# ALADDIN 시스템 설계 및 구현

윤승용*, 오진태*, 장종수*, 김익균*
*한국전자통신연구원 보안관제기술연구팀
e-mail : syyoon@etri.re.kr

# Design and Implementation of ALADDIN System

Seung-Yong Yoon*, Jin-Tae Oh*, Jong-Soo Jang*, Ik-Kyun Kim*
*Managed Security Research Team, ETRI

**요 약**

ALADDIN(Advanced Layer-free DDoS Defense INfrastructure) 시스템은 양방향 10Gbps 트래픽을 처리할 수 있는 안티 DDoS 전용 시스템이다. 로드 밸런서 엔진, 안티 DDoS 분석 엔진, PCI-Express 엔진으로 구성된 세 개의 FPGA 기반 하드웨어 엔진과 소프트웨어 엔진으로 이루어진 시스템은 인라인 모드로 동작하면서 Wire-speed 로 패킷을 처리한다. 시스템은 네트워크 레벨의 DDoS 공격뿐만 아니라 어플리케이션 레벨의 DDoS 공격도 실시간으로 탐지하고 대응한다. 본 논문에서는 ALADDIN 시스템의 설계 및 구현, 테스트 결과에 대해 기술한다.

## 1. 서론

최근 웹 서비스, P2P 서비스, 모바일 서비스 등의 증가로 인터넷 트래픽은 급속히 증가하고 있으며, 특히 DDoS 공격도 수백 Mbps 의 공격에서부터 최대 20~30Gbps 의 트래픽을 유발하는 대형 공격까지 다양한 형태로 발생하고 있는 실정이다[1]. 이러한 DDoS 공격 동향은 기존의 보안 장비로는 기능과 성능 면에서 효과적으로 방어하기가 힘들게 만들고 있다. 따라서 보안 업체들은 기존의 기가급 장비들을 수십 기가급 장비로 업그레이드하여 증가된 네트워크 트래픽 환경에서도 DDoS 공격을 정확하게 탐지하여 대응할 수 있는 새로운 제품을 출시하고 있다[2]. 그러나 시스템 사양상으로는 10Gbps 인터페이스를 제공하지만, 대부분의 상용 제품들은 실질적으로 해당 성능을 만족시키지 못하고 있다. ALADDIN 시스템은 이러한 요구에 의해 개발된 시스템으로 양방향 10Gbps 트래픽을 패킷 손실없이 인라인(In-line) 모드로 동작하면서 DDoS 공격을 탐지하고 대응할 수 있는 안티 DDoS 전용 장비이다. 본 논문에서는 ALADDIN 시스템의 설계 및 구현, 테스트 베드 상에서의 시험 결과에 대해 상세히 기술한다.

## 2. DDoS 공격유형 분류

DDoS(Distributed Denial-of-Service) 공격은 불특정 다수의 공격자가 시스템의 정상적인 서비스를 방해할 목적으로 대량의 데이터를 보내 대상 네트워크나 시스템의 성능을 급격히 저하시켜 시스템에서 제공하는 서비스를 사용하지 못하게 하는 공격이다[3].

DDoS 공격 유형은 여러 가지 기준에 의해 분류될 수 있으나[4], 크게 Network Level 공격과 Application Level 공격으로 분류하는 것이 이해하기도 쉽고, 개념적으로도 명확하다.

Network Level 공격은 소프트웨어의 취약성을 이용한 공격과 IP header 를 변조한 공격유형을 묶어서 Logic 공격, 정상적인 패킷과 구분이 어려운 공격성 패킷을 무작위로 많이 발생시켜 타겟 시스템을 마비시키는 형태의 공격인 Flooding 공격으로 구분할 수 있다.

Application Level 공격은 각각의 Application Protocol 별로 공격을 분류할 수 있는데, HTTP(Web) Flooding, SIP(Voip) Flooding, DNS Flooding 등이 대표적인 예이다. 표 1 은 DDoS 공격 유형 분류를 보여주고 있다.

