 기술이다. 데이터 마이닝 기법은 침입 탐지 분야에서 이상탐지와 관련하여 많이 연구되어 오고 있다.[7] 이 기법은 정확한 탐지가 가능하지만 신뢰도 있는 충분한 데이터의 확보가 우선 되어야 하며 운용자의 관리가 필수적이다. 기존의 공격 탐지에는 유용하지만 새로운 유형에 대해서는 빠르게 적용 할 수가 없는 단점이 있다.

3. 시스템 설계

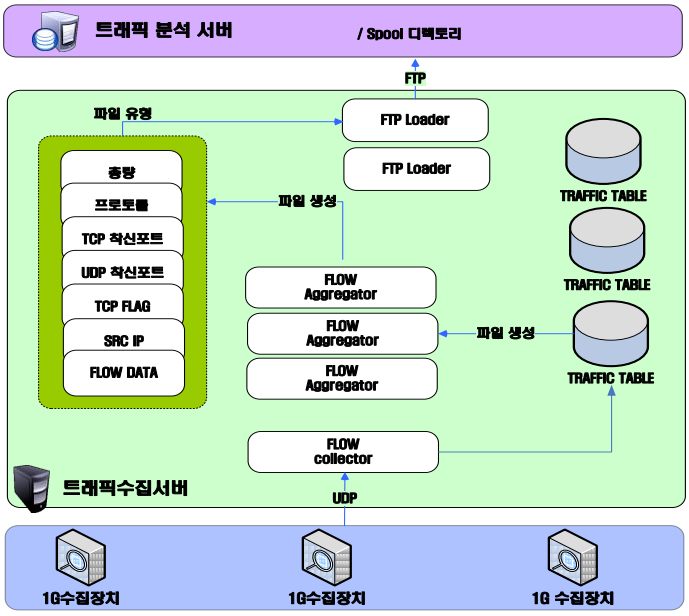
DDoS 공격 대응 시스템의 주요 기능은 실 시간으로 네트워크 트래픽 변화를 모니터링 할 수 있어야 한다는 것이다. 그러므로 트래픽 데이터를 수집하는 기능의 별도의 서버가 필요하다. 수집 서버는 트래픽을 수집 하여 플로우 데이터를 생성하고 분석 서버로 전송 한다. 분석 서버는 플로우 데이터 통계 생성과 플로우 데이타 관리를 위한 트래픽 DB 구축, 구축된 DB 를 이용한 통계 생성 기능, DDoS 공격 탐지 기능, DDoS 공격 분석 기능 등이 있어야 한다. 또한 위의 내용들을 사용자가 관리 할 수 있는 사용자 인터페이스(이하 GUI) 기능도 있어야 한다. 위와 같이 시스템은 수집 서버와 분석 서버, GUI로 구성 되고 전체 구성도는 <그림 1> 과 같다.



<그림 1> 시스템 구성도

3.1 트래픽 수집 서버

기가급 규모의 트래픽 수집이 가능 해야 한다. 본 논문에서는 트래픽 수집에 NetFlow와 sFlow(RFC 3176)를 이용 한다. NetFlow는 본래 네트워크 서비스 이용 과금을 위해 개발된 프레임워크로 플로우 단위로 정보를 제공한다. 보호 해야 하는 서비스나 서버의 상황에 따라 플로우 기반 다양한 통계 정보를 제공하는 sFlow도 사용한다. 대부분의 분산 서비스거부 공격이 급격하게 플로우를 증가시킴으로써 대역폭을 가득 차게 하여 네트워크의 인터넷 연결을 막기 때문에 위와 같이 플로우를 기반으로 트래픽을 수집 하여 분석하는 것은 DDoS 공격 특성을 분석 하는데 유리하다. 수집 서버는 수집 장치에서 수집한 트래픽을 일정한 형식의 파일로 구분하여 생성한다. 이때 기본적인 DDoS 공격 탐지를 수행하고 탐지 된 공격이 있다면 해당 정보도 파일로 생성한다. 생성 된 파일들은 Ftp를 이용하여 트래픽 분석 서버로 전송 한다. 트래픽 수집 서버의 구조는 <그림 2>와 같다.



