pISSN: 2287-5891

http://dx.doi.org/10.3745/KTCCS.2013.2.3.125

A DDoS Attack Test, Analysis and Mitigation Method in Real Networks

Jin-Seok Yang† · Hyoung-Chun Kim†† · Tai-Myoung Chung†††

ABSTRACT

In this paper, We send DDoS(Distributed Denial of Service) attack traffic to real homepages in real networks. We analyze the results of DDoS attack and propose mitigation method against DDoS Attacks. In order to analyze the results of DDoS Attacks, We group three defense level by administrative subjects: Top level defense, Middle level defense, Bottom level defense. Also We group four attack methods by feature.

We describe the results that average of attack success rate on defense level and average of attack success rate on attack categories about 48ea homepages and 2ea exceptional cases. Finally, We propose mitigation method against DDoS attack.

Keywords : DDoS Attack, DDoS Attack Defense

DDoS 공격 실험 결과, 분석 및 피해 완화 방안

양 진 석† · 김 형 천†† · 정 태 명†††

요 약

본 논문은 DDoS 공격과 유사한 트래픽을 생성하고 ISP를 포함한 네트워크를 통해 실제 운용 중인 웹서버에 전송하여 결과를 분석하였다. 결과 분석을 위해서 대응 장비의 관리 주체에 따라 DDoS 공격의 대응 방법을 ISP(Top), 네트워크(Middle), 시스템(Bottom) 레벨 대응으로 분류하였으며 전송 트래픽을 특징에 따라 4종으로 분류하였다.

실험 결과는 48개 홈페이지의 대응 레벨별 평균 공격 성공률과 공격 분류별 평균 공격 성공률을 기술 및 분석하였으며 2개의 예외 상황에 대해서 기술하였다. 5장에서는 실험 결과를 기반으로 피해완화방안을 제시하였다.

키워드 : DDoS 공격, DDoS 공격 대응

1. 서 론

분산서비스(DDoS) 공격은 목표 시스템에 다량의 트래픽을 전송하여 시스템의 성능 저하 및 마비를 일으켜 정상적인 접근을 방해하는 전통적인 공격 방법이다[11]. 최근에는 시스템 취약점을 이용하거나 소량의 트래픽으로도 공격이 가능한 방법으로 발전하였고, 공격으로 인한 시스템 성능 저하뿐만 아니라 하드웨어 및 파일시스템 파괴 등 공격 방법 고도화 및 피해가 확대되고 있는 실정이다[5, 6].

DDoS 공격의 대응을 위해 많은 연구가 진행되고 있지만 공격 트래픽이 정상적인 트래픽과 유사하고 최근에는 소량의 트래픽을 전송하는 방향으로 진화하여 방어가 매우 어렵다[1, 2, 3, 4, 5 ,6].

본 논문에서는 실제 운용 중인 웹서버에 대해 DDoS 공격을 수행하고 공격 및 대응 결과를 분석한다. 또한 이 결과를 기반으로 공격에 대한 피해를 완화할 수 있는 방안에 대해서 기술한다.

본 논문에서 기술한 DDoS 공격은 대역폭까지의 트래픽을 실험 대상 홈페이지에 전송해보고 홈페이지의 정상 접속 여부 확인을 목적으로 하여 실제 DDoS 공격 트래픽과는 차이가 있지만, ISP(Internet Service Provider)를 포함한 실망에서 운용 중인 실서버가 대상이기 때문에 실험 결과 분석 및 제안한 피해 완화 방안에 대해서 의미가 있을 것으로 판단된다.

본 논문의 2장은 DDoS 공격에 사용한 4종의 공격 분류별 특징과 홈페이지의 대응 방법에 대해서 기술한다. 3장은 공격 방법, 모니터링 등을 포함한 공격 프레임워크에 대해서 기술한다. 4장은 공격 결과 및 예외 상황을 기술하고 이에 대한 피해 완화 방안은 5장에서 기술한다.

† 정 회 원 : 한국전자통신연구원 부설 연구소 선임연구원
†† 정 회 원 : 한국전자통신연구원 부설 연구소 팀장
††† 종신회원 : 성균관대학교 컴퓨터공학과 교수
논문접수 : 2012년 2월 1일
수 정 일 : 1차 2013년 1월 21일
심사완료 : 2013년 1월 21일
* Corresponding Author : Tai-Myoung Chung(tmchung@ece.skku.ac.kr)

2. 공격 및 대응 방법

2.1 공격 방법

DDoS 공격은 다량의 트래픽 전송을 통해 접속을 제한하는 전통적인 공격이다. 본 실험에서는 여러 자원에 대한 DDoS 공격을 수행하기 위해 TCP(Transmission Control Protocol) Connection Flooding 공격, CC(Cache Control) 공격, SQL Query Flooding 공격, Get Flooding 공격, UDP(User Datagram protocol) Flooding 공격, SYN Flooding 공격 등 6종을 선정하였다. 6종의 공격은 통신량 한계 초과, 접속처리 한계 초과, 홈페이지 부하 가중, 응용대상 부하 가중 공격으로 공격대상 홈페이지뿐만 네트워크 및 응용레벨, 운영체제 설정 등에 대한 테스트를 수행할 수 있도록 선정하였다[8].

