情報保護學會論文誌
第 22 卷 第 3 號, 2012. 6

다단계 방어기법을 활용한 DDoS 방어시스템 설계

서 진 원,[1†] 곽 진[2‡]
[1]이베이, [2]순천향대학교 정보보호학과

The Design of Anti-DDoS System using Defense on Depth

Jin-won Seo,[1†] Jin Kwak[2‡]
[1]eBay Inc.,
[2]Department of Information Security Engineering, Soonchunhyang University

요 약

2009년 7.7 DDoS 공격은 기존 DDoS공격과는 달리 감염 PC별로 적은 용량의 패킷 전송으로 웹페이지를 마비시켰으며, 또한 HTTP Flooding이라는 공격기법을 활용하여 공격을 성공한 사례였다. DDoS 공격은 시스템을 손상시키는 것이 아니라 일시적으로 서비스의 가용성을 해치는 것이므로, 효과적인 방어를 위해서는 공격자의 공격보다 높은 가용성을 확보하거나, 정확한 방어전략을 실행하여 서비스 시스템의 가용성을 확보하는 방법 등이 있다. 본 논문에서는 기존의 가용량 증설을 통한 방어기법과 달리, DDoS 공격의 특성에 기반하여 공격을 차단하여 서비스 시스템의 가용성을 확보하는 다단계 방어기법을 활용한 웹사이트 전용 DDoS 방어시스템 구축 방안을 제안한다.

ABSTRACT

There were clear differences between the DDoS attack on 7th July 2009 and the rest of them prior to the attack. Despite It had emitted relatively small sized packets per infected PC, the attack was very successful making use of HTTP Flooding attack by aggregating small sized packets from the well sized zombie network. As the objective of the attack is not causing permanent damage to the target system but temporal service disruption, one should ensure the availability of the target server by deploying effective defense strategy. In this paper, a novel HTTP based DDoS defense mechanism is introduced with capacity based defense-in-depth strategy.

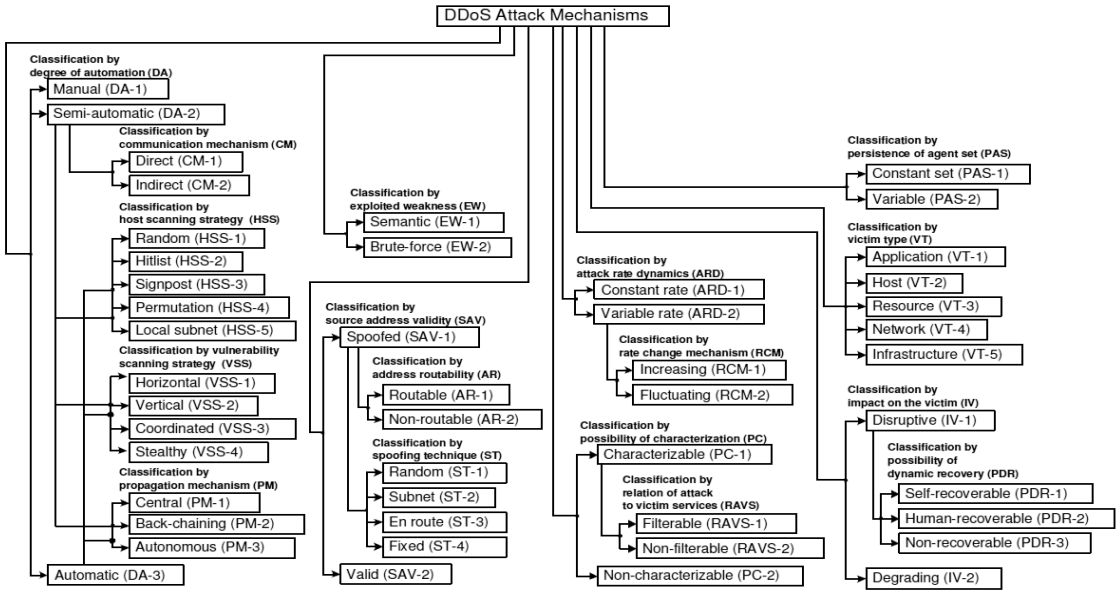
Keywords: DDoS, Defense-in-Depth, L3/L7 Layer defense

I. 서 론

2009년 7.7 DDoS 침해사고 당시, 대부분의 공격 대상 홈페이지는 서비스가 부분적으로 마비되는 심각한 상황이 발생하였다. 당시 많은 기관들이 DDoS 대응장비를 구축하여 운영 중이었음에도 불구하고 DDoS 공격은 기존의 방어체계를 가볍게 무력화시켰고 방어 담당자들은 공격에 속수무책으로 당할 수밖에 없었다. 이 공격으로 인해 기존의 장비위주의 방어로는 신규 외부위협에 대응하기 어렵다는 사회 전반의 자각과 함께 범정부 차원에서 DDoS 공격에 대한 방어 및 대응체계 마련의 필요성이 강하게 대두되었다.

DDoS 공격자들이 실행하는 공격기법은 매우 단순하지만 그로 인한 피해는 상당히 크다. 과거 많은 연구들이 DDoS 공격을 방어하기 위해서는 먼저 공격자들의 DDoS 공격기법을 연구할 필요가 있다고 판단하여 공격기법에 대한 연구를 수행하였다. 그러나 과거의 연구는 공격자의 공격기법만을 나열하는 것에 그쳐

접수일(2012년 4월 19일), 수정일(2012년 6월 14일), 게제확정일(2012년 6월 15일)
† 주저자, happy035@gmail.com
‡ 교신저자, jkwak@sch.ac.kr



〔그림 1〕 DDoS 공격 메커니즘의 분류

서 실제 방어에 활용하기에는 부족한 점이 많았다.

DDoS 공격은 시스템을 변조하거나 저장데이터를 손상시키는 것이 아니라 단지 일시적으로 서비스의 가용성을 해치는 것이다. 그러므로 DDoS 공격을 방어하기 위해서는 첫 번째로 공격자의 공격량보다 높은 가용성을 확보하는 것이 중요하다 할 수 있다. 그리고 두 번째로 공격자의 공격을 지속적으로 차단하면서 서비스 가용성을 확보하는 방법이 있다.

