情 報 保 護 學 會 誌
第19卷 第3號, 2009. 6

DDoS 공격 및 대응 기법 분류

전 용 희*, 장 종 수**, 오 진 태**

요 약

분산 서비스 거부(DDoS: Distributed Denial of Service) 공격이 인터넷에 대하여 거대한 위협을 제공하고 있으며, 이에 대한 대응책들이 많이 제시되었다. 그러나 공격의 복잡성과 다양성으로 인하여 어떤 대응 기법이 효과적인지도 상당히 혼란스럽게 되었다. 공격자들은 보안 시스템을 우회하기 위하여 꾸준히 공격도구들을 변경하고 있으며, 이에 대한 방패로써 연구자들 역시 새로운 공격에 대한 대응책을 강구하고 있다. 따라서 본 논문에서는 DDoS 기술동향, DDoS 공격 및 대응 기법에 대한 분류법 및 DDoS 대응 기법의 과제에 대하여 기술하고자 한다. 이를 통하여 효과적인 DDoS 공격 대응책을 수립하는데 필요한 기초 자료로 활용하고자 한다.

Ⅰ. 서 론

서비스 거부(DoS) 공격은 흔히 말하는 보안의 3대 요소인 CIA(Confidentiality, Integrity, Availability) 중 가용성을 저해하는 공격이다. DDoS는 이 목표를 달성하기 위하여 복수의 공격 엔티티가 참여한다. 그 결과로써 희생자는 악성 트래픽을 수신하게 되고 손실을 입게 된다. DoS 공격은 아래와 같은 세 가지 유형으로 보통 발생 한다:

- 시스템의 취약성이나 소프트웨어 구현의 버그를 이용한 공격
- 타깃 머신의 가용 자원을 소모해버리는 공격
- 희생 머신에 대한 가용 대역폭을 모두 소모하는 공격(즉, 대역폭 공격)

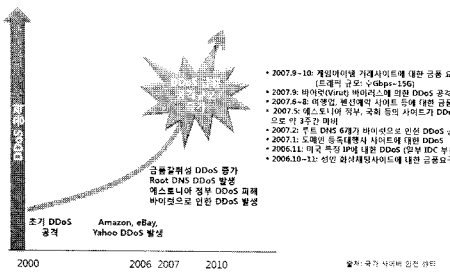
DDoS 공격을 가능하게 하는 인터넷의 설계 요소는 다음과 같다[1]:

- 인터넷 보안은 상호의존적이다: DDoS 공격은 보안이 침해된 시스템을 통하여 보통 개시된다. 특정 호스트가 보안이 잘 되어 있어도 인터넷상의 다른 취약 호스트들을 통하여 공격이 발생할 수 있다.
- 책임성을 추적하기 힘들다: IP(Internet Protocol) 프로토콜의 비연결성 성질로 인하여, IP 스푸핑 공격을 생성하기 쉽다. 따라서 공격의 진정한 소스를 결정하는 것을 아주 어렵게 만든다. 예로서 Smurf 공격이 있다.
- 인터넷 자원의 제약성: 호스트, 네트워크, 서비스 등의 모든 인터넷 요소들의 자원이 많은 사용자들에 의하여 소비될 수 있는 제한된 자원을 가지고 있다. 따라서 제한된 대역폭, 처리력 및 저장 용량 모두가 DoS 공격의 대상이 된다.
- 종단 대 종단 통신 패러다임 설계: 서비스 보장을 위하여 필요한 대부분의 기능은 종단 호스트에 있는 반면, 중간 노드에서는 패킷의 신속한 처리를 위한 제한된 처리력만 가지고 있다. 동시에 중간 네트워크의 고대역폭이 제한된 대역폭을 가지고 있는 호스트에 대하여 오용될 가능성을 제시한다.
- 분산된 제어 방식: 인터넷 관리가 분산되어 지역 정책에 의하여 운영되므로, 전역적인 보안 메커니즘을 실행하는 것이 어렵다.
- 수많은 취약 환경의 존재: 취약성을 가진 수많은 네트워크와 호스트 때문에 DDoS 공격의 개시가 쉽다.
- 방어보다 공격이 쉽다: 보안 기능을 가진 네트워크 인프라와 프로토콜을 개발하는 것보다, 이를 공격하는 방법을 개발하는 것이 더 쉽다. CERT 자료에 의하면 인터넷에 연결된 시스템에 대한 공격은 점