1) 통신량 한계 초과 공격

통신량 한계 초과 공격은 대량의 트래픽을 전송하여 네트워크에 과부하를 일으키는 공격방법으로 UDP Flooding, ICMP(Internet Control Message Protocol) Flooding 등이 대표적이며 동일 네트워크에서 운영 중인 모든 서버의 접속 장애를 유발하는 특징을 가진다[7, 10].

2) 접속처리 한계 초과 공격

접속처리 한계 초과 공격은 Three-way handshaking을 하는 TCP 프로토콜의 특성을 악용하여 다수의 SYN 패킷을 보내 서버의 연결대기 큐를 고갈시키는 SYN Flooding 공격과 다수의 정상적인 TCP 세션을 생성하여 서버의 CPU 및 메모리 자원을 고갈시키는 TCP Connection Flooding 공격이 있다[8].

3) 홈페이지 부하 가중 공격

홈페이지 부하가중 공격은 Three-way Handshaking을 수행하여 정상적인 TCP connection을 맺은 후, 짧은 시간 동안 반복적으로 웹페이지를 요청하여 웹서버의 과부하를 유발시킴으로써 원활한 웹서비스를 불가능하게 하는 공격 기술로써 일반적으로 GET Flooding 공격이라 부르며 변형된 공격 기법으로 CC Attack, Slowloris Attack 등이 있다[7].

4) 응용 대상 부하 가중 공격

응용 대상 부하 가중 공격은 웹서버에서 동작하는 웹 응용 또는 웹서버 프로그램의 취약점을 이용하여 DDoS 공격을 수행함으로써 웹서버 또는 DB서버에 부하를 가중시키는 공격기술로써, 공격대상 서버에 정상적인 접속을 수행하기 때문에 공격징후를 탐지하기가 쉽지 않고 다양한 형태의 공격기술이 출현할 것으로 예상된다. 특히 실험에서 사용한 SQL Query Flooding 공격은 DB 서버의 부하를 주는 공격 방법으로 홈페이지에서 제공하는 검색 서비스에 SQL Query를 전송하여 부하를 주는 방식으로 기존의 DDoS 공격이 다량의 트래픽을 전송하여 피해를 유발한 반면에 SQL Query Flooding 공격은 소량의 트래픽을 전송하여 피해를 유발할 수 있다.

2.2 대응 방법

DDoS 공격에 대한 대응 방법은 실험 대상 홈페이지에서 적용한 방법에 대해서 기술한다. 50개의 실험 대상 홈페이지는 대부분 DDoS 대응 장비 및 방화벽을 사용하였으나 각 홈페이지마다 여러 가지 대응 기법으로 DDoS 공격에 대응하였다.

1) URL 우회설정

URL 우회설정은 DDoS 대응장비 외에 공격 대상 홈페이지에서 가장 많이 사용한 대응 기법이다.

URL 우회설정은 동일 서버에 메인 페이지를 우회 설정하는 방법과 다른 서버로 우회 설정하는 방법이 있다. URL 우회설정은 구현이 매우 간단하고 대응 효과가 양호하다. 메인페이지의 컨텐츠 크기에 따라 동일서버에 URL 우회설정만으로도 수배에서 수백배의 부하를 줄일 수 있다.

2) 웹가속기 사용

웹가속기는 웹서비스 요청에 대한 응답을 캐싱(caching)하여 처리함으로써 서버에 대한 부하를 감소시키고 특정 컨텐츠는 압축하여 전송함으로써 트래픽 부하를 감소시킬 수 있다. 웹 가속기는 이러한 특성 때문에 원래의 목적이 DDoS 공격 대응이 아니지만 DDoS 공격의 피해를 완화시킬 수 있다.

3) 운영체제 및 웹서버 최적화

운영체제 및 웹서버 최적화는 운영체제나 웹서버의 설정값을 최적화하여 DDoS 공격의 피해를 완화시킬 수 있는 방법을 말한다. 윈도우즈 운영체제의 경우 레지스트리의 TCP/IP 파라미터인 SynAttackProtect 변수 값을 1로 설정하거나 TcpMaxHalfOpen 변수값을 충분히 크게 설정하여 최적화가 가능하다.