하지만 방어자가 공격자의 공격량만큼 가용성을 확보하는 것은 많은 비용과 시간이 소요되며 또한 공격자의 공격량 예측이 거의 불가능하기 때문에, 사전에 방어용량을 예측하여 충분한 가용성을 제공할 수 있는 시스템을 구축하는 것은 매우 어려운 상황이라 할 수 있다. 그에 반해 공격자가 공격에 사용하는 좀비PC를 확보하는 것은 방어자에 비해서 상대적으로 낮은 시간 비용과 투자비용이 소요된다고 할 수 있다.

두 번째 방법인 효과적인 차단은 공격의 특성을 파악하여 방어하는 방법으로서 공격의 특성을 파악하기 위해서는 현재 발생하는 공격이 무엇인지 정확하게 분석되어야 하지만 많은 DDoS 보안제품들이 다양한 공격유형과 방법에 대해 대응하기에는 한계가 존재한다. 결국 현재 서비스 중인 웹사이트에 가해지는 DDoS 공격이 어떤 기법을 사용하고 있는 것인지를 정확히 분석하지 못하기 때문에 효과적인 방어전략을 수립하기 어려운 것이다.

그러므로, 본 논문에서는 DDoS공격을 방어하기 위해서 현재 발생하는 DDoS 공격유형을 상세하게 분석하고 분석된 결과에 따라 방어전략을 수립하는 다단계 방어기법을 활용한 새로운 DDoS 방어시스템에 대하여 제안한다.

II. 최근 DDoS 공격기법 분석

DDoS 공격기법의 분류에 대해서는 과거 많은 연구가 진행되어 왔으나 방어를 위한 공격기법 상세 분석을 통한 분류에 대한 연구는 미비한 실정이며, 또한 기업이나 기관이 인터넷 서비스를 제공하는 IT 환경은 DDoS 공격에 비하면 매우 소규모의 운영환경이다. 특히 국내의 경우 가정마다 보급된 초고속 인터넷 환경은 역설적으로 공격자에게 매우 양질의 DDoS 공격 환경을 제공하고 있다고 할 수 있다.

"A Taxonomy of DDoS Attack and DDoS Defense Mechanisms"[1] 연구에서는 공격자의 공격 방법(Degree of Automation), 사용 취약점(Exploited Weakness to Deny Service), 발신지 주소 유효성(Source Address Validity), 동적인 공격 규모(Attack Rate Dynamics), 특성화 가능성(Possibility of Characterization) 등으로 구분하여 공격방법에 대해 분류하고 있다.

이 분류법은 일견 상세하게 분류하고 있어 보이나 오직 공격자의 자동/수동 공격과 공격 패킷 형태의 전송 유무만으로 구분을 짓고 있다. 또한, "서비스거부공격(Denial of Service)의 유형 및 대응"[2] 연구에서는 〔표 1〕과 같이 간략하게 구분하는 방법을 제시하고 있다. 이렇듯 대부분의 연구들이 다양한 방식으로 공격기법을 분류하고 있으나, 공격 기법별 방어대책에 대한 연구결과는 매우 미비한 실정이다.

또 다른 연구인 "분산서비스 거부공격 차단 및 분석 기술과 그 특징에 관한 연구"[3]에서는 DDoS 공격에 대해 네트워크 패킷 레벨로 분석하여 공격자가 수행하는 공격의 특징을 분석하였다. 이러한 연구 결과는 DDoS 공격에 대한 방어전략 수립에 일정수준의 가이드를 제공할 수 있을 것으로 분석된다.

그러나, '09년 7.7 DDoS와 '11년 3.4 DDoS에서 사용된 DDoS 공격의 형태는, 기존의 공격유형에 비해 지능화되고 고도화된 형태의 공격이라 할 수 있다. 기존의 공격이 동일한 공격기법을 지속적으로 발생하는 것과 달리 Syn, UDP, ICMP, HTTP Flooding 공격이 동시에 발생한 것으로, 방어자들은 다양한 Flooding 공격과 웹 어플리케이션의 과부하를 동시에 공격하는 유형에 대한 경험이 없는 상황에서 Flooding 공격에 특화된 기존 방어장비가 한계용량을 보임으로써 많은 문제점을 야기한 사례라 할 수 있다.

〔표 1〕 DDoS 공격 유형 구분

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	HTTP 공격	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, DHCP 공격, SQL 공격, Netbios 공격, RPC 공격 등

이렇듯, 동시에 다양한 공격이 발생하는 경우에 대해서 기존의 방어장비가 효과적인 방어를 수행하지 못하면서 새로운 방어기법의 필요성이 제기되고 있다. 그러므로, 본 논문에서는 다양한 유형의 DDoS 공격을 방어하기 위해 방어계층을 다층적으로 구성하는 다단계 방어기법에 대하여 제안한다. 이를 위해 공격자의 DDoS 공격기법과 직접 피해를 입는 네트워크 계층을 응용하여 다단계 방어기법에 활용하도록 한다.

III. 기존 DDoS 방어기법의 문제점 및 요구사항 분석

한국인터넷진흥원(이하 KISA)에서 2004년에 발간한 "분산서비스거부공격 차단 및 분석기술"[4]에서는 국내 대형 통신사인 ISP 차원에서 DDoS 공격 방어를 제안하고 있으며 여기에서는 블랙홀라우팅, uRPF, 싱크홀(Sinkhole) 등의 방법을 제안하고 있다. 그러나 이러한 방법은 주로 L3 Layer인 IP 레벨에서 제어가 가능한 방법으로 SYN/UDP/ICMP Flooding 방법에는 효과적이나 L7 Layer인 HTTP GET Flooding 등은 방어가 불가능하다는 단점을 내포하고 있다.

