10Gbps 분산서비스거부(DDos) 공격 탐지 엔진 구현

오진태*, 장종수*
*한국전자통신연구원
e-mail : showme@etri.re.kr, jsjang@etri.re.kr

An Implementation of 10Gbps DDoS Detection Engine

Jintae Oh* and Jongsoo Jang*
*Electronics and Telecommunication Research Institute

요 약

지난 3 월 3 일 발생한 분산서비스 거부 공격의 경우 보안 패치 업데이트를 방해하는 현상이 신고되어 공격 시작 전에 악성코드가 분석됨으로 초동 대응이 가능하였다. 하지만 일반적인 분산서비스 거부 공격은 이러한 초동 분석이 불가능한 경우가 대부분이다. 따라서 네트워크에서 공격 트래픽을 효과적으로 탐지 차단하는 DDoS 탐지 엔진이 필요하다. 또한 빠른 트래픽 증가로 인하여 10Gbps Ethernet 사용이 일반화 되고 있고, 이미 수 백 Gbps 의 공격 트래픽이 수시로 발생하고 있다. 본 논문에서는 선로 속도 10Gbps 성능의 분산서비스거부 공격 탐지 칩 셋의 구현에 대해 기술한다. 칩 구현을 위한 고려 사항, 엔진 구조, 하드웨어 합성 결과 및 시스템에 장착된 칩의 성능에 대하여 소개하고자 한다.

1. 서론

네트워크와 컴퓨터 기술의 발전은 다양한 멀티미디어 서비스를 가능하게 하였고 특히 최근 몇 년간 스마트폰에 인한 트래픽이 빠르게 증가하고 있다. 또한 최근 단말들은 멀티코어 프로세스를 장착한 CPU를 사용하게 되었고, 단말의 컴퓨팅 성능은 더 강력한 사이버 공격에 악용되고 있다. 우리에게 잘 알려진 사이버 공격중의 하나가 분산서비스거부(DDoS) 공격이다[1]. 분산서비스거부 공격은 분산된 클라이언트에서 과도한 트래픽을 발생하여 서버가 오작동하게 하거나, 정상적인 서비스를 제공하지 못하도록 하는 일종은 사이버 공격이다. 또한 분산서비스거부 공격은 네트워크 좀비를 통한 Bot 기술에 의하여 더욱 강력한 공격이 가능해졌다. Bot에 감염된 컴퓨터 사용자는 자신의 컴퓨터가 좀비로 악용된다는 사실을 인지하지 못하는 상황에서 C&C 서버의 제어를 받아 공격에 악용되고 있다 [2, 3, 4]. 이미 백본 네트워크 및 대규모 ISP 들은 10Gbps 네트워크의 사용이 일반화되었으며, 망으로 유입되는 DDoS 트래픽을 탐지/차단하기 위한 10Gbps 성능의 대응 시스템들을 필요로 하고 있다. 또한 DDoS 공격의 경향이 Syn flooding, UDP flooding, ICMP flooding등의 네트워크 공격뿐만 아니라 Get flooding 이나 CC attack과 같은 응용계층 공격이 증가하고 있으며, 이들 공격들이 혼합된 형태의 복합 공격들이 발생하고 있어 단순한 임계치 기반의 대응 방법으로는 대응에 한계를 보이고 있다[5, 6]. 또한 공격 기법이 다양화되고 있어 트래픽 전수 분석에 의한 공격 탐지기법이 개발되어야 할 것이다.

본 논문은 Syn flooding 부터 CC attack까지 다양한 공격을 실시간 전수 분석할 수 있는 하드웨어 기반의 DDoS 탐지 엔진에 대한 것이다. 본 엔진을 구현하기 위한 요구사항을 제시하고 각 기능 블록을 HDL (Hardware Description Language)로 구현하여 합성한 결과를 소개하고자 한다. 또한 본 엔진을 장착한 20Gbps DDoS 대응 시스템의 실험 결과를 제시하여 선로 속도의 DDoS 공격 탐지 및 대응 요구사항을 만족하는 엔진이 개발되었음을 보이고자 한다.