4) 로드밸런싱

로드밸런싱은 L4 스위치를 이용하여 구축하는데 2대의 이상의 웹서버를 추가로 구성해야한다. 로드밸런싱은 복수개의 웹서버를 이용하여 트래픽을 분배함으로써 웹서버의 부하를 감소시킨다.

5) Anti DDoS 서비스

Anti DDoS 서비스는 ISP에서 DDoS 대응장비를 구축하여 DDoS 공격에 대한 방어를 제공하는 서비스이다. ISP의 백본 네트워크에서 대용량 트래픽에 대한 모니터링이 가능한 DDoS 대응 장비를 구축하고 DDoS 공격 징후 탐지 시 해당 트래픽을 차단하는 서비스를 제공한다. 이 대응 기법은 DDoS 트래픽이 ISP 레벨에서 차단되므로 대용량 트래픽의 모니터링 및 차단이 가능하다.

6) 회선 이중화

회선 이중화는 두 개의 ISP 회선을 미리 구축하여 회선 하나가 DDoS 공격으로 문제가 생겼을 경우 미리 구축된 다른 하나의 회선을 이용하여 해당 회선을 사용하는 사용자에게 서비스를 지속적으로 제공하는 대응 기법이다. 회선 이중화의 경우 문제가 생긴 ISP 회선을 사용하는 사용자는 홈페이지 접근이 불가능한 단점이 있다.

7) 대역폭 자동전환

대역폭 자동전환은 임계치를 넘어서는 트래픽이 전송될 경우 자동으로 대역폭을 확장하는 방법이다. 예를 들어 해당 홈페이지의 대역폭을 초과하는 트래픽 유입 시 대역폭을 증가시켜 서비스가 지속적으로 가능하게 한다.

8) CDN(Contents Delivery Network) 서비스

CDN서비스는 ISP의 네트워크 하단에 여러 대의 캐시서버(임시저장장치)를 설치한 후 컨텐츠를 캐시서버에 미리 옮겨놓고 사용자의 수요가 있을 때 해당 컨텐츠를 사용자에게 전달해 주는 시스템을 말한다. 캐시서버는 일반적으로 인터넷 사용자가 자주 찾는 정보를 따로 모아두는 서버로, 인터넷 검색을 할 때마다 발생하는 시간을 절약해 주는 네트워크 장비를 말한다. CDN 서비스는 추가적인 설비 및 예산이 투입된다는 단점이 있지만 대용량 트래픽의 부하를 효과적으로 분산할 수 있는 장점이 있다.

3. 공격 프레임워크

Fig. 1에서 보는 바와 같이 실망에서 DDoS 공격 테스트를 위해 테스트 베드를 구축하였다. 공격 트래픽은 트래픽 생성 장비에서 시작하여 ISP를 거쳐 대상 홈페이지의 네트워크를 통과하여 웹서버를 목적지로 하여 전송하였다.

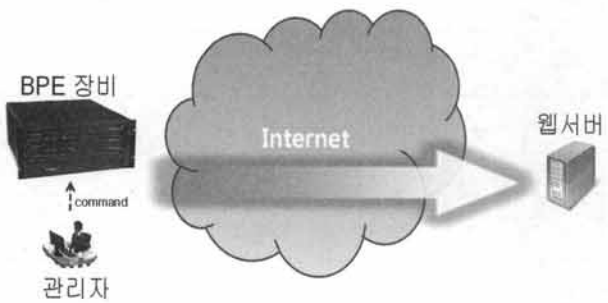

Fig. 1. DDoS attack framework

DDoS 공격 트래픽은 Fig. 1에서 보는 바와 같이 BreakingPoint Elite(BreakingPoint社에서 개발한 트래픽 발생장비)를 이용하여 다량의 트래픽을 발생시킨 후 ISP를 거쳐 공격 대상 홈페이지에 전송하여 부하를 유발하는 방식으로 수행하였다[9].

본 실험에서는 실제 DDoS 공격과 유사한 트래픽 발생을 위해 기존의 공격 패킷을 샘플링하여 트래픽을 생성하였고 약 30,000여개의 공인 IP 주소를 사용하였다.

트래픽 전송량은 홈페이지의 대역폭(ϕ)을 기준으로 Table 1에서 보는 바와 같이 공격의 특징에 따라 구분하여 트래픽을 전송하였다.