<그림 2> 수집 서버 구성도

*1차 DDoS 공격 탐지 프로세스

수집 서버에서 1차로 기본적인 DDoS 공격 탐지를 수행 한다. 탐지된 플로우는 파일로 생성 하여 분석 서버로 전송 한다. 1차로 탐지 하는 DDoS 공격 유형은 <표 1> 과 같다.

<표 1> 1차 탐지 DDoS 공격 목록

Land Attack
TCP Port 0 Attack
UDP Port 0 Attack
Unassigned/Reserved IP Protocol Attack
TCP SYN/ACK/NULL Attack
ICMP Attack
TCP Port Scan Attack
Loopback Attack

*파일 생성 프로세스

수집 한 트래픽을 정의 된 형식의 파일로 생성 한다. 생성한 파일을 트래픽 분석 서버로 ftp를 이용하여 임의의 저장 디렉터리로 전송 한다. 생성 하는 파일의 형식은 아래 <표 2> 과 같다.

<표 2> 수집 파일 형식

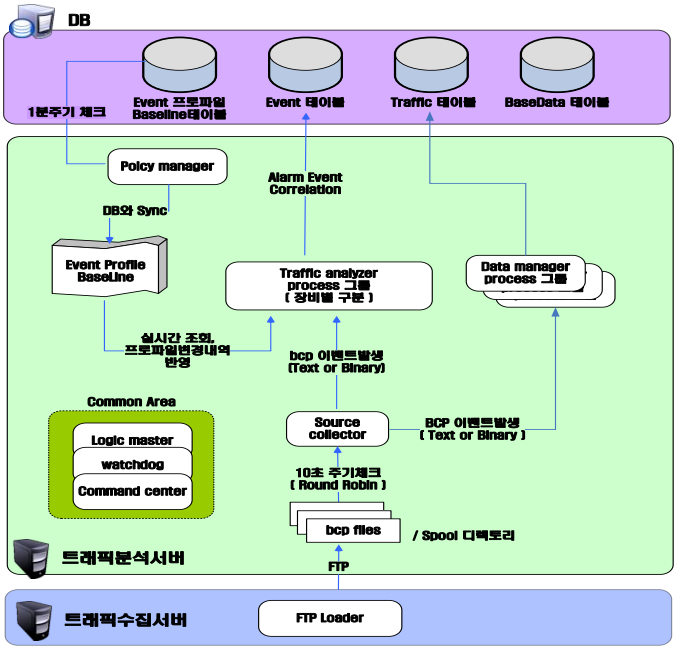
유형 구분	총량, 프로토콜, TCP착신주소, UDP착신주소,Tcp Flag, SrcIp, Flow Data, Attack
데이터 값	총량: 0 프로토콜: 1,6,17 등 프로토콜 값 TCP 착신포트 : 80, 8080 등 포트 값 UDP 착신포트 : 514, 포트 값 TcpFlag : Tcp flag 값 SrcIP : IP 주소 값
BPS	Byte Per Second 값
PPS	Packet Per Second 값
FPS	Flow Per Second 값
CPS	Count of Source IP 값

*트래픽 저장 프로세스

NetFlow나 sFlow 로 수집한 트래픽 데이터를 정의된 형식 대로 데이터 베이스에 임의 저장 한다.