본 논문의 2장에서는 DDoS 탐지 엔진의 실시간 데이터 처리를 위한 요구사항에 대해 기술할 것이며, 3장에서는 엔진의 구조에 대해 논한다. 4장에서는 HDL 합성 결과와 실험 결과를 보이고, 5장에서 본 논문의 결론을 맺고자 한다.

2. 10Gbps DDoS 탐지 엔진 요구사항

이미 수년 전부터 10Gbps Ethernet 사용이 일반화되고 있다. 또한 10Gbps POS(Packet Of SONET)를 주로 사용하는 ISP 들도 장비 사용 연한이 다하면 10Gbps Ethernet 을 도입하려는 움직임을 보이고 있다. 또한 Anti-DDoS 장비 등을 도입하려는 많은 망이 10Gbps Ethernet 을 사용하는 경우가 많아 10Gbps 의 선로 속도에서 동작되는 Anti-DDoS 장비에 대한 요구가 증가되고 있다. 하지만 현재의 10Gbps Anti-DDoS 장비들은 선로 속도로 패킷을 분석하지 못하는 경우가 대부분이다. 또한 공격 기법의 정교화로 인하여 과거 단순한 임계치 기반의 탐지 기법으로는 공격을 효과적으로 막아내지 못하는 것이 현실이다. 따라서 10Gbps 속도의 패킷 처리 성능이 보장되는 DDoS 탐지 엔진 개발이 요구된다. 또한 TCP 세션을 이용한 공격을 탐지하고 차단하기 위해서는 최소 수백만 세션을 동시

에 추적하고 관리할 수 있는 세션 관리 기능이 요구된다. 이러한 세션 관리 기능은 먼저 TCP 프로토콜을 이용한 공격에 효과를 볼 수 있다. 이를 위해서는 특정 서버를 향하는 패킷의 IP 정보를 Flow 테이블로 관리해야 한다. 또한 UDP 나 ICMP 처럼 세션을 갖고 있지 않는 프로토콜에 대한 DDoS 공격을 탐지하기 위해서 Flow 테이블을 활용해야 한다. 또한 각 호스트의 접속 이력을 관리하여 spoof 된 IP 에서 발생하는 공격 패킷들을 차단하는 기능이 필요하다. HTTP Get 등의 응용계층 공격은 대부분 TCP 프로토콜을 이용하므로 이들 공격을 탐지하기 위해서는 TCP 세션 테이블을 필요로 한다. 하지만 기본적인 TCP 세션 테이블은 세션의 시작과 종료에 대한 정보만이 관리된다. 하지만 HTTP Get 공격을 세션 단위의 접속 의도 기반의 DDOS 탐지를 위해서 세션 테이블에 접속 의도에 대한 정보를 관리하는 기능이 필요하다. 또한 특정 호스트의 접속 의도를 분석하는데, 한번의 비정상적인 접속 의도 만으로 공격으로 판단하는 경우 오탐이 발생할 수 있으므로 특정한 시간 간격 동안 발생한 이벤트 수를 관리하기 위해 이벤트 테이블이 필요하다 [7].

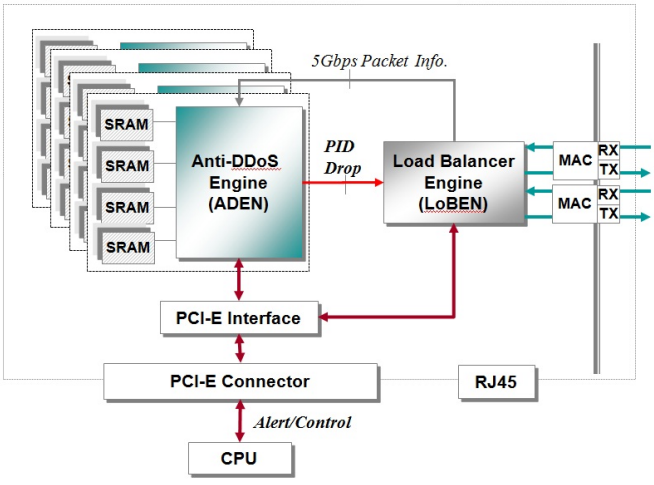
표 1 에서 보는 바와 같이 L3 계층에서 발생하는 다양한 공격 중에 IP spoofing 된 경우와 fragment 된 공격도 찾아 낼 수 있어야 한다. L7 계층의 경우 HTTP 웹 서버를 대상으로 하는 공격을 탐지하고 대응 할 수 있어야 한다. 20Gbps DDoS 대응 시스템은 최대 800 만개의 세션을 관리하고, 세션을 spoofing 할 수 없는 응용계층 HTTP Get 공격은 공격자 IP 를 자동 차단하기 위하여 200 만개의 자동 ACL 을 지원하도록 하였다. 또한 양방향 10Gbps 처리속도를 지원하며, 50usec 이하의 지연시간을 갖도록 설계되었다.