전송 트래픽은 실제 운영되는 홈페이지를 대상으로 하였기 때문에 통신량 한계 초과 공격을 제외하고 대상 홈페이지의 대역폭 이상으로 전송하지 않았다. 다만 통신량 한계 초과 공격은 공격의 특징 상 공격 대상 네트워크의 대역폭을 선점하는 공격 방법이므로 해당 홈페이지 대역폭의 약 2배로 전송하였다. 단, 대역폭이 100M 이하인 경우는 공격의 종류와 상관없이 대역폭 정도의 트래픽만을 전송하였다.

Table 1. DDoS traffic amount(if ϕ > 100M)

공격 구분	트래픽 전송량
통신량 한계 초과 공격	ϕ->2ϕ
접속처리 한계 초과 공격	ϕ/4->ϕ/2->ϕ
홈페이지 부하 가중 공격	
응용 대상 부하 가중 공격	ϕ/100->ϕ/10->ϕ/2->ϕ

접속처리 한계 초과 공격 및 홈페이지 부하 가중 공격은 공격 대상 홈페이지 대역폭의 1/4에서 대역폭 정도까지 트래픽을 전송하였다. 응용 대상 부하 가중 공격은 그 특징을 고려하여 대상 홈페이지 대역폭의 1/100 수준에서 전송을 시작하여 대역폭까지 전송량을 증가하였다.

공격 성공 유무의 판단은 해당 홈페이지의 접속 유무를 기준으로 하였다. 홈페이지 접속 유무 판단을 위해 공격 시 사용한 ISP의 유선 라인과 다른 ISP의 유선 라인, HSDPA(High Speed Downlink Packet Access) 및 Wibro (Wireless Broadband)의 무선 모듈 등을 사용하여 총 4개의 모니터링 포인트와 홈페이지 접속 서비스를 제공하는 홈페이지 등 5개의 포인트 모두 접속 불가할 경우 공격 성공으로 판단하였다.

4. 결과 분석

이번 장에서는 48개 홈페이지에 대한 공격 분류별 공격 성공률에 대한 결과 분석에 대해서 기술한다.

DDoS 공격 실험 시 50개 홈페이지를 목표로 실험을 수행할 예정이었으나 2개 홈페이지는 실험 중 네트워크 장비 및 CDN 설정 오류로 인해 실험을 중지하여 결과에 반영하지 않았다. 4.2절에서는 2개 홈페이지의 실험 중단 원인에 대해서 기술한다.

4.1 결과 분석

본 논문에서는 결과 분석을 위해 공격의 대응 주체에 따라 ISP 레벨과 네트워크 레벨, 시스템 레벨로 분류하였다. 대상 홈페이지는 레벨별로 다음과 같은 대응을 수행하였다.

Table 2. Results of DDoS attack testing

홈페이지 No	대응 레벨	접속처리한계		홈페이지 부하가중		응용대상 부하가중	통신량 한계초과	대역폭 (MBytes)
		Connection Flooding	SYN Flooding	GET Flooding	CC Flooding	SQL Injection	UDP Flooding	
1	TMB	1	0	0	0	1	0	200
2		1	1	1	1	1	0	100
3		1	1	0	0	1	0	50
4	TM	0	0	0	1	1	0	1000
5		1	0	1	1	1	0	100
6		1	1	1	0	0	0	50
7		1	0	1	0	0	0	45
8	MB	0	0	1	1	0	0	1200
9		0	0	1	1	0	0	1000
10		1	0	0	1	0	0	1000
11		1	0	0	0	0	0	1000
12		1	0	0	1	0	0	1000
13		1	0	0	0	1	0	1000
14		1	0	0	0	1	0	1000
15		1	0	0	0	1	0	1000
16		1	0	0	0	0	0	1000
17		0	0	0	0	0	0	1000
18		1	0	1	1	0	0	1000
19		0	0	0	0	0	0	1000
20		0	0	0	1	0	0	1000
21		1	0	0	0	0	1	1000
22		1	1	1	0	0	0	1000
23		0	0	1	0	0	0	1000
24		0	0	0	0	0	0	800
25		1	1	1	1	1	0	200
26		1	1	1	1	1	0	155
27		1	1	1	1	1	1	50
28	M	0	0	0	1	1	0	1000
29		0	0	1	1	0	0	1000
30		1	0	0	0	1	0	1000
31		0	0	0	0	1	0	1000
32		0	0	0	0	1	0	1000
33		0	0	1	1	1	0	1000
34		1	0	1	1	1	0	1000
35		1	1	1	1	1	0	1000
36		1	1	1	1	1	0	1000
37		0	0	0	0	1	0	1000
38		1	1	1	1	1	1	1000
39		1	0	1	0	0	0	622
40		1	1	1	1	1	0	400
41		1	1	1	1	1	0	380
42		1	1	1	1	1	1	300
43		1	0	0	1	1	0	200
44		1	1	1	1	1	1	155
45		0	1	0	1	1	1	150
46		0	0	1	1	1	0	100
47		1	0	1	1	1	0	45
48		1	0	0	0	1	0	45