3.2 트래픽 분석 서버

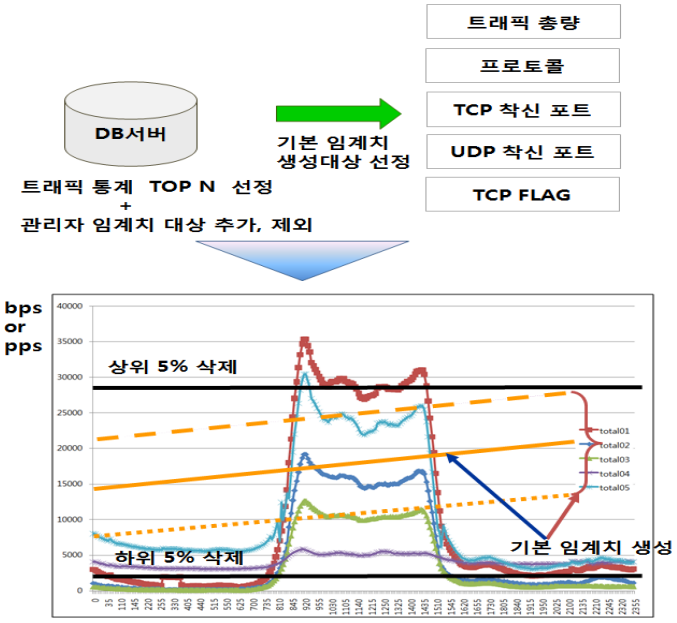
수집 된 트래픽을 일, 주간, 월 별로 통계를 생성하여 DDoS 공격 탐지에 기본이 되는 임계 값을 생성한다. 하지만 이 임계 값만으로는 효과적으로 DDoS 공격을 탐지 할 수 없다. 그러므로 산출된 임계 값과 더불어 표준 편차를 이용한 임계 값도 같이 산출 한다. 실제 상황의 트래픽이 산출 한 기본 임계 값과 표준편차를 이용한 임계 값을 어느 양 만큼 초과해서 유입 되고 있는지에 대한 정보 값도 필요하다. 본 논문에서는 초과한 정도를 주의(Minor), 심각(Major), 매우 심각(Critical)의 3가지로 구분하여 적용 한다. 분석 서버는 위와 같은 요소들을 토대로 수집서버 에서 생성 한 파일을 분석하여 보안 장비나 수집 서버에서 탐지 하지 못하는 새로운 유형의 DDDoS 공격을 탐지 한다. DDoS 공격으로 의심 되는 트래픽이 탐지 되면 알람 이벤트를 발생 시키고 해당 정보를 데이터 베이스에 저장 한다. 관리자는 GUI에서 탐지 된 알람 이벤트를 확인 할 수 있다. 트래픽 분석 서버의 구조는 아래의 <그림 3> 와 같다.



<그림 3> 분석 서버 구성도

*기본 임계 값 생성 프로세스

데이터 베이스에 저장 된 트래픽 정보를 바탕으로 임의 기간 동안의 트래픽 기본 임계 값 정보를 생성 하고 보정 하는 기능을 한다. 기본 임계 값은 총량, 프로토콜, TCP 착신주소, UDP 착신주소, TcpFlag 5개 유형에 관해서 BPS, PPS 를 생성 한다. 기본 임계 값은 신뢰성을 보장 하기 위해 신뢰 구간, 표준 편차, MIN, MAX 임계 치 등의 개념이 적용된다. 생성 된 임계 값 은 임계치를 가지는 기본 임계 값과 그 값을 기준으로 하여 공격 탐지에 사용 되고 공격 심각 도를 알 수 있는 주의(Minor), 심각(Major), 매우 심각(Critical)의 알람 등급 값을 가지게 된다. 기본 임계 값 생성 과정은 <그림 4>와 같다.



<그림 4> 기본 임계 값 생성 과정

기본 임계 값 생성과 관련 된 파라 미터는 <표 2>와 같다.