<표 1> DDoS 공격유형 분류

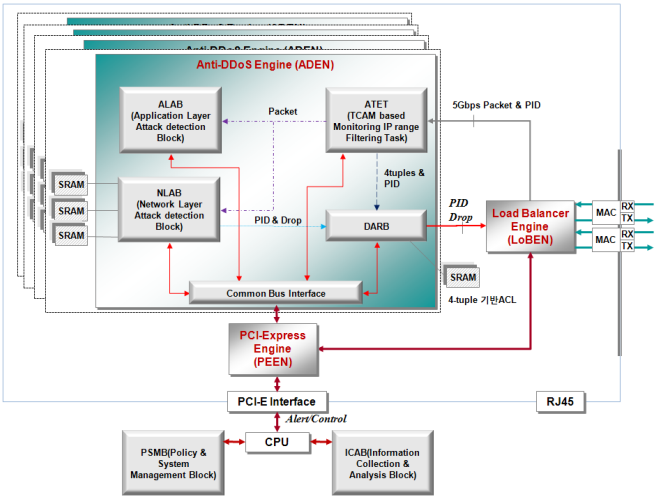
| Network Level | | Application Level | |
|---|---|---|---|
| Flooding 공격 | ● TCP SYN Flooding<br>● TCP Flag Flooding<br>● TCP Open Flooding<br>● TCP Connection Flooding<br>● UDP Flooding (Frag/Non-Frag)<br>● ICMP Flooding (Frag/Non-Frag)<br>● IGMP Flooding | HTTP Flooding | ● Get Flooding<br>● Page Refresh Flooding(F5)<br>● CC(Cache Control) Attack<br>● Slowloris Attack<br>● R.U.D.Y/OWASP HTTP Post Attack |
| Logic 공격 | ● Smurf, Fraggle<br>● LAND<br>● IP Null<br>● TCP/UDP Port Anomaly<br>● Ping of Death<br>● Teardrop, Boink, Bonk | SIP Flooding | ● REGISTER Storm<br>● INVITE Attack<br>● BYE Attack |
| | | DNS Flooding | ● DNS Query Flooding |
| | | Etc | ● DHCP Attack<br>● FTP Attack<br>● Email Attack<br>● SQL Attack<br>● Netbios Attack<br>● RPC Attack<br>● … |

### 3. ALADDIN 시스템 설계

ALADDIN 시스템은 10Gbps 네트워크 트래픽 환경에서 DDoS 공격을 정확하고 신속하게 탐지 및 대응하기 위해 FPGA 기반 세 개의 하드웨어 엔진과 소프트웨어 엔진으로 설계되었다. 각각의 엔진 별 기능은 다음과 같다.

- **Load Balancer Engine(LoBEN)**
  - 패킷 정합 기능: 데이터링크 계층 MAC 프레임을 대상으로 Type 필드를 보고 ARP, RARP, VLAN, IP 이면 정합 기능을 수행한다. 인라인 모드로 동작하면서 수신한 패킷을 다음 단으로 Wire-speed 로 전송하기 위해 사전 정의된 전송 타임아웃(Tx_Threshold) 임계치에 따라 패킷을 전송한다.
  - 로드 밸런싱 기능: 양방향 10Gbps 트래픽, 총 20Gbps 트래픽을 4 개의 ADEN 칩으로 5Gbps 씩 분배한다. ADEN 칩에서는 세션을 추적하여 DDoS 공격을 분석하므로, 동일 세션에 속한 패킷을 동일 ADEN 칩으로 분배하는 알고리즘이 적용된다.
- **Anti-DDoS Engine(ADEN)**
  - 네트워크 레벨 분석 기능: L3/L4 레벨에서 트래픽을 모니터링하고 플로우 별로 분류하여 DDoS 공격을 탐지한다. 세션 추적 및 관리, 접속이력 기반의 화이트리스트(Whitelist) 생성, 목적지 주소 기반의 플로우 별 트래픽 측정 기능을 통해 Flooding 공격을 탐지하고, 패킷 헤더의 유효성 검사를 통해 Logic 공격을 탐지한다.
  - 어플리케이션 레벨 분석 기능: L7 레벨에서 트래픽을 분류 및 모니터링하여 DDoS 공격 분석에 필요한 정보를 추출한다. 사용자 의도 기반의 탐지 알고리즘을 적용하여 어플리케이션 계층 HTTP Get Flooding/CC Attack 공격을 오탐률 없이 탐지한다[5].
  - 대응 기능: 탐지된 공격에 대해 직접적으로 대응이 이루어지며, Packet-by-Packet 혹은 플로우 별로 대응 정책이 적용된다. 대응 정책은 공격 유형별로 설정되면 Rate Limit, ACL, 패킷 Drop 등이 선택적으로 적용된다.
- **PCI-Express Engine(PEEN)**
  - 경보 및 트래픽 정보 전송 기능: ADEN 에 의해 탐지된 DDoS 공격에 대한 경보 정보와 플로우 별로 측정된 트래픽 정보가 손실없이 전달된다.
  - 패킷 펌핑 기능: ADEN 분석 기능 외에 추가적인 공격 분석이 필요한 경우, 해당 패킷을 펌핑하여 S/W 분석 엔진으로 전달한다.
- **S/W Analysis Engine(SAEN)**
  - 탐지 및 트래픽 정보 수집/분석 기능: 탐지 경보 및 트래픽 정보를 수집하여 데이터베이스에 관리한다. 그리고 S/W 적으로 필요한 2 차 분석 기능을 수행한다.
  - 정책 및 시스템 관리 기능: DDoS 공격 탐지 결과에 대한 대응 정책, 사용자에 의해 설정된 탐지 및 대응 정책을 관리한다. 또한 시스템 제어 및 모니터링 기능을 통해 시스템을 관리하고, GUI 를 통해 다양한 DDoS 공격 및 이벤트 정보를 시각화하여 보여준다.