- Top 레벨(ISP 레벨에서 대응 방법)
  : CDN 서비스, Anti DDoS 서비스, 회선이중화, 대역폭 자동전환
- Middle 레벨(네트워크 레벨 대응 방법)
  : DDoS 대응 장비, 로드밸런싱, 웹가속기, 방화벽 등 보안 장비
- Bottom 레벨(시스템 레벨 대응 방법)
  : 운영체제 및 웹서버 설정 최적화, 웹서버 다중화, URL 우회설정

Table 2는 홈페이지별 실험 결과를 나타낸다. 실험 결과는 48개 홈페이지에 대한 대응 레벨, 각 공격별 공격 성공 여부, 대역폭을 나타낸다.

Table 2에서 대응 레벨의 TMB(Top-Middle-Bottom)는 Top 레벨, Middle 레벨, Bottom 레벨로 대응을 수행한 홈페이지, TM(Top-Middle)은 Top 레벨, Middle레벨로 대응을 수행한 홈페이지, MB(Middle- Bottom)은 Middle 레벨, Bottom 레벨로 대응을 수행한 홈페이지, M은 Middle 레벨로만 대응을 수행한 홈페이지를 의미한다.

접속처리한계, 홈페이지 부하가중, 응용대상 부하가중, 통신량한계초과 항목은 정상적인 접속이 불가능하여 공격이 성공한 경우"1"로 표시하였고 정상적인 접속이 가능하여 공격이 실패한 경우"0"으로 표시하였다. 본 실험은 DDoS 공격 후 홈페이지의 정상 접속 여부 확인을 목적으로 진행되었기 때문에 전송 트래픽양은 기록하지 않았다. 대역폭 항목은 홈페이지가 연결된 네트워크의 대역폭을 나타낸다.

Table 3은 Table 2의 각 홈페이지별 실험 결과 데이터를 기반으로 각 대응 레벨에 따른 각 공격별 공격 성공률, 대응 레벨별 평균 공격 성공률과 공격분류별 평균 공격 성공률을 계산하였다.

Table 3의 공격 분류별 평균 공격 성공률을 봤을 때 통신량 한계 초과 공격에 대한 대응은 매우 양호한 것을 볼 수 있다.

반면에 응용 대상 부하 가중 공격의 경우 평균 공격 성공률이 매우 높았고 TMB 레벨에서 공격 성공률이 예상외로 가장 높았다. 이와 같은 결과로 볼 때 응용 대상 부하 가중 공격은 트래픽 전송량이 상대적으로 매우 적기 때문에 임계치를 통한 대응이 아닌 탐지 알고리즘이 정교해야 효율적인 대응이 가능할 것으로 보인다.

또한 응용 대상 부하 가중 공격으로 인해 일부 트래픽이 유입된다 하더라도 시스템 생존성을 위해 반드시 Bottom 레벨을 적용해야한다. 일부 공격 대상의 경우 대역폭의 1/100 정도 트래픽(약 10Mbytes/second)으로도 충분히 공격 성공이 가능함을 실험을 통해 알 수 있었다. Bottom 레벨 적용 시에도 보다 정교한 시스템 최적화가 필요하다.

홈페이지 부하 가중 공격과 접속처리 한계 공격의 경우 잘 알려진 공격임에도 불구하고 예상과 달리 매우 높은 공격 성공률을 보였다. 홈페이지 부하 가중 공격에 사용한 CC 공격은 공격 패턴이 존재하기 때문에 탐지 패턴이 있으면 쉽게 막을 수 있는 공격임에도 불구하고 공격 성공률이 높았다. 또한 TCP Connection Flooding 공격도 다수의 연결이 짧은 시간에 맺어지지 때문에 탐지하는 알고리즘이 있음에도 불구하고 높은 공격 성공률을 보였다. 이는 대응 장비가 존재해도 일부 홈페이지의 경우 탐지규칙을 적용하지 않았거나 설정에 문제가 있는 것으로 볼 수 있다.

다음은 대응레벨별 대한 평균 공격 성공률에 대해서 분석한다.