<표 2> 기본 임계 값 생성 파라미터

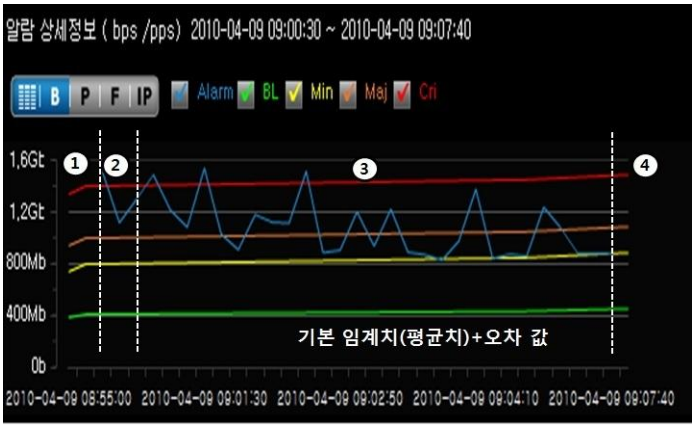
유형 구분	임의의 절대 임계치, 기본 임계 값
생성 유형	휴일, 평일
BL 유형	총량, 프로토콜, 포트
적용비율	상 하위 백분율 값 (95 -5)
하한 값	절대 하위 값
표준편차	표준 편차 적용 비율

*트래픽 저장 프로세스

트래픽 수집서버에서 생성 된 파일을 정해진 형식에 따라 데이터 베이스에 저장 한다. 통계나 분석을 위한 데이터가 더 필요 할 경우엔 파일에서 검색하여 해당 데이터를 데이터 베이스에 추가로 저장 한다.

*2차 DDoS 공격 탐지 프로세스

트래픽 수집 서버에서 생성 된 총량, 프로토콜, TCP 착신포트, UDP 착신포트, TcpFlag 파일에 대하여 기본 임계 값을 기준으로 해서 DDoS 공격 트래픽을 탐지 한다. DDoS 공격이 탐지 되면 알람 이벤트를 생성하고 데이터베이스에 저장 한다. 실시간 트래픽의 변화에 따라 탐지 된 공격 알람의 상태를 관리 하고 감시 하는 기능을 한다. 공격 탐지 기준은 현재 트래픽의 BPS 나 PPS 의 값이 일정 시각 동안 기본 임계 값을 기준으로 하여 초과한 정도를 기준으로 탐지를 한다. 이때 기본 임계 값 생성 시 같이 산출된 공격 심각도에 따라 초과 한 정도를 계산하여 알람의 심각도 즉 등급을 부여 한다. 탐지 된 알람이 일정 시각 동안 기본 임계 값 이하로 떨어지면 알람 상태를 종결 처리 한다. DDoS 공격의 탐지 및 종료 과정은 <그림 5>와 같다.



<그림 5> DDoS 공격 탐지 흐름

① 설정 시간만큼 지속 안 되는 경우 감지 대상 제외

② 주의(Minor) 임계 치를 초과하여 설정 한 시간만큼 지속되면 현시점부터 알람 이벤트 발생
③ 탐지 시점부터 알람 이벤트가 지속되는 경우 지속적인 탐지
④ 주의(Minor) 임계 치 이하로 트래픽이 감소하는 경우 알람 이벤트 종료

3.3 GUI

GUI는 수집 된 트래픽의 일, 주간, 월 통계와 DDoS 탐지 알람 이벤트 분석 기능을 한다. DDoS 공격 탐지를 위한 기본 임계 치 생성 룰의 설정과 탐지 된 DDoS 공격 알람 이벤트를 관리자가 인지 하고 관련 된 조치를 수행 할 수 있도록 하는 기능 등을 한다.

***실시간 트래픽 모니터링**

임의 시간을 기준으로 수집 된 트래픽 데이터의 실시간 추이를 보여 준다. 총량 데이터는 실시간의 추이를 보여주고 프로토콜, TCP 착신포트, UDP 착신포트, TCPFlag, SrcIP 등은 상위 N개의 데이터를 확인 할 수 있다.

***기본 임계 치 생성 및 보정**

분석 서버에서 생성 된 기본 임계 치 데이터를 확인 할 수 있다. 생성 된 기본 임계 치 데이터가 오류로 인해 잘 못 생성 되었거나 보정이 필요한 경우에는 해당 정보를 수정 하여 다시 적용 할 수 있다.