또한, 장비들간의 협력을 통한 DDoS 방어를 프레임워크 형태로 제안한 연구인 "A Framework for A Collaborative DDoS Defense"[5]에서는, DefCOM 노드라는 장비가 주요역할을 수행하는 구조를 제안하고 있다. DefCOM 노드 장비는 방어 네트워크에 Inline으로 연결되어 있으며, 공격이 탐지가 되면 주변 라우터에게 경고메세지(Alert Message)를 보내어 용량 제어(Rate Limit)를 수행하는 것을 주요 기능으로 제안하고 있다. 그러나 DefCOM 노드는 인입구간이 아닌 네트워크 구간마다 존재해야 하고, 또한 다수의 노드를 네트워크에 Inline으로 설치하기 위한 네트워크의 구조변경 등의 문제점으로 인해 실제 서비스에 적응하기에는 많은 어

려움이 존재한다. 그리고 DefCOM 노드가 발생하는 경고메세지를 기존의 네트워크 장비(라우터, 스위치 등)가 이해하기 위해서는 새로운 프로토콜의 설계가 필요하기 때문에 기존 네트워크 환경과의 호환성 문제도 발생하게 된다. 이와 유사한 연구로는 DDoS 공격을 방어하는 방식으로 라우터들간의 통신을 통한 방어방법을 제안한 "A Defending Mechanism against DDoS Based on Registration and Authentication"[6]이 있다. 그러나 이 연구에서는 방어에 참여하는 모든 네트워크 장비와 서버들에 대한 공개키 설정과 발생, 해당 공개키를 통한 암호화 통신으로 정보를 주고받는 방식을 채택하여 실제 시스템에 적용하기에는 많은 어려움이 존재하며, 이는 결국 DDoS 방어를 위해 라우터들간의 또 다른 표준 프로토콜이 추가적으로 필요하다는 의미를 가지게 되는 것이다.

다른 방법으로는 동적네트워크(Active Network)에서 동작하는 기법으로서 DDoS를 방어하는 방법인 "An Active-Network- Powered Defense Mechanism against DDoS Attacks"[7] 연구 역시 네트워크 토폴로지를 이용하여 DDoS공격을 방어하는 연구라 할 수 있다. 그러나 네트워크가 능동적으로 DDoS 공격에 대한 탐지와 대응을 진행해야 한다는 점 또한 실제 네트워크 환경에서는 아직 동적네트워크가 구현되지 않은 시점에서 많은 문제점을 가지고 있다. 또 다른 연구인 "A Study of Defense DDoS Attacks using IP Traceback"[8]에서는 공격 근원지인 출발지 주소를 확인하기 위한 spoofing IP에 대한 추적 방법을 소개하고 있다.

이렇듯 DDoS 방어를 위해서도 많은 연구가 진행되고 있지만, 최근에 발생한 7.7과 3.4 DDoS 공격 사례에서 볼 수 있듯이 2-3가지의 공격기법으로 공격이 동시에 진행되는 사례에 대한 정확한 분석과 이를 바탕으로 하는 방어전략에 대한 연구는 많이 부족하다 할 수 있다.

그러므로, 본 논문에서는 기존의 DDoS 공격 패킷 형태별 분류방식이 아닌 DDoS 공격이 어떤 네트워크 계층에 영향을 미치는지에 대한 분석을 통해 다단계 방어기법을 활용한 DDoS 방어시스템에 대하여 제안한다.

다음 〔표 2〕는 앞에서 분석한 여러 DDoS 공격기법을 해당 공격이 목표로 삼고 있는 네트워크 계층을 중심으로 재 분석한 것이다. 여기에서 볼 수 있듯이 공격자의 다양한 공격방법은 OSI 3계층과 OSI 7층으로 구분지어 공격을 수행하고 있다. 이것은 두 계층이 인터넷 서비스의 근본이 되기 때문이다. 실제 한국인터넷진흥원이 발간한 "인터넷침해사고 동향 및 분석월보"[9]에서 소개한 DDoS 공격 사례에서도 볼 수 있듯이 공격자의 공격은 L3 대상인 TCP/UDP/ICMP Flooding 공격과 L7 대상인 HTTP GET Flooding이 주를 이루고 있다.

〔표 2〕 각 DDoS 공격기법별 공격 대상 OSI 계층분류

대분류	DDoS 공격 소분류	프로토콜	공격대상 OSI
ICMP/ IGMP Flooding	Broadcast Flooding	ICMP/ IGMP	Layer 3
	Unreachable Storm		
	Ping of Death		
	Smurf		
	Ping Flooding		
	Ping Sweep		
	Multicast	ARP	Layer 2
UDP Flooding	UDP/TCP	UDP/ TCP	Layer 3
	UDP/TCP Port	UDP	
	DNS Reply		
	UDP LoopBack		
	Snork Attack		
TCP Flooding	TCP SYN, NULL	TCP	
	TCP FIN, ACK		
	TCP PUSH, REST		
	TCP URG, XMAS		
	TCP SYN-ACK		
	Land Attack		
	WinNuke		
HTTP Flooding	Valid/INvalid HTTP GET Flooding	HTTP	Layer 7
	GET with CC		
	저대역폭 HTTP DoS		
	Fragmented HTTP Header Attack		
	DNS Query Flooding	DNS	
	Telnet Flooding	Telnet	
	FTP PASV DoS	FTP	

3.1 기존 방어의 문제점

최근의 DDoS 공격기법에 대해 앞에서 분석한 결과를 바탕으로 기존의 DDoS 방어체계가 지니고 있는 보안문제점을 정리하면 다음과 같이 크게 4가지로 정리할 수 있으며, 다음의 보안문제점들에 대해 대응할 수 있는 방어시스템이 구축되지 않을 경우에는 궁극적으로 DDoS 공격에 대해 방어할 수 없다는 것을 의미한다.

3.1.1 다양한 공격 형태가 혼합된 DDoS 공격 대응 문제

7.7과 3.4 DDoS 공격 사례에서 볼 수 있듯이 다양한 공격이 동시에 발생하는 경우에는 기존의 DDoS 장비가 효과적인 방어를 수행하지 못하였다. 이는 기존의 보안장비들이 대용량 트래픽을 처리하는데 중점을 두고 있어서 어플리케이션에 영향을 미치는 공격을 차단할 능력이 부족하였기 때문이다. 다시 말하면 공격의 특성별로 방어를 효과적으로 하는 여러 계층(Layer)의 독립적인 방어체계를 구축해야 한다는 것을 의미한다. IT보안인증사무국에서 발행한 "DDoS 대응장비 보안기능 요구사항"[10]에서도 혼합 공격에 대한 문제점을 인식하고 있어서 DDoS 보안장비가 방어해야 할 공격기법으로 명시하고 있다.