본 실험을 수행하기 전, TMB 레벨의 대응 기법을 적용한 홈페이지의 공격 성공률이 가장 낮고 M레벨의 대응 기법을 적용한 홈페이지의 공격 성공률이 높을 것으로 예상했다. Table 3에서 보는 바와 같이 M레벨 대응 기법 적용은 예상대로 가장 높은 공격 성공률은 보였다. 그러나 TMB 레벨 대응 기법을 적용한 홈페이지의 공격 성공률이 약 54%로 M레벨과 유사한 공격 성공률을 보였다.

TMB 레벨이 예상보다 높게 나온 이유는 통신량 한계초과 공격을 제외한 3종(접속처리한계, 홈페이지부하가중, 응용대상 부하가중)의 공격이 대역폭 정도의 트래픽을 전송했기 때문에 Top 레벨 대응 기법이 유용하지 않았던 것으로 사료된다. 현실에서 DDoS 공격은 홈페이지 대역폭의 수십에서 수천배 이상의 대용량 트래픽이 발생하기 때문에 TMB 레벨 혹은 TM 레벨 적용 시 효율적인 대응이 가능할 것으로 분석된다.

Table 3. Attack success rate(%)

공격분류 / 대응레벨	접속 처리 한계	홈페이지 부하가중	응용대상 부하가중	통신량 한계 초과	대응 레벨별 평균 공격 성공률
TMB	84	33	100	0	54.25
TM	50	63	50	0	40.75
MB	43	43	30	10	31.5
M	50	67	90	19	56.5
공격 분류별 평균공격 성공률	56.75	51.5	67.5	7.25	

4.2 예외 상황 분석

이번 실험은 총 50개의 홈페이지를 대상으로 진행하였으나 2개 홈페이지는 분석에서 제외하였다. 2개 홈페이지의 실험을 중단했던 이유는 다음과 같다.

• 네트워크 장비의 노후화

라우터 및 스위치 등 네트워크 장비가 노후화되어 트래픽 처리 시 다운되는 증상이 있었다. DDoS 공격은 대응 장비뿐만 아니라 네트워크 장비의 성능도 충분히 고려해해야한다.

• 실시간 데이터를 고려하지 않은 대응 기법 적용

Fig 2는 CDN 서비스 적용 시 실시간 데이터를 포함한 홈페이지의 트래픽을 나타낸다.

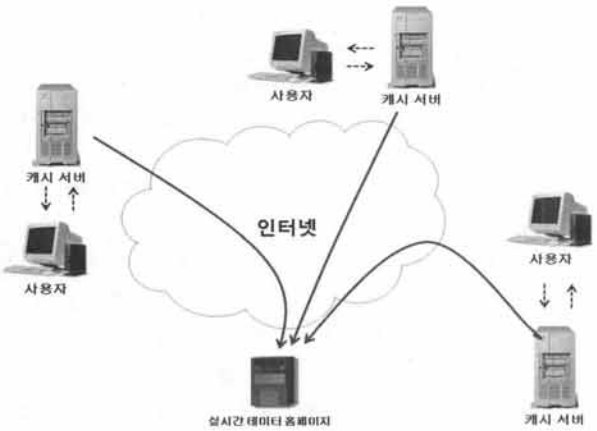

Fig. 2. Traffic of homepage with real-time data using CDN service

Fig. 2에서 보는 바와 같이 일반적인 경우(점선 화살표) 사용자는 캐시서버에 접근하여 데이터를 수신하지만 실시간 데이터를 갖는 홈페이지의 경우 사용자가 데이터를 요청하면 캐시서버는 다시 홈페이지에 데이터를 요청(실선 화살표)하게 되어 실시간 데이터에 대해서는 트래픽 분산 효과가 없게 된다. 결과적으로 DDoS 공격 시 실제 홈페이지로 실시간 데이터 요청 트래픽이 발생하여 시스템이 DDoS 공격을 받는 현상이 발생한다.

실시간 데이터를 고려하지 않은 대응 기법을 적용한 홈페이지도 Fig. 2와 같이 캐시서버의 트래픽 요청 급증으로 인한 홈페이지 서버 이상으로 실험을 중단하였다.

5. 피해 완화 방안

5.1 대응 인프라 구성 방안

DDoS 공격은 정상적인 접속과 유사하기 때문에 패턴이 존재하거나 다량의 트래픽이 유입되는 경우를 제외하면 사실상 완벽한 방어가 불가능하다. 따라서 이번 장에서는 상기 실험 결과를 기반으로 DDoS 공격 피해완화 방안에 대해서 기술한다.

Fig. 3은 DDoS 공격의 피해를 완화하기 위한 다중 레벨 대응의 개념을 보여준다. Fig. 3에서 보는 바와 같이 DDoS 공격에 대한 대응은 반드시 Top 레벨을 포함한 다중 레벨의 대응 방법을 적용해야한다.