***DDoS 공격 알람 이벤트 탐지 모니터링 및 분석**

분석 서버에서 탐지 한 알람 이벤트 정보를 실시간으로 보여 준다. 탐지 된 알람 이벤트의 상세 정보 및 탐지 된 알람 이벤트의 기준 정보인 임계 치 데이타 정보도 나타내어 실제로 DDoS 공격 인지 정상적인 트래픽인지에 대한 종합 적인 상황 판단이 가능 하다.

***트래픽 및 알람 이벤트 통계 분석**

트래픽 데이타의 일, 주간, 월 통계를 보여준다. 생성 된 통계 데이터로 평상 시의 트래픽 상황을 알 수 있고 DDoS 공격 탐지를 위한 기본 임계 치 생성에 관련 된 정보로 활용 한다.

***서버 관리 및 보안 장비 연동**

시스템의 여러 보안 장비와 수집 서버, 분석 서버의 상태를 모니터링 할 수 있고 DDoS 공격 탐지 알람 이벤트가 발생 했을 경우 보안 장비와의 연동으로 실제 DDoS 공격의 여부와 보안 장비의 상태를 확인 할 수 있다.

4. 시스템 구현

본 논문에서 제안 한 시스템은 Linux 환경에서 구현하였고 데이터를 저장하고 읽어오는 속도를 향상시키기 위해서 Main Memory Data Base를 사용하였다. 상세 내용은 <표 3>과 같다.

<표 3> 시스템 구현 환경

수집 서버	CPU:2.16G*2 MEM: 8G HDD:146*2 OS:REDHAT ES v4 DB: mysql v5
분석 서버	CPU:2.16G*2 MEM: 16G HDD:146*2 OS:REDHAT ES v4 DB:Altibase 5.1.5
GUI	Apache2.0 JBoss 5 DB:Altibase 5.1.5

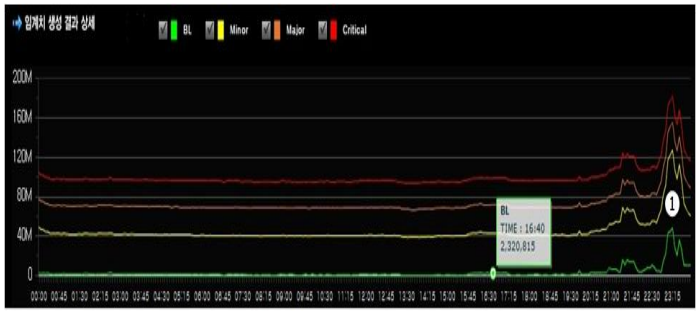
<그림 6>은 실시간 트래픽의 추이와 DDoS 공격 탐지 알람 이벤트 등을 확인 할 수 있는 모니터링 화면이다.

<그림 6> 실시간 트래픽 모니터링 화면

①은 실시간 트래픽 모니터링 화면으로 관리자는 총량의 그래프로 현재 트래픽의 전체 추이를 확인 할 수 있고 프로토콜과 기타 다른 부분으로는 현재 트래픽 데이터의 상위 N개에 해당 하는 데이터의 양을 확인 할 수 있다.
②는 현재 DDoS 공격으로 의심 되는 트래픽을 분석 서버가 탐지하여 알람 이벤트가 발생 한 것을 확인 할 수 있다. 관리자는 알람 이벤트를 확인 하고 실제 DDoS 공격 인지 여부를 보안 장비 연동 등으로 확인 할 수 있고 이에 적합한 대응을 할 수 있다.

<그림 7>은 A 사의 기본 임계 치 화면이다. 트래픽의

양이 2M 이하로 일정 하게 유입 돼다가 오후 9시부터 차츰 증가 하여 ①부분의 시각 오후 11시에서 40M 정도로 가장 높은 것을 확인 할 수 있다.