3.1.2 세션 기반 DDoS 공격에 대한 낮은 세션 처리능력

과거의 방어체계는 네트워크의 세션[1]기반으로 방어하지 않고 공격패킷 기반으로 방어를 수행하였다. 그러나 HTTP Flooding 공격은 패킷기반으로 동작하는 것이 아니라 3-Way Handshaking 후에 공격 데이터를 전송하며 이는 필연적으로 TCP 연결 세션을 소모하게 된다. 이를 효과적으로 방어하기 위해서는 웹 서버의 트래픽에서 세션제어를 담당하는 방어계층을 포함시켜서 새로운 DDoS 방어체계를 구축해야 한다.

3.1.3 공격 대상에 대한 가용량 확대의 어려움

DDoS 공격은 공격자와 방어자의 가용량 싸움이라 할 수 있다. 즉, 공격자와 방어자 중에서 더 많은 컴퓨팅 자원을 소유하는 쪽이 공격 또는 방어에서 효과적인 위치를 차지한다고 할 수 있다. 이런 점에서 기존의 방어자들은 공격자의 공격량 보다 더 많은 자원을 확보하는 것만이 최선의 방어라고 생각했다. 그러나 비용을 들이지 않고 공격 인프라인 봇넷(Botnet)을 소유한 공격자와, 장비와 네트워크 증설에 많은 비용이 드는 방어자와의 관계는 처음부터 누가 효과적인 우위를 점하는지에 대해 논할 필요가 없는 부분이었다. 만일 비용문제가 해결된다고 하더라도 공격을 당하는 즉시 원하는 만큼의 가용량을 확보하는 것도 용이한 일이 아니기 때문에 방어자의 어려움이 더욱 크다고 볼 수 있다. 다행히 최근에 주요 화두로 떠오른 클라우드 컴퓨팅 환경을 활용하는 경우 일정수준 해결이 가능하다고 할 수 있다.

3.1.4 HTTP Flooding의 비대칭 트래픽 용량에 대한 응답 문제

HTTP는 서비스 특성상 사용자의 GET 요청보다 서비스 서버가 전달하는 응답 패킷이 월등히 많은 용량을 차지한다. 그러므로 좀비 PC가 지속적으로 GET요청을 하는 경우 트래픽 전송에 비대칭성이 형성되며 지속적인 GET Flooding 공격시 네트워크 가용량을 손상시키게 되어 DDoS 공격이 성공하였다. 최근에도 방어를 위하여 네트워크 회선과 웹서버를 일시적으로 증설을 하는 방식 여전히 많이 사용되고 있지만 효과적인 방어기법인지는 여전히 미지수이다. 방어자가 충분한 비용을 확보하고 있다고 하더라도 무한정의 컴퓨팅 자원을 확보하는 것이 결코 쉽지 않기 때문에 무한정의 서비스인프라의 확충보다 공격 트래픽이 서비스 네트워크로 유입되는 것을 차단하는 방법을 고려하여 방어자의 한정적인 자원을 효과적인 활용이 요구된다.

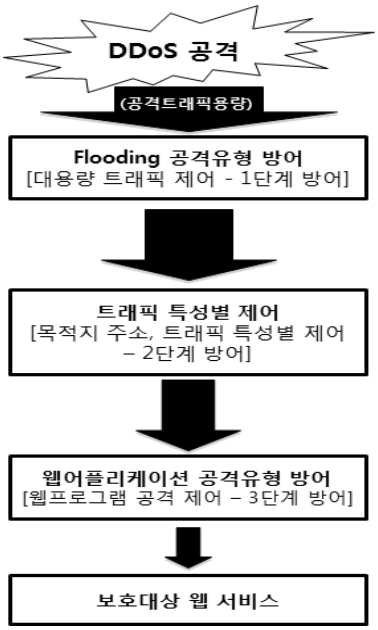
HTTP 통신의 트래픽 비대칭성, 기존 보안장비들의 낮은 세션 처리 능력 등의 다양한 문제 해결을 위해서 본 논문에서는 "다단계 방어기법을 활용한 DDoS 방어시스템"을 제안한다.

IV. 다단계 방어기법을 활용한 DDoS 방어시스템 설계

다단계 방어기법이 추구하는 기본 개념은 여러 계층 장비의 협업으로 DDoS 공격을 방어하는 개념이다. 이는 기존 DDoS 보안장비들이 Anti-DDoS를 표방하나 쉽게 방어하지 못하는 단점을 개선하기 위함이다. 앞서 표 1.에서 살펴보았듯이 각 공격들은 명확히 어떤 OSI 계층을 공격할 것인지를 목표로 삼고 있다. 이러한 공격을 효과적으로 방어하기 위해서는 각 계층별로 방어기제를 구축하고 계층별 데이터 분석을 통한 협업방식의 방어시스템을 구축해야 한다. 다단계 방어기법은 L3 방어계층과 L7 방어계층을 별도로 구축하고 두 계층 간의 정보를 공유하여 DDoS 방어에 활용하는 새로운 개념의 DDoS 방어시스템이라 할 수 있다.

1) 본 내용에서의 세션이란 통신의 시작부터 끝까지 통신당사자가 주고받은 통신 내역을 의미한다.