Top 레벨 대응 방법은 대규모의 트래픽이 유입되었을 때 ISP에서 이를 탐지 및 차단하여 일정 트래픽 이하로 낮추는 1차 방어선 역할을 한다. DDoS 공격은 그 특성상 대용량 트래픽이 유입되기 때문에 이를 홈페이지에 연결된 대응 장비에서 차단하는 것은 장비의 성능 등을 고려할 때 불가능하다.

Top 레벨에서 공격 트래픽을 1차로 필터링한 후 홈페이지가 운용되는 네트워크에 유입되면 네트워크 레벨의 대응 방법인 DDoS 대응장비 운영, URL 우회설정, 웹가속기 운영, 로드밸런싱 적용, IPS/방화벽 등의 보안 장비 운영 등의 대응을 통해 2차 방어를 수행해야한다. 2차 방어를 수행하지 않고 다량의 트래픽이 유입되면 웹서버는 이를 감내할 수 없다.

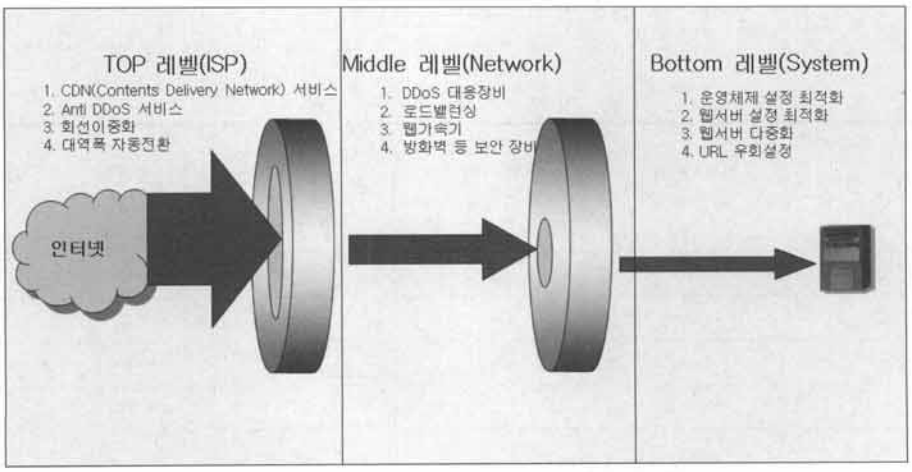

Fig. 3. Concept of multi-level response against DDoS attack

시스템 레벨의 설정은 일종의 쿠션 역할을 수행하게 된다. 홈페이지가 구축된 시스템의 운영체제 및 웹서버의 설정값을 최적화하면 2차 방어 후 유입되는 트래픽을 흡수할 수 있고 평상시에도 사용자에게 빠른 응답을 줄 수 있다.

각 레벨별 탐지률 설정은 평소 트래픽과 홈페이지의 특징을 고려하여 반드시 전문가가 설정해야한다.

위와 같은 사항을 고려하여 A 홈페이지는 다중레벨 대응 개념을 이용한 DDoS 공격 대응 완화 기법을 다음과 같이 적용할 수 있다.

1. TOP 레벨(ISP 레벨) : CDN 서비스
2. Middle 레벨(네트워크 레벨) : DDoS대응장비, URL 우회설정
3. Bottom 레벨(시스템 레벨) : 웹서버 설정 최적화

다중레벨 대응 기법은 매우 이상적인 DDoS 피해 완화 방안이기 때문에 비용이나 인력 등의 문제로 대응 방법을 적용하기 어려우면 아웃소싱을 통해 대응 서비스를 제공받는 것도 좋은 방법이다.

5.2 예외 상황에 대한 대응 방안

DDoS 공격에 대한 대응 방안은 4.2절에서 기술하였던 예외 상황도 반드시 고려해야한다.

네트워크 장비 노후화는 네트워크 장비의 다운으로 공격 대상 네트워크 전체를 마비시킬 수 있기 때문에 절적한 성능을 가진 네트워크 장비를 운용해야한다.

CDN 서비스 적용 시 실시간 데이터를 메인 페이지에 놓이지 않도록 홈페이지를 설계해야한다.

이 외에도 응용대상 부하 가중 공격인 SQL Query flooding 공격은 공격의 특성상 소량의 데이터로도 공격이 가능하기 때문에 이에 대한 대응 방안이 필요하나 네트워크 레벨에서 이를 탐지하기는 쉽지 않다. 특히 대역폭이 큰 네트워크에서 임계치 기반의 탐지를 수행하는 경우 네트워크 보안 장비의 임계값도 상대적으로 크게 설정하기 때문에 더욱 그러하다. 또한 공격 패킷의 패턴도 없어 탐지가 쉽지 않다. 따라서 응용대상 부하 가중 공격의 경우는 Bottom 레벨의 대응 방안을 적용하는 것이 최선의 방법으로 사료된다.