* 대구가톨릭대학교 컴퓨터정보통신공학부(yhjeon@cu.ac.kr)
** 한국전자통신연구원 지식정보보안연구부(jsjang@etri.re.kr, showme@etri.re.kr)

점 더 정교해진 반면에 공격을 파악하는 데 필요한 기술이나 지식은 점점 더 줄어들었다. 공격방법은 점점 더 자동화되고 있으며 피해 범위가 더욱 커질 수 있게 되었다. [그림 1]은 DDoS 공격 동향을 보여주며, 주요 변화는 다음과 같다:

- 최근 게임아이템 거래사이트, 증권사 등 국내 웹사이트를 대상으로 무차별적인 협박성 DDoS 공격으로 피해가 확대되고 있음.
- 공격대상 사이트뿐만 아니라, 해당 사이트와 연결된 IDC 및 ISP 환경에도 심각한 피해를 야기 시키고 있음.
- 정치적/군사적 목적의 DDoS 공격이 증가되고 있음.



〔그림 1〕 DDoS 공격 동향

DDoS 공격 형태에서도 다음과 같은 변화가 있다:

- 수 Gbps에서 수십 Gbps 규모로 DDoS 공격 규모가 확대되고 있음.
- 과거에는 소수 좀비 PC가 공격을 시도하였으나, 최근에는 봇넷으로 구성된 다수의 좀비 PC가 공격에 활용되고 있음.
- DDoS 공격이 네트워크 레벨에서 시스템(커널) 레벨로 다시 응용 레벨로 진화되고 있음.

본 논문에서는 DDoS 기술동향, DDoS 공격 및 대응 기법에 대한 분류법을 알아보고 각각의 특징 분석을 통하여, 효과적인 대응책을 수립하는데 필요한 기초 자료로 활용하고자 한다. DDoS 공격의 분류는 [2]의 방법을, 대응 기법의 분류에서는 [2], [3]에 대한 자료를 중심으로 기술한다. DDoS 공격 및 대응 기법의 분류를 통하여 다음과 같은 중요한 질문에 대한 대답을 또한 구할 수 있다[2]:

- 기존의 대응 시스템에 의하여 효과적으로 처리될 수 있는 공격 유형
- DDoS 공격을 수행하는 방법 유형
- 여러 가지 유형의 공격에 대한 대응 시스템의 성능
- 대응 시스템의 취약성, 상호보완 관계
- DDoS 향후 연구 분야

Ⅱ. DDoS 기술 동향

본 장에서는 DDoS 공격, 탐지 및 차단 기술 동향을 요약하여 기술한다.

2.1 DDoS 공격 기술

먼저 호스트를 대상으로 하는 DDoS 공격에 대하여 분류하고 특징을 기술한다.

- 응용(L7) 공격: 특정 호스트 내의 응용에 대한 공격으로 정당한 사용자의 서비스를 제한하는 공격이다. 공격 특징은 아래와 같다:
  - 공격 대상 응용만 서비스가 제한되기 때문에, 동일 호스트 내 다른 응용은 정상 동작될 수 있음.
  - 관리자에 의한 공격 발생 확인이 늦어지는 경향이 있음.
  - 공격 트래픽의 양이 매우 적음.
  - 전체 트래픽을 대상으로 검사하는 일반적인 트래픽 탐지 기법으로는 탐지하기 어려움.

이 범주에 속하는 공격의 예로는 HTTP Get Flooding, Cache Control 공격, VoIP/SQL/RPC 공격 등이 있다.

