DPI/QoS를 이용한 DDoS 탐지 및 방어 시스템 설계

박현우, 최찬호, 김용훈, 최간호
(주)시스메이트
e-mail:hwpark@sysmate.com

A Design of DDoS Detection and Defense System using DPI/QoS

Hyun-Woo Park, Chan-Ho Choi, Yong-Hun Kim, Gan-Ho Choi
SYSMATE Inc.

요 약

DDoS 공격의 빈도와 규모가 계속 증가하고 있으며 그에 따른 피해와 파급도 커지고 있다. 최근 동향에서 봇넷을 이용한 패킷 플루딩 공격이 여전히 상위 공격순위를 차지하고 있다. 공격유형으로는 TCP SYN, UDP fragment 및 SSDP 플루딩 공격 등이 여전히 강세를 보이고 있다. 이러한 공격들은 source IP가 변조된 악의적인 패킷을 대량으로 발생시켜서 공격대상 네트워크 인프라를 마비시킨다. DDoS 공격 탐지를 위해서는 내부로 유입되는 초당 패킷수와 사용자와 서버간의 연결인 네트워크 플로우수의 변화를 관측하는 것이 필요하며 방어를 위해 트래픽 제어 기술이 필요하다. 이에 본 논문에서는 네트워크 서비스 분석 및 제어 기술인 DPI/QoS 솔루션을 이용한 플로우 기반의 DDoS 탐지 및 방어 시스템을 제안한다. 네트워크 모니터링과 제어를 위하여 사용하던 DPI/QoS 솔루션에 DDoS 탐지 및 방어 기능을 추가함으로써 효율성 및 경제성에서 강점을 가질 것으로 기대한다.

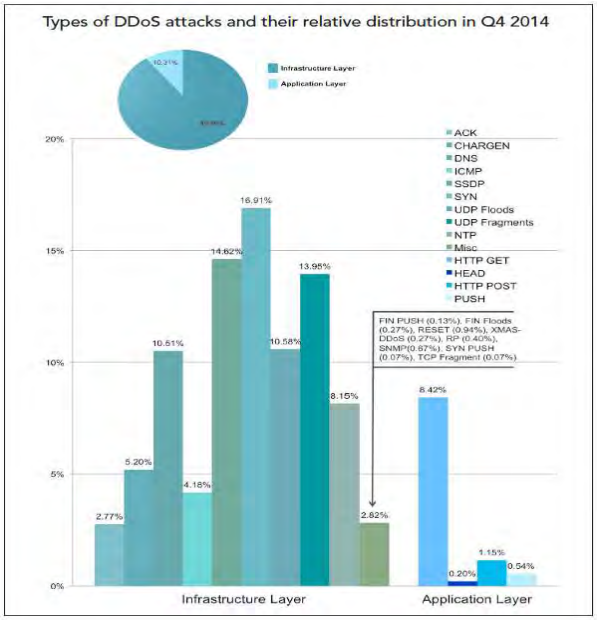
1. 서론

시스템이나 네트워크의 취약점을 이용하여 서비스의 성능을 저하시키거나 중단시키는 DoS(Denial of Service) 공격과 분산된 에이전트들을 동원하여 대상 서비스 뿐만 아니라 네트워크 인프라까지도 마비시키는 DDoS(Distributed Denial of Service) 공격은 투입된 노력에 비하여 막대한 경제적 손실과 이미지 실추를 유발한다[1].

DDoS 공격의 최근 동향을 살펴보면 인프라 레벨의 공격과 어플리케이션 레벨 공격 비율이 9:1로 발생하고 있다. 또한, 인프라 레벨의 공격유형을 살펴보면 SYN floods, SSDP floods, UDP fragment, UDP floods 및 DNS 공격이 상위권을 차지하고 있다. 이에 따라 네트워크 인프라에 대한 플루딩 공격의 탐지와 방어가 중요함을 알 수 있다. (그림 1)은 이를 보여주고 있다.