(그림 1)은 전술한 분석 엔진과 해당 기능 블록을 도시한 ALADDIN 시스템의 기본 구조를 보여주고 있다.




(그림 1) ALADDIN 시스템 기본구조

### 4. 구현 및 테스트 결과

ALADDIN 시스템은 두 포트의 10Gbps 광모듈과 MAC 칩을 가지고 있다. 수신된 트래픽은 LoBEN 칩을 통해 4 개의 ADEN 칩으로 분배되고, 탐지 경보는 PEEN 칩을 통해 PCI-E 인터페이스를 거쳐 S/W 로 전달된다.

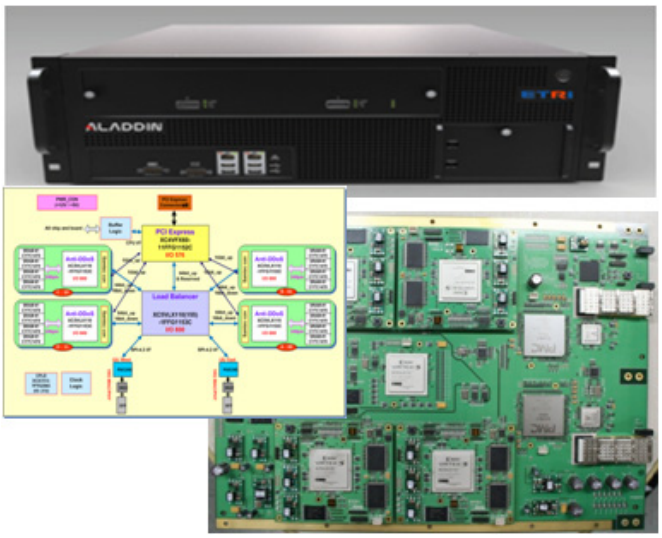
LoBEN 은 PHY/MAC 칩(PM5390)과 SPI-4.2 인터페이스를 통해 패킷을 수신하며, 내부적으로 20Gbps 성능을 처리하기 위해 grade-1 Speed 의 Vertex-5 Xilinx FPGA 위에 구현되었다.

ADEN 은 5Gbps 의 패킷 분석을 통해 DDoS 공격을 탐지하기 위해 LoBEN 과 동일 사양의 FPGA 4 개의 칩에 구현되었다. 각각의 ADEN 에는 세션 테이블, 화이트리스트, 플로우 테이블, ACL 테이블을 위해 4 개의 외부 SRAM(CYPRESS CY7C1372C, 2MB)이 연결되어 있다. ADEN 은 LoBEN 과 64-bit 데이터 버스, 100Mhz 클럭으로 인터페이스 되어 있고, 내부적으로는 32-bit 데이터 버스, 178Mhz 클럭 스피드까지 합성이 성공적으로 이루어졌다. 실제 SRAM 과의 동작을 위해 150Mhz 로 구현되어 있으나, SRAM 이 스펙상 200Mhz 까지 지원하므로 ADEN 은 최대 5.69Gbps 까지 성능으로 동작할 수 있다. ADEN 은 Verilog HDL 로 구현되었고. Simulation 을 위해 Mentor Graphics 사의 ModelSim PE 6.4 을 사용하였고[6], Synthesis 를 위해 Synplicity 사의 Synplify Pro 9.4 툴을 사용하였다[7]. 그리고 로직 Mapping 과 Place & Routing 을 위해 Xilinx ISE 10.1 개발 환경 툴을 이용하였다[8].