4.1 다단계 방어기법의 개념



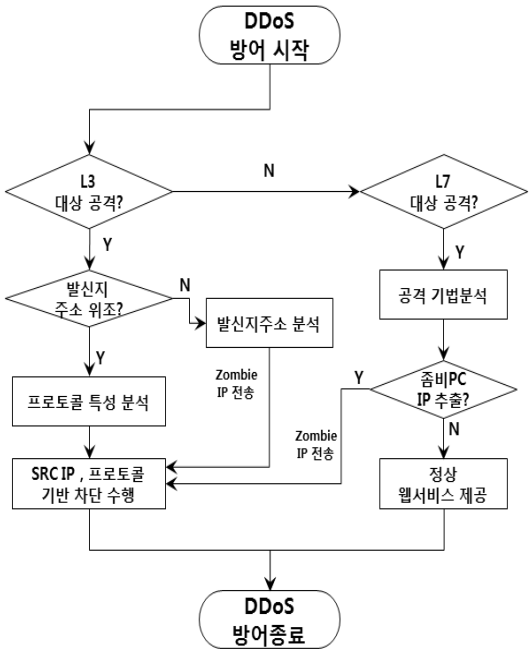
〔그림 2〕 다단계 방어기법의 개념도

앞서 말했듯이 다단계 방어기법은 계층별로 DDoS 공격에 대한 방어를 수행하는 개념이다. 공격 패킷이 상위 계층(L7)으로 가기 위해서는 반드시 하위 계층(L3)을 먼저 통과해야 하기 때문에, L3계층 방어에서 1단계 방어를 수행하고 2단계, 3단계에서 각각 방어를 수행하여 공격자의 공격트래픽을 감소시키는 원리로 방어를 수행하며 DDoS 공격과 방어를 수행하는 네트워크 계층을 연계시키면 아래의 〔그림 3〕과 같다.

앞서도 언급했듯이 DDoS 공격은 누가 더 많이 컴퓨팅 자원을 소유하고 있는지에 대한 공격자와 방어자 간 가용성 싸움이다. 또한 공격자는 서비스에 대한 고민없이 공격만을 수행하지만 방어자는 공격을 방어하면서 정상서비스를 제공해야 하는 어려움을 가지고 있다. 다단계 방어기법은 공격자의 공격을 가장 효과적

L3방어 계층	Layer 3	TCP/UDP/ICMP Flooding filter
		Black list IP filter
L7방어 계층	Layer 7	HTTP Flooding filter
		Web cache & Proxy

〔그림 3〕 공격 및 방어 Layer 연계



〔그림 4〕 다단계 방어기법의 방어 시나리오

으로 방어할 수 있는 최적의 계층에서 공격을 차단하는 방식이며 본 논문은 다단계 방어기법의 방어절차를 〔그림 4〕와 같이 제안한다.

4.1.1 L3계층 방어

L3계층 방어에서는 L3 계층에 대한 공격을 방어하며, 주로 대용량 Flooding 유형의 공격을 방어하는 것이다. L3계층에 해당하는 공격은 TCP, UDP, ICMP, IGMP Flooding 공격 등을 예로 들 수 있으며, 이에 대한 방어기법은 주로 대용량 Flooding 공격을 차단하는 방법을 사용하여 L3 계층에서 방어를 수행하게 된다. 다단계 방어기법은 상위계층(L7)의 공격을 효율적으로 방어하는 것이므로 L3공격에 대한 방어 방법은 다단계 방어 이전의 방어방법을 그대로 차용하여 방어할 수 있다.

4.1.1.1 TCP Flooding 패킷 공격

대용량의 Flooding 공격 시 모든 패킷에 대하여 일일이 발신지를 추적한다는 것은 현실적으로 불가능하지만, TCP는 이에 대한 해결책이 어느 정도 존재한다. TCP 프로토콜이 일정시간 응답이 없을 경우 해당 패킷을 재전송하는 것을 이용하여 국내 대부분의

DDoS 장비제조사는 SYN Flooding에 대한 방어기법으로 First-SYN Drop방식을 차용하고 있다. 즉, 최초에 도착하는 SYN 패킷을 메모리에 저장한 후에 패킷을 Drop시킨다. 이후 정상 세션이라면 다시 해당 발신지 IP에서 SYN 패킷을 재전송할 것이고 보안장비에서는 메모리에 저장된 발신지 IP를 비교하여 해당 패킷을 허용하는 방법을 사용하여 공격을 방어할 수 있다.

4.1.1.2 UDP Flooding 패킷 공격

UDP 패킷은 TCP와 달리 연결지향형이 아니므로 First SYN Drop 기법을 사용할 수 없지만 Stateful Inspection(이하 SI) 방식을 사용하여 패킷을 제어할 수 있다.

SI메커니즘에서는 TCP와 UDP 통신의 처음부터 마지막 세션까지를 모두 메모리에 저장하여 통신을 점검하는 방식으로 UDP 통신 역시 최초 통신내역을 저장한 후에 동일한 IP에서 지속적인 요청이 발생하는 통신내역을 점검하여 공격 여부를 판별할 수 있다. 지속적으로 동일한 IP에서 트래픽이 전송되는 경우는 일반적으로 임계치 설정방식을 사용하여 해당 트래픽을 제어하는 방법을 사용한다.

4.1.1.3 블랙리스트 기반 방어

블랙리스트 기반 방어기법은 문제가 되는 발신지 주소를 추출하여 데이터베이스에 저장한 후에 이를 발신지주소 차원에서 차단하는 방식으로서 방어자 입장에서는 가장 강력한 효과를 볼 수 있다. 다만 블랙리스트가 잘못 구성이 되는 경우 정상 사용자까지 서비스 차단이 발생할 수 있으므로 정교한 블랙리스트를 구축해야 한다.

방어자가 고려해야 할 점은 L3계층에서 볼 수 있는 정보가 IP밖에 없기 때문에 L3계층에서 얻어진 정보만으로는 블랙리스트 구축이 매우 어렵다는 것이다. 단적인 예로서 발신지 주소가 위조된 공격지 주소를 네트워크에서 차단하는 경우 전혀 다른 사용자가 피해를 입을 수 있다. 그러므로 블랙리스트는 해당 발신지 주소가 위조되지 않았으며 확실한 통신주체인 경우에만 찾아낼 수 있다.

다단계 방어시스템에서는 블랙리스트 구축을 위해서 L7 방어계층에서 추출한 감염PC의 발신지 정보를 활용한다. L7방어 계층에서는 HTTP 통신을 수행하여 HTTP통신은 TCP 연결이 모두 완료된 뒤에 시작되므로 발신지 주소의 조작이 불가능하기 때문에 블랙리스트 구축에 정확히 활용될 수 있다.