플루딩 방식의 DDoS 공격에 대하여 임계치 기반의 탐지와 트래픽 제어를 통한 방어 기법이 널리 사용되고 있다[4]. 이러한 탐지 및 방어를 위해서는 라우터의 설정 및 연동이 필요하거나 고가의 전용 장비의 도입이 필요하다.

이에 본 논문에서는 최근 네트워크 모니터링 및 제어를 위해 널리 도입되고 있는 DPI/QoS 장비에 DDoS 탐지 및 방어 기능을 통합하는 시스템의 설계를 제안한다. DPI/QoS의 플로우 및 서비스 분석 기능을 이용하여 DDoS 장비를 통합 개발함으로써 경제성 및 효율성에서 강점을 가질 것으로 기대한다.



(그림 1) 2014년 4분기 DDoS 공격 동향

2장에서는 기존 DDoS 공격유형 분류, 탐지 및 방어 기법에 관하여 기술한다. 3장에서는 제안하는 시스템의 관

이 연구는 2014년 정부(미래창조과학부)의 재원으로 글로벌전문기술개발사업의 지원을 받아 수행되었음 (10044520)

심 공격유형 및 특성을 분석하고 4장에서는 DPI/QoS를 이용한 DDoS 탐지 및 방어 방법을 기술한다. 5장에서는 시스템 설계를 기술하며, 끝으로 6장에서 결론 및 향후 연구과제에 대하여 기술한다.

2. 관련연구

본 장에서는 DDoS 공격유형과 이에 대한 탐지 및 방어 기법에 대하여 요약하여 기술한다.

2.1 공격유형

공격유형 분류는 (1)공격대상의 피해범위를 기준으로 분류하는 방법과 (2)기술적인 공격 특성을 기준으로 분류하는 방법이 있다.

[3]은 (1)의 방법을 기반으로하여 호스트를 대상으로 하는 공격과 네트워크를 대상으로 하는 공격으로 분류하였다. <표 1>은 호스트 대상 DDoS 공격을 보여준다.

<표 1> 호스트 대상 DDoS 공격

대상	종류	특징
L7	HTTP Get Flooding, CC공격, VoIP/SQL/RPC, ...	-공격대상 응용으로 범위 제한 -공격 트래픽 양이 적음, -트래픽 검사하는 방식으로 탐지 어려움
L4	TCP SYN, SYN-ACK, RESET Flooding, UDP Flooding, ...	-특정 호스트의 모든 네트워크 또는 시스템 자체를 마비 -L4 이상의 네트워크 마비
L3	IP Flooding, ARP, ICMP Flooding	-L3 이상의 네트워크 마비

<표 2>는 네트워크 대상 DDoS을 보여주고 있다.

<표 2> 네트워크 대상 DDoS 공격

대상	종류	특징
중요 노드	DNS Lookup Flooding, SYN Flooding, ...	-DNS서버, 라우터, 병목 링크 등의 네트워크 중요 자산 공격
대역폭 소비	UDP Flooding, ICMP Flooding	-한정된 대역폭을 가지는 네트워크 회선 상에 막대한 트래픽을 전송하여 네트워크 마비
하부 공격	Root DNS서버, 대형 백본 라우터, 인증서 서버 등에 대한 공격	-인터넷 망 자체를 마비시키는 공격 -동시다발적인 인터넷 인프라 공격

[4]는 피해범위를 기반으로하여 대역폭 소진공격과 서비스 마비공격으로 구분하고 있다. <표 3>은 이를 보여주고 있다.

<표 3> KISA의 공격유형 분류

비고	대역폭 소진공격	서비스 마비공격
대표 공격	UDP/ICMP Flooding, SYN Flooding	HTTP Get Flooding
공격 형태	UDP/ICMP Traffic Flooding, UDP/ICMP Flooding, DNS Flooding, IP Flooding, ...	HTTP Traffic Flooding, GET Flooding, Get with CC, TCP Connection Flooding, ...
프로 토콜	3~4계층	7계층
공격 대상	네트워크 인프라	웹서버, 정보보호 장비 등
스푸핑 여부	사용/미사용	미사용
증상	회선 대역폭 고갈, 네트워크 마비	서버 장애발생, 시스템 마비

[5]에서도 마찬가지로 피해범위를 기반으로 공격유형을 분류하였다. 이러한 공격대상의 피해범위를 바탕으로한 분류방법은 자산분석과 위협분석을 기반으로한 위험분석을 모델로 하고 있으며 피해규모를 분석하는데 장점이 있다.