<표 1> 20Gbps DDoS 대응 시스템 성능

항목			성능치
탐지 및 대응	L3	Spoofed/non-spoofed UDP/ICMP/TCP/IP	임계치 및 접속 이력 관리를 통한 DDoS 공격 탐지 및 대응
		Combined UDP/TCP/ICMP	
		Spoofed/non-Spoofed UDP/ICMP Fragments	
	L7	HTTP GET	세션단위 서버 접속 의도 분석 기술을 통한 공격 탐지 실시간 대응 : 200 만개 ACL 대응
		CC Attack	
		Incomplete Get Attack	
		Multiple Get request	
일반 특징		CPS	초당 100 만 세션
		Max Connection	최대 800 만 세션
		Throughput	양방향 10Gbps 지원
		Latency	50 μs 이하
		대응 방식	In-Line, Out-of-Path

3. 시스템 구조

20Gbps DDoS 대응 시스템은 그림 1 과 같은 구조로 설계되었다. 그림 1 의 오른쪽에 10Gbps 두 포트를 수용하며, 시스템에서는 총 20Gbps 의 패킷을 처리한다. 또한 본 시스템은 L3 에서 L7 까지의 트래픽을 분석하여 DDoS 공격을 탐지한다. 특히 HTTP Get 또는 CC 공격의 경우 패킷의 페이로드를 분석해야 공격을 탐지 할 수 있으며, 모든 패킷의 세션을 유지하고 관리하기 위한 세션 테이블이 디자인의 병목이 되고 있다. 세션 테이블을 TCAM 을 활용하여 구현 할 수 있으며, TCAM 의 동작 속도를 고려하면 하나의 칩에서 20Gbps 성능의 엔진을 구현 할 수도 있겠으나, 동시 처리해야 하는 세션 수, 동시 flow 수, white list 수, 그리고 ACL 개수 등을 고려하면 소요되는 TCAM 이 너무 많고 이를 제어할 칩의 핀 수가 부족하다. 따라서 현재 제공되는 FPGA 와 SRAM 으로 이러한 테이블들을 구현하도록 하였다. 현재 가장 빠른 SRAM 은 약 200Mhz 의 동작 속도를 가지고 있으며, 32 비트의 버스를 제공하여 있다. 따라서 5Gbps 트래픽을 처리하는 엔진을 분산하여 설계하는 경우 20Gbps 트래픽을 처리 할 수 있다. 이러한 고려 사항을 반영한 시스템의 구조를 그림 1 에 보였다. 그림 1 의 LoBEN 은 20Gbps 트래픽을 4 개의 탐지 엔진으로 분배하는 기능을 수행한다. 탐지 엔진은 각각 5Gbps 의 트래픽을 실시간으로 처리하는 기능을 수행한다. 또한 ADEN 은 4 개의 SRAM 이 연결되어 있으며, 각각 세션 테이블, flow 테이블, white list 테이블, 그리고 ACL 테이블로 사용되고 있다. 표 1 에 보인 탐지 및 대응 기능은 ADEN 에서 수행된다. 또한 탐지된 결과와 특정 패킷은 PCI-E 접속을 통하여 CPU 로 전달되고 분석되며, CPU 에서 대응 정책을 내려 패킷들을 차단하는 기능을 수행한다. 관리 기능에는 로그 관리 기능과 상세 분석 기능이 수행된다. 모든 탐지 및 대응 기능이 하드웨어 칩으로 구현되었지만, 상세한 분석이 필요한 공격을 추가로 찾기 위해 특정 패킷을 소프트웨어로 분석하는 기능을 갖고 있다.