4.1.2 L7계층 방어

L7계층 방어에서는 공격자의 공격특성을 분류하여 사용자의 요청과 공격자의 공격을 구분하는 기법을 도입하였으며 이는 기존의 DDoS 방어체계와 구별되며 다단계 방어기법에서만 분석 및 적용이 가능한 방어기법이다. 그러므로 다단계 방어기법에서 L7계층의 역할은 방어와 분석이 동시에 진행되고 때로는 블랙리스트 생성을 위한 감염 PC 정보를 추출하는 역할을 수행하며, 이렇게 추출된 감염PC 정보는 L3 계층정보로 전송되어 L7계층으로 공격트래픽이 유입되지 못하게 함으로써 L7계층의 세션용량을 보호하고 서비스 제공에 필요한 가용성을 확보하면서 동시에 정상 사용자의 접속을 제공하는 등의 장점을 가지고 있다.

"사용자 의도 기반 응용계층 DDoS공격 탐지 알고리즘"[11]에서 보면 공격자가 GET 요청을 어떻게 수행하는지 그리고 이를 탐지하여 차단할 것인지를 연구하고 있다. 그러나 해당 연구는 공격자의 공격을 분석하고 해당 공격을 차단하는 방법만을 제시하여 다단계 방어기법이 사용하는 사용자와 감염PC라는 개념을 사용하지는 않고 있다. 다단계 방어기법에서는 공격자의 다양한 공격기법을 위해서 "DDoS 사이버대피소 & 대용량 패킷분석"[12]에서 제안한 기법을 참고하여 L7계층 방어에 활용하였으며 정상 사용자의 요청과 감염PC를 구별하는 방법을 다양한 방식으로 수립하여 다음과 같이 제안한다.

■ **GET Flooding의 임계치 활용** : 다단계 방어기법에서는 웹서비스로 유입되는 GET Flooding을 정상 사용자와 감염PC의 공격으로 구분하기 위해서 CPS(Connection Per Second)라는 개념을 도입하여 방어에 활용한다. 즉, 동일 발신지 주소에서 동일한 서비스 페이지를 초당 몇 번이나 GET 요청을 하는 것인가를 산술적으로 계산하는 것이다. 이는 정상사용자라면 동일한 페이지를 동일한 시간대에 지속적으로 요청하지 않는다는 사용자 패턴에 기반한 개념이다. 다단계 방어기법에서는 CPS값을 임계치로 설정하여 해당 임계치를 초과하는 경우 감염PC의 발신지주소로 간주하고 블랙리스트에 등재하고, 이를 L3 방어 계층으로 전달하여 공격 트래픽의 추가 유입을 차단한다. 그러나 CPS의 임계값이 너무 낮게 설정되는 경우 오탐(False-Positive)이 발생하고 임계치를

너무 높게 설정하면 미탐(False-Negative)이 발생할 수 있다. 또한, 웹사이트의 회선대역폭, 서버가용량 등이 모두 상이하기 때문에 모든 웹사이트에 적용되는 범용적인 CPS값을 추출하기는 쉽지 않기 때문에 임계치 설정에 주의하여야 한다.

■ **HTTP 리다이렉션 코드 활용** : 감염PC와 사용자의 접속을 구분하는 다른 방법으로는 HTTP 리다이렉션 코드를 활용하여 구분하는데 이 방법은 웹서버의 환경 설정으로 손쉽게 구성할 수 있다는 장점을 가지고 있다. 웹서비스를 사용하기 위해서 정상사용자는 웹브라우저를 이용하지만 공격자는 감염PC의 공격프로그램을 사용하게 된다. DDoS 공격이 발생하는 경우 공격대상이 되는 페이지의 파일명을 변경한 후에 공격대상이 되는 페이지에 변경시킨 파일명으로 리다이렉션을 하는 코드를 삽입한다. 이렇게 설정이 완료되면 웹브라우저의 경우 리다이렉션 코드를 수신한 후에 이를 해석하고 신규 페이지를 다시 요청하여 접속하지만 공격자가 사용하는 공격 프로그램의 경우 웹브라우저가 아니므로 리다이렉션 코드를 해석하지 못해 신규 페이지를 요청하지 못한다. 여기에서 리다이렉션 코드가 존재하는 페이지와 리다이렉션 대상 페이지를 모두 접속한 발신지 주소는 사용자의 브라우저라고 볼 수 있으며, 리다이렉션 대상 페이지를 접속하지 못하는 경우 공격자의 감염PC로 간주하여 발신지 IP를 추출하여 차단한다.

■ **CAPTCHA 활용** : CAPCHA(Completely Automated Public Turing test to tell Computers and Humans Apart)란 어떠한 사용자가 실제 인간인지 컴퓨터 프로그램인지를 구별하기 위해 사용되는 방법으로, 인간은 구별할 수 있지만 컴퓨터는 구별하기 힘들게 의도적으로 비틀어 놓거나 그림을 주고 그 그림에 쓰여 있는 내용을 물어보는 방법이 흔히 사용된다.[13] DDoS 공격이 시작되면 공격대상이 되는 페이지를 서비스하기 이전에 CAPTCHA를 제시하고, 이것을 해결한 발신지IP는 사용자의 접속으로 간주하고 그 외에는 공격자의 감염PC로 간주하여 차단하는 방식이다.

이렇듯 L7계층에서는 공격자의 공격을 차단하고 또한 공격에 사용되는 감염 PC를 구분할 수 있는 정보를 제공해주는 일종의 허니팟의 역할도 수행한다. 이는 어떤 공격도 HTTP 프로토콜을 벗어나서는 공격이 성공하지 못한다는 점, 또한 발신지주소를 위조할 수 없다는 점등이 방어를 위한 정보수집에 도움을 주는 것이다. 이는 방어계층을 다단계로 구분하여 해당 단계에서 분석을 수행하고 적합한 방어기법을 제안하는 다단계 방어기법에서만 적용이 가능하고 가장 확실한 DDoS 방어대책이라고 볼 수 있다. 또한 앞서 논의했던 기존 DDoS 공격의 주요이슈가 다단계 방어기법에서는 〔표 3〕에서와 같이 해결됨으로써 기존 장비위주의 DDoS 방어기법과 확실하게 차별되는 방어대책이라 할 수 있다.