<그림 7> 생성 된 기본 임계 치 화면

<그림 8>은 A사의 기본 임계 치 데이터를 토대로 A사의 DDoS 공격을 탐지하고 이를 분석 한 화면이다. 오후 6시 40분부터 평소 트래픽 보다 훨씬 많은 2Gbyte 정도로 트래픽이 증가 하여 알람 이벤트가 발생 하였고 <그림 8>의 ①부분에서는 22Gbyte로 최고조에 달한 것을 확인 할 수 있다. 천 개 이상의 Source IP에서 평균 40M 크기의 패킷을 A사의 서버로 전송 하는 것을 ②와 ③ 부분에서 확인 할 수 있다. 또한 ④ 부분을 보면 Flow Data의 프로토콜 대부분이 UDP로 대역폭을 고갈 시키는 전형 적인 DDoS 공격으로 UDP Flooding 공격임을 확인 할 수 있다.

<그림 8> DDoS 알람 이벤트 분석 화면

위의 내용에서 확인 할 수 있듯이 DDoS 공격은 평소 트래픽 유형과는 다른 형태를 보이는 것을 알 수 있다. 평소와는 다른 트래픽이 유입 될 때 이를 신속하게 탐지 하여 DDoS 공격 알람 이벤트를 발생 시키고 지속적으로 모니터링 하여 DDoS 공격에 대응 해야 한다. <표 4>는 제안 된 시스템과 기존의 DDoS 공격을 탐지 하는 시스템과의 차이점을 나타 낸다.

<표 4> 타 시스템과의 비교

	타 시스템	제안 시스템
DDoS 탐지 시간	1 분 이상	1 분 이내
보호 시스템 부하	있음	없음
탐지 시 패킷 손실	부분적으로 있음	없음
관제 및 분석 기능	부분적으로 있음	있음
장비 연동 및 제어	부분적으로 있음	있음

5. 결론 및 향후 연구

본 논문에서는 실시간으로 트래픽을 수집 및 분석 하여 DDoS 공격을 신속하게 탐지하고 대응 할 수 있는 시스템의 설계와 구현에 관하여 기술 하였다. 새로운 유형의 DDoS 공격은 계속 나타나고 있으며 기존의 DDoS 공격이라 해도 완벽한 방어는 현실적으로 불가능 하다. 특히 대역폭을 고갈 시키는 DDoS 공격은 공격 받는 서비스의 서버뿐만 아니라 망 사업자들에게도 큰 손실을 끼친다. DDoS 공격 징후를 신속하게 탐지 하여 대응 하는 것도 중요하지만 공격하는 Zombie의 Source IP를 신속하게 판단하여 차단한다면 더 효율 적으로 DDoS 공격에 대응 할 수 있을 것이다.

6. 참고 문헌

[1] Thomer M. Gil and Massimiliano Poletto, “MULTOPS: a data-structure for bandwidth attack detection”, Proceedings of the 10th USENIX Security Symposium, pp. 23-38, August 2001.

[2] Chan EYK, Chan HW, “IDR: an intrusion detection router for defending against distributed denial-of-service (DDoS) attacks”, Parallel Architectures, Algorithms and Networks, 2004, 10-12 May 2004.

[3] Laura Feinstein, Dan Schnackenberg, Ravindra Balupari, Darrell Kindred, “Statistical Approaches to DDoS Attack Detection and Response”, Proceedings of the DISCEX 2003, 2003.

[4] Arbor Networks. The Peakflow Platform. http://www.arbornetworks.com.

[5] Gaspary LP, Sanchez RN, DWAntunes, and Meneghetti E., “A SNMP-basedplatform for distributed stateful intrusion detection in enterprise networks”, IEEE Journal on Selected Areas in Communications, Vol. 23, No. 10, pp. 1973~1982, 2005

[6] Feinstein L., Schnackenberg D, Balupari R., Kindred D.,"Statistical Approaches to DDoS Attack Detection and Response", DARPA Information Survivability Conference and Exposition(DISCEX 2003), April 22-24, 2003

[7] Wenke Lee, Salvatore J. Stolfo, "Data Mining Approaches for Intrusion Detection," Proc. of the 7th USENIX Security Symposium, pp. 79-94, Jan.1998.