(그림 1) 10G DDoS 대응 시스템 하드웨어 구조도

4. 칩 합성 결과와 성능

LoBEN 은 단순한 패킷 분배 기능을 수행하며, 패킷 버퍼링 기능만을 수행하므로 공격 탐지 대응 기능을 수행하는 ADEN 칩의 합성 결과와 시스템의 탐지/대응 성능에 대해서만 기술하고자 한다.

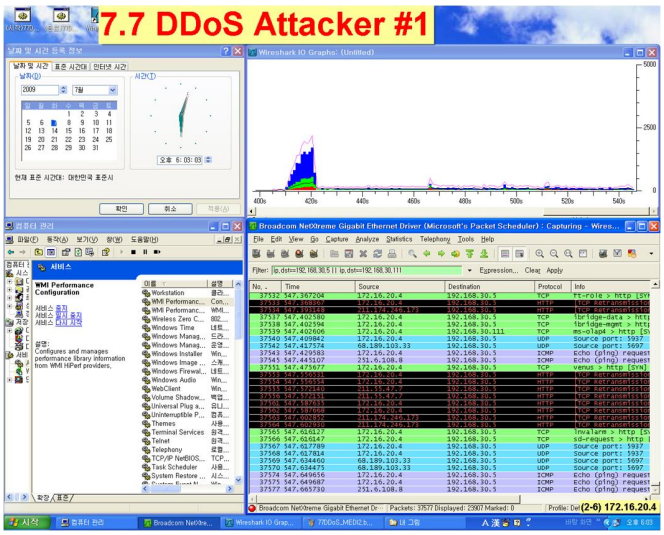
ADEN 칩은 Verilog HDL 로 구현되었다. LoBEN 칩과 ADEN 칩은 64 비트 100Mhz 속도로 연결되어 6.4Gbps 의 전달 속도를 갖는다. ADEN 내부에서 데이트는 32 비트로 처리되고 있으며, 166Mhz 클록으로 동작되는 경우 5.3Gbps 의 처리 성능이 보장된다. 최소 패킷 사이즈는 64 바이트이며, ADEN 에서 최소 크기 패킷을 처리하기 위해서 모든 룩업 테이블의 룩업 시간은 16 클록 이내에 처리하도록 하여 실시간 처리가 가능하도록 구현되었다. 또한 HTTP Get 등의 공격을 탐지하기 위해서는 최대 1518 바이트 크기의 패킷의 페이로드에 특정 contents 가 포함되어 있는지 분석해야 한다. 따라서 세션 테이블 룩업 이전에 특정 contents 를 찾기 위해 380 클록의 전처리 지연이 발생한다. 이때 칩의 동작 클록을 150MHz 클록을 사용하는 경우 한 클록은 약 8 nsec 의 시간이므로 패킷 처리를 위한 지연은 약 3.2 usec 가 된다.

ADEN 은 Xilinx Vertex-5 XC5VLC110-1 칩을 사용하였으며, 최대 동작 주파수는 178Mhz 로 약 5.69Gbps 의 패킷 처리 속도를 갖는다. 또한 현재 구현된 엔진은 칩의 내부 리소스를 약 35%를 사용하고, 사용 가능한 핀이 50% 이상 남아 있어 하나의 칩에 두개의 엔진을 넣을 수 있다. 따라서 현재 적용된 크기의 칩의 경우에도 최소 두개의 엔진을 올릴 수 있어 11Gbps 의 실시간 처리 성능을 갖는 칩이 구현될 수 있다.