4.2 다단계 방어 기법 검증을 위한 시험

4.2.1 시험 환경

이제까지 다단계 방어기법을 활용한 DDoS 방어기법을 제안하였으며 이를 검증하기 위하여 소규모의 시험환경을 구축하고 제안한 기법에 대한 시험을 실시하였다. 시뮬레이션을 위한 환경은 인터넷 환경이 아닌 내부에서 자가로 구축한 시험환경을 사용하였으며 L3 계층 공격과 L7 공격을 구현하기 위하여 국내에서도 널리 활용되는 공격도구를 활용하여 공격을 수행하였으며 전체 시험환경에 사용된 장비 및 환경은 다음과 같다.

〔표 3〕 DDoS 주요 이슈에 대한 다단계 방어기법의 해결 방안

기존 방어의 문제점	다단계 방어기법을 적용한 문제 해결
다양한 공격 유형이 혼합된 DDoS 공격 문제	다단계 방어시스템이 공격에 맞는 방어 filter에서 구분하여 방어하므로 다양한 공격에도 효과적으로 대응
세션 기반의 공격에 대한 낮은 세션 처리 문제	지속적으로 발생하는 좀비PC의 세션요청을 L7 filter에서 분석하고 그 결과를 L3 filter로 전송하여 신규 세션을 차단하도록 함
공격 대상에 대한 신속한 가용량 확대의 어려움	다단계방어기법은 L3/L7 filter에서 탐지한 공격근원지를 IP레벨에서 차단함으로써 회선이나 서버 증설 없이도 가용량 확보 가능
HTTP Flooding의 비대칭 트래픽 용량 문제	비대칭트래픽을 발생시키는 공격 근원지 PC를 IP레벨인 L3 filter에서 차단함으로써 장기적으로 HTTP공격 차단

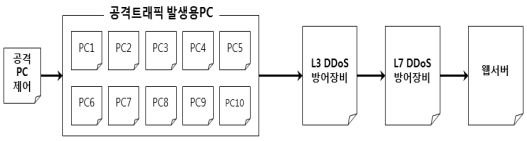
〔표 4〕 테스트 환경 구성 장비

사용장비	수량	용도
PC	가상PC10대	공격 트래픽 발생용
노트북	1대	공격용 PC 제어용
L3 / L7 DDoS방어장비	각 1대	L3/L7 계층 방어용
웹 서버	1대	공격 시험용

〔표 4〕에 명시된 장비를 활용하여 다음과 같이 시험 네트워크를 구성하였으며 네트워크는 외부의 트래픽이 발생하지 않은 폐쇄망으로서 오직 시험환경인 공격트래픽 발생용 PC에서만 트래픽이 발생하는 환경이다.

다단계 방어 기법을 검증하기 위한 시험시나리오는 공격을 수행한 후에 공격에 감행되는 IP를 L7에서 추출하여 L3 계층으로 전달하여 일정수준의 공격트래픽을 방어하는 방식으로서 UDP Flooding과 GET Flooding 기법을 활용하여 시험용 웹서버에 공격 트래픽을 전송하는 시험을 다음의 절차에 의거 진행하였다.

- 환경이 구성된 시험망에 공격트래픽 발생용 PC 10대를 사용하여 UDP Flooding과 GET Flooding 공격을 수행한다.
- 공격트래픽을 발생시킨 IP를 탐지하고 차단하여야 하므로 L3 공격에 2대, L7 공격에 8대를 할당하여 공격 트래픽을 생성하였다.
- 이후 공격트래픽을 일정시간 모니터링 한 후에 좀비PC IP를 추출하여 L3 방어장비로 전송하고 트래픽 변화를 살펴본다.
- 다단계 방어기법을 활용한 방어라면 L3 계층에는 최초 공격이 지속적으로 유입되지만 L7 계층으로 유입되는 트래픽은 앞선 차단정책 때문에 감소한 형태의 그래프가 나타날 것이다.
- 이후 공격을 종료하고 네트워크를 트래픽이 없는 단계로 환원시킨다.

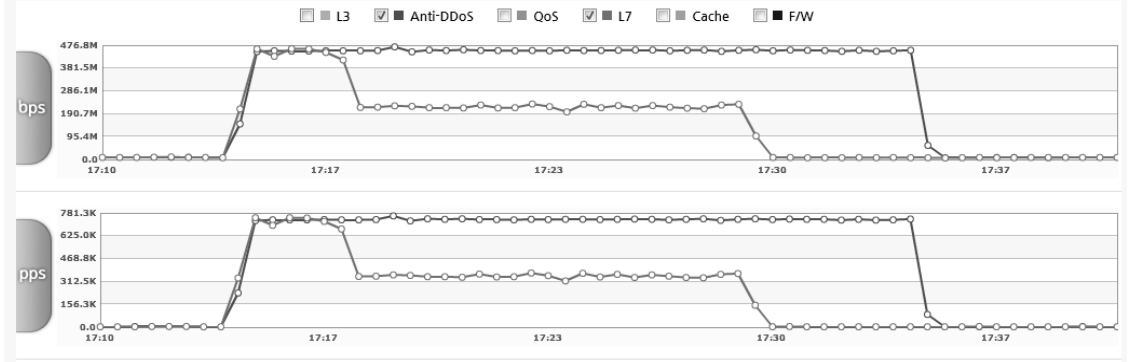


〔그림 5〕 시험환경 네트워크 구성도

시험에 사용한 공격은 HTTP Get Flooding 공격과 UDP Flooding을 동시에 공격하였다. 그래프 초기에는 L3 장비와 L7 장비에서 유사한 트래픽의 부하가 걸리는 것으로 나타나면서 이 공격이 L3 계층을 넘어서 L7계층까지 도달함을 알 수 있다. 이후 L7에서 공격내역을 분석하고 우선 UDP Flooding 공격을 발생시키는 IP를 L3 DDoS 방어장비에 적용하였다. 이후 L3 장비는 여전히 UDP flooding 트래픽 처리를 하고 있지만 L7장비에는 패킷이 도달하지 않음을 알 수 있다. 이후 L7 계층의 트래픽을 기반으로 HTTP Get Flooding 공격을 수행하는 IP를 모두 차단한 경우 트래픽이 L7계층에서는 모두 차단됨을 알 수 있다.