PEEN 는 PCI-E 인터페이스 지원을 위해 Vertex-4 Xilinx FPGA 위에 구현되었고, LoBEN 과는 64-bit 데이터 버스, ADEN 과는 16-bit 데이터 버스로 연결되며, 100Mhz 클럭으로 통신하도록 구현되어 있다.

SAEN 은 "C" 언어로 프로그래밍 되어 GCC 4.1.2 버전으로 컴파일 되었고, MySQL DB[9]를 이용하여 각종 정보들을 관리한다.

(그림 2)와 (그림 3)은 실제 구현된 ALADDIN 시스템의 프로토타입과 GUI 화면을 보여주고 있다.

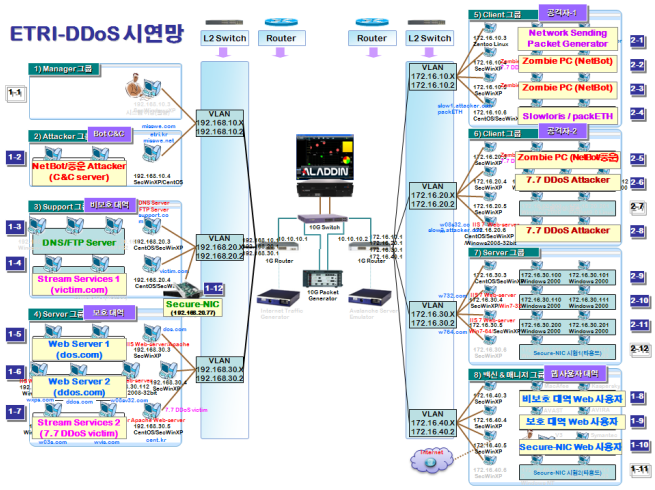


(그림 2) ALADDIN 시스템 프로토타입

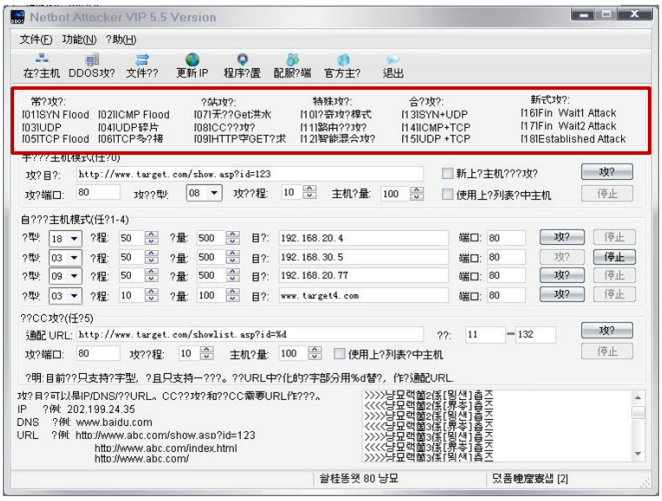
(그림 3) ALADDIN 시스템 GUI 화면

(그림 4)는 ALADDIN 시스템의 테스트 베드를 보여주고 있다. 테스트 베드에는 DDoS 공격 툴로 유명한 Netbot Attacker 를 이용하여 Botnet 을 구성하였고, 2009 년 발생한 7.7 DDoS 대란에 이용된 악성 코드로 감염시킨 좀비 PC 를 배치하여 당시 공격을 그대로 재현시킬 수 있도록 환경을 구성 하였다.

<표 2>와 <표 3>은 Netbot Attacker VIP 5.5 Version 공격 툴(그림 5)과 7.7 DDoS 공격에 대한 테스트 결과를 보여주고 있다. 테스트 결과를 보면, ALADDIN 시스템은 TCP/UDP/ICMP 등 네트워크 레벨의 공격뿐만 아니라 어플리케이션 레벨의 HTTP Get Flooding/CC Attack 등의 공격도 정확하게 탐지함을 알 수 있다. 또한 이 들이 혼합된 복합 공격도 정확하게 탐지함을 알 수 있다.