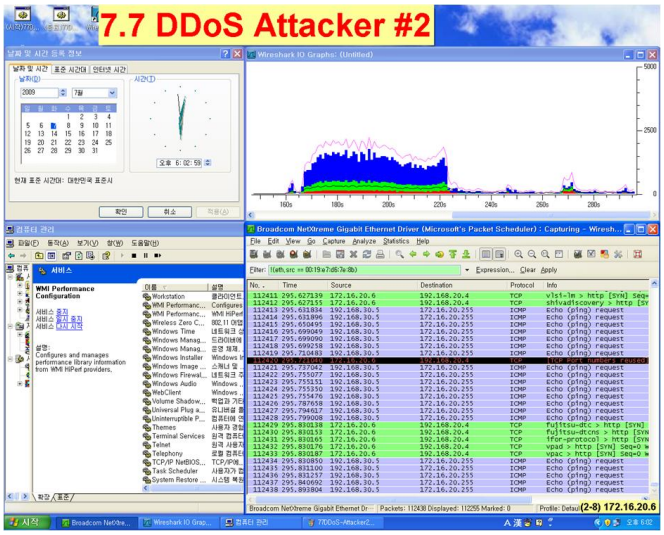
칩 합성을 위해서 사용한 Synthesis 툴은 Synplify Pro 9.4 이며, 로직 시뮬레이션은 Modelsim PE 6.4 로 수행했고, FPGA 통합 툴은 Xilinx ISE 10.1 을 사용하였다.

L3 이하의 DDoS 공격을 탐지하고 차단하는 것은 기본적인 기능이며 정상 동작을 확인하였지만 시험 결과를 본 논문에 보이지는 않았다. 그림 2 에서 4 까지는 지난 2009 년 77 DDoS 에 사용된 좀비가 발생하는 공격을 탐지하고 차단한 결과를 보이고 있다.

(그림 2) 77 DDoS 공격 탐지결과



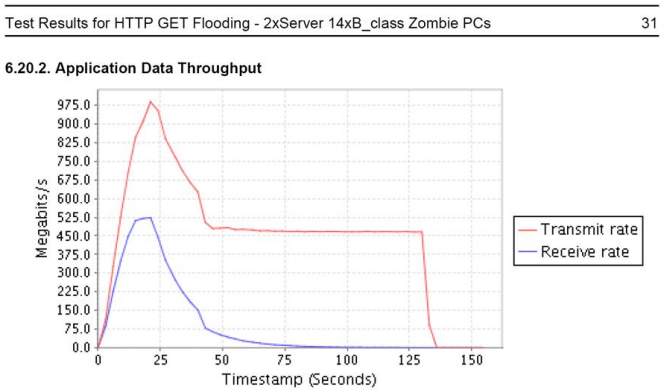
(그림 3) 77 DDoS 공격 탐지결과



(그림 4) 77 DDoS 공격 탐지결과

그림 2 는 본 논문의 DDoS 탐지 시스템의 GUI 화면이다. 본 실험을 하기 위해서 8Gbps 의 백그라운드 트래픽을 실험 망에 인가하고 2 대의 77 좀비가 서버들을 공격하도록 망을 구성하였다. 77 좀비의 경우 공격지 정보를 특정 파일을 읽어 확인하도록 되어 있다. 따라서 공격을 시험을 위해서 시험망의 DNS 서버를 조작하여 타겟 서버의 주소를 시험망에 있는 서버의 주소로 응답하여 공격 패킷이 발생하도록 하였다. 그림 3 과 그림 4 는 좀비에서 발생하는 공격 트래픽을 wireshark 프로그램으로 보였다. 먼저 그림 2 의 중앙에 4 개의 그래프가 보이는데, 이중 왼쪽 상단의 그래프가 각 엔진으로 입력되는 트래픽을 보이고 있다. 왼쪽 상단의 그래프를 보면 그래프의 중간에서 트래픽이 증가한 것이 보이는데, 이는 좀비에서 발생한 트래픽이 나타난 것이다. 또한 이 그래프에서 하나의 선은 계속 이전의 트래픽 량을 보이고 있는데, 이는 우리 시스템이 가진 기능중의 하나인 보호 영역 설정 기능을 보이고 있다. 본 실험에서 그림 3 의 좀비는