V. 결론

본 논문에서는, 현재 발생하는 DDoS 공격에 대해서 효과적으로 방어하기 위해 공격을 계층별로 방어하는 다단계 방어기법을 활용한 DDoS 방어시스템을 제안하였다. 제안하는 시스템에서는 공격자가 대용량 패킷을 전송하는 SYN, UDP, ICMP Flooding 유형



〔그림 6〕 다단계 방어 기법 적용 결과

에 대해서는 L3계층에서, 또한 HTTP GET Flooding과 같은 어플리케이션 공격은 L7계층에서 방어하는 기법으로써 공격자의 다양한 공격을 동시에 방어할 수 있는 기존 방어와는 차별화된 방어기법을 제안하였다.

특히 L7계층에서는 공격자의 공격과 정상사용자의 접속을 구분하고 이를 방어에 활용하기 위하여 사용자 접근 임계값을 활용하는 방법, HTTP 리다이렉트 코드를 활용하는 기법과 사람과 컴퓨터를 구분하는 CAPTCHAT를 활용하는 방법을 제안하였다. 또한 L7방어 계층에서 구별되어진 감염PC에 대한 정보를 L3방어 계층으로 전송하여 공격을 차단하는 상이한 계층간의 협업을 통한 DDoS 방어기법으로써, 오직 다단계 방어기법에서만 가능한 방어방식으로 기존의 단일 장비 위주의 방어와 차별성을 보여주고 있다.

참고문헌

〔1〕 Jelena Mirkovic and Peter Reiher, "A Taxonomy of DDoS Attack and DDoS Defense Mechanisms," ACM SIGCOMM Computer Communication Review, pp. 39-32, Apr. 2004.

〔2〕 구자현, "서비스 거부 공격(Denial of Service)의 유형 및 대응," *주간기술동향*, 1377호, pp. 6, 2008.

〔3〕 김정윤, 최형기, "분산 서비스 거부 공격과 그 특징에 관한 연구," 제27회 한국정보처리학회 춘계학술발표대회, 14권, 1호, pp.1060~1062, 2007.

〔4〕 인터넷침해사고대응지원센터, "분산서비스 거부 공격 차단 및 분석기술," KRCERT-TR-2004, 한국정보보호진흥원, pp. 17, 2004.

〔5〕 George Oikonomou, Jelena Mirkovic, Peter Reiher, and Max Robinson, "A Framework for A Collaborative DDoS Defense," Proceedings of the 22nd Annual Computer Security Applications Conference, pp. 33-42, Dec. 2006.

〔6〕 Eric Y. Chen, "AEGIS: An Active-Network-Powered Defense Mechanism against DDoS Attacks," IWAN2001, 92001.

〔7〕 Wei Zhang, Shize Guo, Kangfeng Zheng, and Yixian Yang, "A Defending Mechanism against DDoS Based on Registration and Authentication," The 9th International Conference for Young Computer Scientists, pp. 2192-2197, Nov. 2008,

〔8〕 Cheol-Joo Chae, Seoung-Hyeon Lee, Jae-Seung Lee, and Jae-Kwang Lee, "A Study of Defense DDoS Attacks using IP Traceback," 2007 International Conference on Intelligent Pervasive Computing, pp. 402-408, Oct. 2007.

〔9〕 "전문공격단체를 이용한 청부형 DDoS 공격과 대응," 인터넷침해사고 동향 및 분석월보 한국인터넷진흥원, pp. 30-38, 2011년 3월.

〔10〕 "DDoS 대응장비 보안기능 요구사항", IT보안 인증사무국, pp. 3 2010. 1.

〔11〕 오진태, 박동규, 장종수, 류재철, "사용자 의도 기반 응용계층 DDoS공격 탐지 알고리즘," 정보보호학회논문지, 21(1), pp. 39-52, 2011.

〔12〕 이재광, "DDoS 사이버대피소 & 대용량 패킷분석," 코드케이드2011 트레이닝코스 발표, pp. 22-68. 2011.

〔13〕 CAPTCHA, http://ko.wikipedia.org/wiki/CAPTCHA, 2012. 4.

〈著者紹介〉

서 진 원 (Jin-won Seo) 정회원
전북대학교(공학사, 공학석사)
2000년~2003년: 한국정보보호진흥원 평가1팀
2003년~2006년: 한국정보보호진흥원 분석대응팀 연구원
2006년~2009년: 한국정보보호진흥원 해킹대응팀 선임연구원
2010년~2011년: 한국정보보호진흥원 웹보안지원팀장
2011년~2011년: 한국정보보호진흥원 해킹대응팀장
2011년~현재: eBay 글로벌정보보안실 침해사고대응팀 APAC 매니저
2010년 3월~현재: 순천향대학교 정보보호학과 박사과정
〈관심분야〉 DDoS, 침해사고대응, 정보보호제품평가, 클라우드컴퓨팅 보안 등

곽 진 (Jin Kwak) 종신회원
성균관대학교 (공학사 공학석사, 공학박사)
2006년~2006년: 일본 큐슈대학교 방문연구원
2006년~2006년: 일본 큐슈시스템 정보기술연구소 특별연구원
2006년~2007년: 정보통신부 개인정보보호기획단 개인정보보호팀 통신사무관
2007년~2009년: 정보통신연구진흥원 집필위원
2007년~현재: 순천향대학교 정보보호학과 교수
2009년~2009년: 순천향대학교 공과대학 교학부장
2009년~2010년: 순천향대학교 정보보호학과 학과장
2010년~2010년: 교육과학기술부 국가기술수준평가 전문위원
현재 : 정보통신산업진흥원 기술평가위원, 사)국제정보능력평가원 쇼핑몰 플래너 자격 검정 출제 및 채점위원, 한국과학기술정보연구원 충남 과학기술 정보협의회 전문위원, 지식경제부 지식경제기술혁신평가단 평가위원, 순천향BIT 창업보육센터 센터장, 순천향대학교 중소기업산학협력센터 센터장
〈관심분야〉 암호프로토콜, 응용시스템보안, 개인정보보호, 정보보호제품평가, 클라우드 컴퓨팅보안 등