[6]에서는 공격 특성을 기반으로 공격유형을 분류하였으며 공격시 정상 세션연결 여부를 기준으로 구분하였다. <표 4>는 이를 보여주고 있다.

<표 4> 공격특성에 따른 분류

비고	정상세션 연결 안함	정상 세션 연결
대표 공격	TCP SYN 등의 TCP기반 Flooding, UDP/ICMP Flooding, 에러 패킷 유발 Flooding	TCP Connectionn Flooding, HTTP Get Flooding, HTTP CC Attack, FTP 취약점 공격 등
공격 증상	-TCP 연결대기 큐 소진 -다양한 패킷 처리로 인한 과부하	-TCP 세션 소진 -HTTP 등 서비스 서버 과부하 -동적 페이지 처리 과부하
프로 토콜	3~4계층	4~7계층

이러한 분류방법은 공격 특성을 이용한 DDoS 탐지와 방어 기법 설계에 장점이 있다.

2.2 탐지 및 방어 기법

본 절에서는 기존 DDoS 탐지 및 방어 기법의 특징과 장단점을 살펴본다.

DDoS 탐지 방법에 관한 연구로 근원지 공격 탐지 기법, 통계적 기법 및 데이터 마이닝 기법 등이 연구되어 왔다[7]. 또한 상용 장비를 기준으로 하여 기존 네트워크 장비를 사용하는 방법, 방화벽 등의 침입 차단장비를 사용하는 방법, 그리고 DDoS 대응 장비를 사용하는 방법 등 주로 3가지 방법이 사용되었다. <표 5>에서 이들의 특징을 보여주고 있다.

<표 5> 기존 DDoS 대응 특징

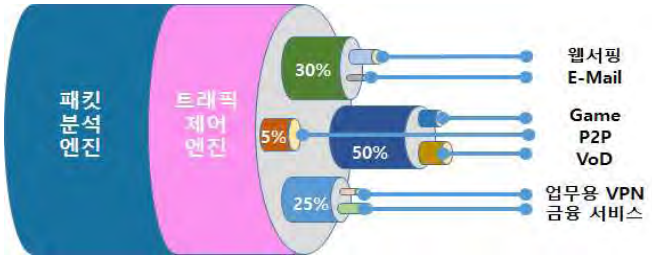
도구	특장점	단점
네트워크 장비	-ACL 패킷 필터링 -Blackholing & Sinkholing -라우터 자체 기능으로 가능	-라우터 과부하 주의 -소스IP 스푸핑 대응 불가 -정교한 방어 어려움 -소규모 망에서 어려움
방화벽	-기존 방화벽 활용	-L7 공격 대응 불가 -소스IP 스푸핑 대응 불가
DDoS 전용장비	-L7 공격 대응 -소스IP 스푸핑 대응	-다른 네트워크 장비와 설치시 패킷 지연 문제 -신규 도입 비용 발생

또한 [8]에서는 사용자 호스트에 위치하면서 패킷카운터와 임계치를 기반으로한 DDoS 탐지 및 방어 시스템이 제안되었다. 이러한 임계치 기반 플루딩 DDoS 탐지 기술은 적은 연산비용으로 효율적인 탐지와 방어가 가능한 장점이 있다.

2.3 DPI/QoS

네트워크 트래픽분석에서 4계층까지의 헤더 분석에 더하여 상위계층에 있는 데이터(페이로드) 부분까지의 정보를 이용하여 서비스를 상세히 분석하는 Deep Packet

Inspection(DPI) 기술과 네트워크 서비스 품질보장 기술인 QoS(Quality of Service)를 합쳐 부르는 용어이며 관련 제품군을 나타내는 용어이기도 하다. 일반적으로 DPI/QoS에서는 DPI를 통한 서비스 상세분석을 통하여 현재 네트워크 상태를 진단한 후 P2P와 같은 과부하 유발 서비스에 대하여 대역폭 제한 등의 제어기술을 이용하여 네트워크 품질을 보장한다.