보호 영역에 있는 서버를 공격하므로 공격 발생 후 바로 차단된 모습을 보이고 있다. 반면 그림 4 의 좀비는 비보호 영역의 서버를 공격하므로 일정 기간 공격이 유지된 것이다. 이는 그림 2 의 좌측 상단 그래프의 중심에서 입력되는 트래픽은 증가되었지만, 다른 하나의 선은 계속 유지되다가 그래프의 마지막 부분에서 공격 받는 서버를 보호 영역으로 설정하면서 바로 탐지 차단되어 트래픽이 줄어든 것을 보이고 있다. 그림 2 의 우측 상단은 차단되어 drop 된 패킷의 양을 보이고 있다. 77 좀비는 복합 공격을 하며 이중 HTTP Get 공격은 초당 약 30 개 정도로 초 저속 공격을 하는 것으로 알려져 있으나, 구현된 20Gbps DDoS 대응 장비에서는 좀비들의 공격을 찾아 차단할 수 있음을 보이고 있다. 그림 3 과 4 에서 트래픽이 차단된 후에도 소량의 패킷이 발생하는 것은 Spoofing 된 L3 공격에 의한 것으로 보인다.



(그림 5) 77 DDoS 공격 탐지결과

(그림 6) 77 DDoS 공격 탐지로그

그림 5 와 6 은 BreakingPoint 를 이용한 180 만 좀비가 동시에 HTTP Get 공격을 시도하는 상황을 연출하고 이를 탐지한 결과를 보이고 있다. 본 실험에서도 10Gbps DDoS 대응 시스템은 모든 공격을 찾아 차단한 것을 볼 수 있다. 이번 3.3 DDoS 에서는 약 11 만 대의 좀비가 동원된 것으로 보고되고 있지만, 더 많은 좀비가 공격에 동원된 경우를 대비하여 최대 200 만대의 좀비를 탐지하고 자동 대응하는 기능 실험을 완료 하였다.

5. 결론

본 논문에서는 10Gbps 선로 속도의 DDoS 공격 탐지 및 대응 칩에 대한 설계 요구사항과 구현 및 실험 결과를 보였다. 구현된 20Gbps DDoS 대응 시스템은 64 바이트 패킷이 20Gbps 속도로 시스템에 유입되는 경우에도 실시간 탐지/대응이 가능하며, 패킷 크기에 의한 패킷 지연이 증가되지 않음을 보였다. 또한 Syn flooding 등의 L3 계층의 공격뿐만 아니라 L7 계층의 HTTP Get 과 CC 공격 등을 효과적으로 탐지 대응할 수 있음을 실험을 통해 보였다. 현재 해당 시스템은 기술 이전이 완료되었고, 상용화를 위한 추가 기능을 구현 중이며, 조만간 상용시스템이 출시 되어 DDoS 에 대한 위협을 줄여 줄 것으로 기대하고 있다. 올해는 40Gbps 성능의 시스템 개발이 예정되어 있다.

참고문헌

[1] KARGL, et al., "Protecting web servers from distributed denial of service attacks", In : Proceedings of the 10th International World Wide Web Conference, 2001, pp. 130~143

[2] HONEYNET. 2005. Know your enemy:tracking botnets. Whitepaper. The Honeynet Project & Research Alliance. Feb. 2005. Go online to www.honeynet.org/index.html

[3] F. Freiling, T. Holz, and G. Wicherski, "Botnet Tracking-Exploring a Root-Cause Methodology," ESORICS 2005, LNCS 3679, pp. 319~335

[4] D. Barroso, "Botnets-The Silent Threat," ENISA Position Paper, no. 3, pp. 1~9, Nov. 2007

[5] Jun Lv, Xing Li, and Tong Li, "Web based Application for Traffic Anomaly Detection Algorithm", Second International Conference on Internet and Web Applications and Services (ICIW'07), pp. 44-49, 2007

[6] Takeshi Yatagai, Takamasa Isohara, and Iwao Sasase, "Detection of HTTP-GET flood Attack Based on Analysis of Page Access Behavior", Communications, Computers and Signal Processing, pp. 232-235, 2007

[7] Jintae Oh, Donggue Park, Jongsoo Jang and Jeacheol Ryou, “A Novel Application-Layer DDoS Attack Detection Algorithm based on Client Intention”, 정보보호학회논문지, 21 권 제 1 호, pp 39-52, Feb. 2011