(그림 4) ALADDIN 시스템 테스트 베드




(그림 5) Netbot Attacker 메인 화면

<표 2> Netbot Attacker 테스트 결과

| 분류 | 공격종류 (메뉴명) | 결과 |
|---|---|---|
| Common Attack | [01]SYN Flood | SYN Flooding 공격으로 탐지함. |
| | [02]ICMP Flood | ICMP Fragmentation Flooding 공격으로 탐지함. |
| | [03]UDP Flood | UDP Fragmentation Flooding 공격으로 탐지함. |
| | [04]UDP Small Size | UDP Flooding 공격으로 탐지함. |
| | [05]TCP Flood | 공격탐지 못함. |
| | [06]TCP Mult-Connect | TCP Connection Flooding 공격으로 탐지함. |

| | | |
|---|---|---|
| WEB Attack | [07]NoCache Get Flood | HTTP Get Flooding 공격으로 탐지함. |
| | [08]CC Attack | CC Attack 공격으로 탐지함. |
| | [09]HTTP Get Nothing | HTTP Get Flooding 공격으로 탐지함. |
| Special Attack | [10]CQ Game Attack | 공격 진행 안됨. |
| | [11]Route Attack | ICMP/UDP/TCP Connection Flooding 공격으로 탐지함. |
| | [12]Smart Auto Attack | ICMP/UDP/TCP Connection Flooding 공격으로 탐지함. |
| Combine Attack | [13]SYN+UDP Flood | SYN Flooding, UDP Flooding 공격으로 탐지함. |
| | [14]ICMP+TCP Flood | ICMP Flooding, TCP Connection Flooding 공격으로 탐지함. |
| | [15]UDP+TCP Connect | UDP Flooding, TCP Open Flooding 공격으로 탐지함. |
| New Attack | [16]Fin_Wait1 Attack | HTTP Get Flooding 공격으로 탐지함. |
| | [17]Fin_Wait2 Attack | HTTP Get Flooding 공격으로 탐지함. |
| | [18]Established Attack | HTTP Get Flooding 공격으로 탐지함. |

<표 3> 7.7 DDoS 공격 테스트 결과

| 레벨 | 프로토콜 | 결과 |
|---|---|---|
| 네트워크 | TCP | - TCP SYN Flooding 공격 탐지<br>- TCP Flag Flooding 공격 탐지 |
| | UDP | - UDP Flooding 공격 탐지 |
| | ICMP | - ICMP Flooding 공격 탐지<br>- Smurf 공격 탐지 |
| 어플리케이션 | HTTP | - HTTP Get Flooding 공격 탐지<br>- CC Attack 공격 탐지 |

## 5. 결론

양방향 10Gbps 트래픽 처리 성능을 갖는 안티 DDoS 전용 시스템인 ALADDIN 시스템은 FPGA 기반의 로드 밸런서 엔진과 4 개의 안티 DDoS 분석 엔진, PCI-Express 엔진, 그리고 S/W 분석 엔진으로 설계 및 구현되었다. 그리고 구현된 ALADDIN 시스템이 기존의 유명한 DDoS 공격 툴인 Netbot Attacker 와 7.7 DDoS 공격을 정확하게 탐지하는 것을 테스트 결과로 확인하였다.

앞으로, 네트워크 레벨의 DDoS 공격을 보다 정확하게 탐지하기 위해 공격 특성 추출(Feature Extraciton), 보다 상세한 세션 상태 추적 및 플로우 측정, 페이로드 검사 등이 포함된 탐지 알고리즘 고도화에 대한 연구가 진행되어야 할 것이다. 그리고 현재 HTTP 응용 프로토콜 공격만 탐지하도록 설계 및 구현 되었는데, SIP, DNS, DHCP, FTP 등 기타 응용 프로토콜에 대한 DDoS 공격 탐지 연구가 이루어져 ALADDIN 시스템 상에 설계 및 구현되어야 할 것이다.

## 참고문헌


[1] 한국정보보호진흥원, “인터넷침해사고 동향 및 분석 월보”, 2008

[2] 커버스토리, “10 곳 중 4 개 사이트 DDoS 장비 바꾸겠다”, 컴퓨터월드, 2010.07

[3] Wikipedia, http://en.wikipedia.org/wiki/Denial-of-service_attack

[4] Christos Douligeris, Aikaterini Mitrokotsa, “DDoS attacks and defense mechanisms; classification and state-of-the art”, in the International Journal of Computer and Telecommunications Networking, Vol.44, Issue 5, Apr 2004

[5] 오진태, 박동규, 장종수, 류재철 “사용자 의도 기반 응용계층 DDoS 공격 탐지 알고리즘, 정보보호학회논문지, 제 21 권 제 1 호, 2011.2, page:39-52

[6] http://www.model.com

[7] http://www.synplicity.com

[8] http://www.xilinx.com

[9] http://www.mysql.com