(그림 2) DPI/QoS 개념도

최근에 DPI/QoS 기술은 인터넷 사업자의 서비스 분석 및 품질 향상, 게임방 등의 사업장에서 네트워크 모니터링, 정보유출 방지를 위한 기업의 네트워크 감시 및 차세대 방화벽 ,IPS 등의 다양한 분야에서 사용되고 있다.

3. DDoS 탐지 및 방어 시스템 설계

3.1 공격유형 분류

본 논문에서 제안하는 시스템의 관심 공격유형은 <표 6>과 같다.

<표 6> 관심 공격유형 분류

대분류	소분류	연번	공격명
비연결	Flooding	1	TCP SYN Flooding
		2	TCP SYNACK Flooding
		3	TCP ACK Flooding
		4	TCP PUSH Flooding
		5	TCP FIN Flooding
		6	TCP RST Flooding
		7	TCP URG Flooding
		8	TCP NULL Flooding
		9	TCP XMAS Flooding
		10	TCP Checksum Error Flooding
		11	UDP Flooding
		12	UDP Checksum Error Flooding
		13	ICMP Flooding
		14	Ping Flooding
		15	IGMP Flooding
		16	IP Checksum Error Flooding
	Anomaly	17	SSDP Reflection
		18	Teardrop Attack
		19	Land Attack
		20	TCP Invalid flags(maerong)
		21	ICMP Unreachable Storm
		22	ICMP Smurf
		23	Ping Sweep
		24	ICMP Ping Of Death
		25	TCP Connection Flooding
연결	Flooding	26	Telnet Flooding
		27	HTTP Get Flooding
		28	HTTP Get with Cache-Control
		29	DNS REQUEST Flooding
	Anomaly	30	HTTP Malformed Packet Flooding
		31	SIP Malformed Packet Flooding
대역폭		32	Volume Flooding

공격유형별 특성을 분석하고 탐지 및 방어 기법을 선정하기 위하여 [6]에서와 같이 비연결, 연결 공격 특성을 기반으로 분류하였다. 이들은 다시 Flooding, Anomaly 분류로 나누어진다. 비연결형/Flooding 공격은 TCP SYN, UDP Flooding 등과 같이 IP 스푸핑에 따른 플로우 세션 급증, 패킷 에러 급증 등의 특징을 가진다. 또한 비연결형 Anomaly 공격은 비정상 패킷이 급증하는 특징을 가진다. 연결형/Flooding 공격은 플로우 세션 증가와 함께 초당 패킷수가 급증하며 연결형Anomaly 공격은 비정상 패킷이 급증하는 특성을 가진다. 비연결 또는 연결 특성에서 분석되지 않는 공격유형들은 트래픽 이상징후 검사를 통한 탐지를 위하여 Volume Flooding 공격유형을 추가하였다.

<표 7> 관심 공격유형별 특징

대분류	소분류	특징
비연결	Flooding	-패킷 에러 급증
	Anomaly	-IP 스푸핑으로 인한 플로우 세션 급증 -비정상 패킷 급증
연결	Flooding	-초당 패킷수 급증 -공격 IP 수집 가능
	Anomaly	-비정상 패킷 급증 -공격 IP 수집 가능
Volume Flooding		-BPS 급증

3.2 DDoS 기능 도출

앞서 도출한 공격유형과 이들의 특성에 따라 다음과 같은 기능을 도출하였다.

3.2.1 에러패킷 차단

에러패킷을 이용하여 시스템 과부하를 발생시키는 공격이나 빠른 공격을 위하여 정상적인 checksum을 계산하지 않은 Flooding 공격을 방어한다.