이번 장은 실험 데이터를 기반으로 피해 완화 방안에 대해서 기술하였다. 상기 기술한 공격 기법과 피해 완화 방안은 실험 결과와 더불어 각 홈페이지 관리자에게 전달하였다.

6. 결 론

본 논문은 DDoS 공격과 유사한 트래픽을 실험 대상 홈페이지에 전송하고 이에 대한 결과 분석 및 피해 완화 방안을 기술하였다.

현재까지 실서버와 실망을 대상으로 DDoS 공격 실험을 수행한 사례가 없다. 본 실험 결과는 실서버를 공격 대상으로 실망에서 수행하였기 때문에 의미가 있다고 판단된다. 또한 실험 후 각 홈페이지 관리자에게 공격 기법 및 대응 방안을 제시하여 홈페이지의 피해를 완화하는데 도움을 줄 수 있었다.

특히 실험 결과 중 예외 상황분석에서 기술하였던 실시간 데이터를 고려하지 않은 CDN 서비스 적용이나 매우 소량(약 10Mbytes/second)의 트래픽으로도 DDoS 공격이 가능하다는 것을 실험으로 확인하였다.

본 논문의 실험은 유선 네트워크 환경에서 이루어졌기 때문에 대역폭이 상대적으로 적은 무선 네트워크 환경은 고려하지 않았다. 향후 이번 실험의 데이터를 기반으로 무선 네트워크 환경으로 확장하고 진화된 DDoS 공격을 고려한 대응 방안에 대한 연구를 진행할 것이다.

참 고 문 헌

[1] 2010 White paper of National Information Security, KISA, 2010.

[2] 2011 White paper of National Information Security, KISA, 2011.

[3] 3.4 DDoS Special report, Ahnlab, 2011.

[4] Jin-tae Oh, et al., "A Novel Application-Layer DDoS Attack Detection Algorithm based on Client Intention", Journal of the KIISC(Korea Institute of Inforamtion Security and Cryptology), Vol.21, No.1, pp.39-52, 2011.

[5] Tai-jin Lee, et al., "Light-weight Defense Mechanisms for application layer DDoS Attacks in the Web Services", Journal of the KIISC, Vol.20, No.5, pp.99-110, 2010.

[6] Ki-Hun Jang, et al., "Smartphone DDoS Attack trend", Review of KIISC, Vol.21, No.5, pp.65-70, 2011.

[7] Yong-Hee Jeon, et al., "Classification of DDoS Attack and Response techniques", Review of KIISC, Vol.19, No.3, 2009.

[8] The lastest DDoS Attack and Defense techniques, Ahnlab, 2010.

[9] Dustin D. Trammell & Todd Manning, "Simulating Distributed Denial of Service with BreakingPoint Storm CTM", White Paper, BreakPoint Systems.

[10] Jelena Mirkovic, Peter Reiher, "A Taxonomy of DDoS Attack and DDoS Defense Mechanisms", ACM SIGCOMM Computer Communication Review, Vol.34, Issue 2. ISSN:0146-4833, April, 2004.

[11] Wikipedia, http://ko.wikipedia.org/

양 진 석

e-mail : jsyang@ensec.re.kr

2003년 성균관대학교 정보공학과(학사)

2005년 성균관대학교 컴퓨터공학과(석사)

2011년 성균관대학교 컴퓨터공학과(박사수료)

2005년~현 재 한국전자통신연구원 부설 연구소 선임연구원

관심분야 : Network Security, Cloud Computing Security

김 형 천

e-mail : khche@ensec.re.kr
1999년 고려대학교 전산학과(학사)
2001년 고려대학교 일반대학원 전산과학전공(석사)
2011년 고려대학교 정보보호대학원 정보보호 전공(박사)
2001년~현 재 한국전자통신연구원 부설 연구소 팀장
관심분야 : Network Security, Software Security, Cloud Computing Security

정 태 명

e-mail : tmchung@ece.skku.ac.kr
1981년 연세대학교 전기공학과(학사)
1984년 일리노이주립대학 전자계산학과 (학사)
1987년 일리노이주립대학 컴퓨터공학과 (석사)
1995년 퍼듀대학교 컴퓨터공학과(박사)
1995년~현 재 성균관대학교 컴퓨터공학과 교수
관심분야 : 통합보안관리, 네트워크, 무선망