3.2.2 플로우 세션기반 임계치

비연결형 이면서 IP 스푸핑된 Flooding 공격인 경우 플로우 세션이 급증하는 특징이 있으므로 해당 공격유형 특성을 가진 패킷이 있는 경우 플로우당 1을 설정한 후 탐지모듈에서 IP별 공격의심 플로우를 합산 후 임계치와 비교하여 DDoS 여부를 판단한다.

3.2.3 패킷기반 임계치

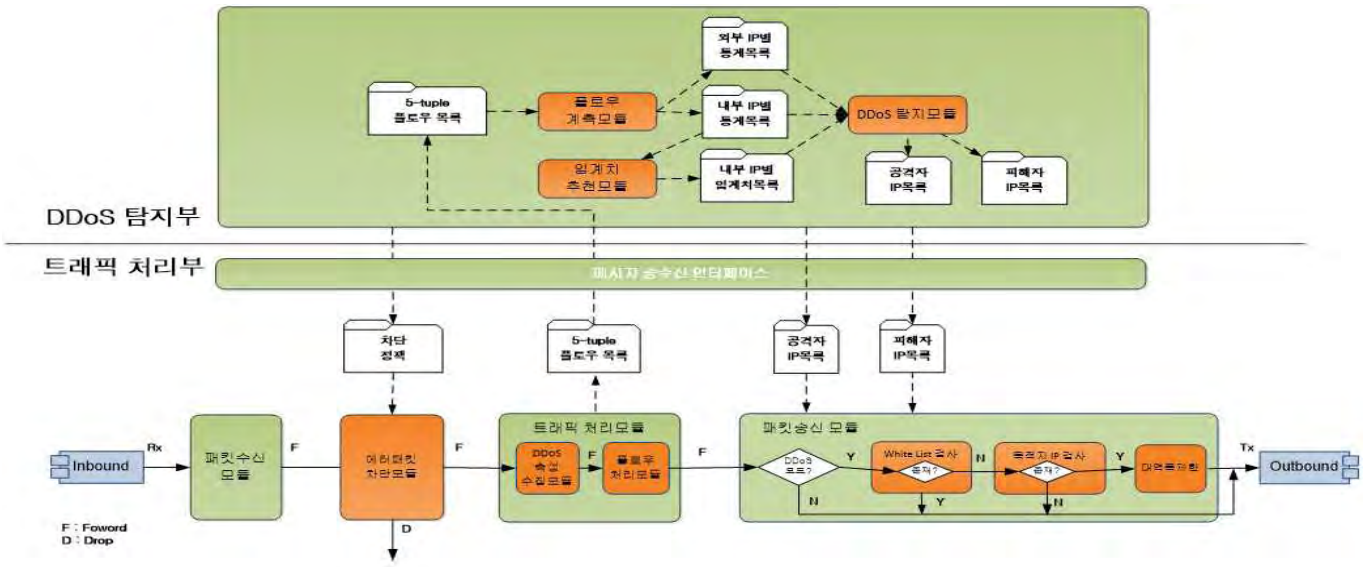
연결형 Flooding 공격인 경우 세션수와 함께 패킷수도 급증하는 특징을 가지므로 플로우별로 15까지 패킷수를 카운팅한 후 탐지모듈에서 IP별로 플로우수와 함께 패킷수도 임계치와 비교하여 DDoS 여부를 판단한다.

3.2.4 피해자 IP 관리

플로우 세션기반 임계치 또는 패킷기반 임계치를 초과한 IP는 피해자 IP 목록에 등록하여 관리한다.

3.2.5 공격자 IP 관리

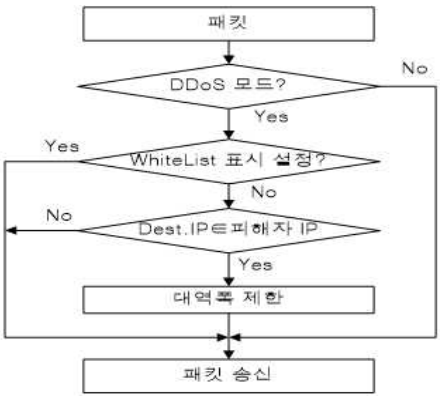
연결형 공격인 경우 Source IP를 관리하여 대역폭 제한 및 좀비 의심 IP 관리에 사용한다.



(그림 3) 시스템 구성

3.3 시스템 구성

본 논문에서 제안하는 시스템은 기존 DPI/QoS 시스템을 기반으로 DDoS 탐지 및 방어 모듈을 추가하여 설계하였으며 트래픽 처리부와 DDoS 탐지부로 나누어진다. 트래픽 처리부는 DPI/QoS 시스템에서 패킷을 수집하여 플로우를 생성한 후 모니터링 서버로 보고하는 기능을 수행하는데 DDoS 탐지를 위하여 플로우 정보에 DDoS 속성 정보를 추가하였다. DDoS 탐지부는 DPI/QoS 시스템에서 플로우 기반 서비스를 모니터링하는 서버에 해당하는 부분이며 DDoS 탐지, 피해자 IP목록 관리 및 하달, 공격자 IP목록 관리 및 하달 등의 기능을 수행을 추가하였다. DDoS 공격이 탐지되면 피해자 IP목록에 등록되어 트래픽 처리부에 하달되고 트래픽 처리부는 DDoS 모드에서 동작한다. 이때부터 유입되는 패킷은 DPI를 통해 잘 알려진 서비스가 분석된 플로우와 그렇지 않은 플로우로 구분되어 대역폭을 제한받는다. 대역폭 제한은 트래픽 처리부의 패킷송신 모듈에서 수행하며 (그림 4)에서와 같이 패킷의 Destination IP가 피해자 IP목록에 속하고 잘 알려진 서비스로 분석되지 않은 플로우인 경우 대역폭을 제한한다.



(그림 4) 대역폭 제한

4. 결론 및 향후 연구과제

최근 DDoS 공격 동향에서 TCP SYN, UDP Flooding 등의 플루딩 공격과 SSDP 등의 증폭 공격이 강세를 보이고 있으며 어플리케이션 공격 역시 유효하게 이용되고 있다. 기존의 네트워크 장비를 이용한 DDoS 방어는 탐지와 방어에서 정밀성이 떨어지며 DDoS 전용장비는 DPI, IPS 등의 기존 장비와 중복사용에 의한 패킷 지연이 늘어날 수 있는 문제점과 중소 사이트인 경우 비용적인 부담이 될 수 있다. 이에 본 논문에서는 기존 DPI/QoS 장비의 플로우 및 서비스 분석 기능과 대역폭 제한 기능을 이용함으로써 패킷 지연시간 증가의 부담을 줄이고 비용 효율적인 DDoS 탐지 및 방어 시스템을 제안하였다. 향후에는 본 시스템의 탐지/방어 성능 평가와 임계치 자동 설정에 관한 연구가 필요하다.

참고문헌

[1] “2013 주요 침해사고 사례와 대응”, KISA, 2013.
[2] “Q4 2014 State of the Internet - Security Report,” Akamai, 2014.
[3] 전용희 외, “DDoS 공격 및 대응 기법 분류”, 한국정보보호학회지, 제 19권, 제3호, 2009.
[4] 인터넷침해사고대응센터, “DDoS 공격대응 가이드”, KISA, 2012.
[5] 양진석 외, “DDoS 공격 실험 결과, 분석 및 피해 완화 방안”, 한국정보처리학회지, 제2권, 제3호, 2013.
[6] “DDoS 최신 공격 기법과 방어 기법”, Ahnlab, 2010.
[7] 김미희 외, “분산 서비스거부 공격 탐지를 위한 데이터 마이닝 기법”, 정보과학회논문지, 제32권, 제3호, 2005.
[8] 김태원 외, “패킷 카운팅을 이용한 DoS/DDoS 공격 탐지 알고리즘 및 이를 이용한 시스템”, 한국시뮬레이션학회 논문지, 제19권, 제4호, 2010.