- L4(TCP/UDP) 공격: 특정 호스트의 모든 네트워킹 서비스 혹은 시스템 자체를 마비시키기 위하여 L4 계층에 대해 시도되는 공격이다. 시스템 내부의 TCP, UDP 스택의 자원관리 상의 취약점을 공격하는 것으로, L4 이상의 계층에 대한 네트워크 기능 마비를 초래한다. 예로는 TCP SYN, SYN-ACK, RESET Flooding, UDP Flooding 공격 등이 있다.
- L3(IP, ARP, ICMP) 공격: 특정 호스트의 모든 네트워킹 서비스 혹은 시스템 자체를 마비시키기 위하여 L3 계층에 대해 시도되는 공격이다. 시스템 내부의 IP, ARP, ICMP 등의 프로토콜의 자원관리 상의 취약점을 공격하는 것으로, L3 이상의 계층에 대한 네트워크 기능 마비를 초래한다. 예로는 IP Flooding(Land 공격), ARP, RARP 스푸핑, ICMP 플러딩 공격 등이 있다.
- 기타 공격: 상기 네트워크 계층 이외의 계층에 대

한 공격 및 특정 버그 등을 이용하여 시스템의 네트워크 기능 혹은 시스템 전체를 마비시키는 공격이다. 공격 대상 호스트가 적절하지 않은 방식으로 도착되는 트래픽을 처리하는 경우, 해당 호스트 전체가 마비될 수 있는 특징이 있다. 호스트가 이러한 유형의 공격에 대해 대응이 가능하다면, 이 공격은 *자원 소비 공격* 형태로 구분된다.

다음으로 네트워크를 공격대상으로 하는 DDoS 공격 기술 동향에 대하여 기술한다.

- 중요 노드 공격: 공격 대상 네트워크 내의 중요 자원에 대한 공격으로, 그 대상은 DNS, 라우터, 병목 링크 등이다. 네트워크를 정상적으로 동작시키기 위해 필요한 중요 서버, 노드 및 자원에 대해 DDoS 공격을 시도하며, 견고한 네트워크 토폴로지를 설계함으로써 대응이 가능하다. 예로는 DNS Lookup 플러딩, SYN 플러딩 등을 이용한 네트워크 장비의 세션 관리 기능 마비 등이 있다.
- 대역폭 소비 공격: 한정된 대역폭을 가지는 네트워크 회선 상에 막대한 공격 트래픽을 전송함으로써 네트워크를 마비시키는 공격이다. 종단간 연결을 필요로 하지 않기 때문에 UDP 혹은 ICMP 패킷을 이용하여 대량 트래픽을 전송하며, 그 때문에 트래픽 어노멀리 탐지가 쉽다.
- 하부 공격: 전체 인터넷 망 자체를 마비시키기 위한 공격이다. 본 공격의 핵심은 공격 대상을 어떻게 마비시키는 가에 있는 것이 아니라, 동시 다발적으로 인터넷 인프라에 대하여 공격이 시도된다는 것에 있다. 인터넷을 구성하는 모든 구성 요소의 협력을 통해서만 대응이 가능해진다. 예로는 Root DNS 서버 공격, 대형 백본 라우터 및 라우팅 프로토콜 공격, 인증서 서버에 대한 공격 등이 있다.

2.2 DDoS 공격 탐지 기술

공격 탐지 기술은 탐지 도구 및 방법에 따라서 아래와 같이 기술할 수 있다.

- 침입탐지시스템/침입방지시스템(IDS/IPS): 특정 시그니처를 사용하여, 상위 랭크 안에 포함된 트래픽 중 평시와 다른 특이 사항(즉, 공격 트렌드) 트래픽을 분석한다. 대분의 ISP가 운용 중이며, 백본, 국내 및 국제 게이트웨이에 설치된다.
- DDoS 대응 시스템: L3 기반으로 고속 DDoS 공격 탐지 및 차단을 수행한다. 공격 발생 시 트래픽을 우회시켜 공격 트래픽을 제거하고 정상 트래픽만 전송한다. 예로는 시스코 가드 및 탐지기, Arbor Peakflow SP 제품 등이 있다. 코어 라우터, 게이트웨이 라우터사이에 설치된다.
- Netflow: 트래픽 패턴 분석 및 불규칙 트래픽에 대하여 식별하고, 소스 IP, 목적지 IP, 프로토콜, AS별 분석을 수행한다. 분석용 서버를 백본 네트워크에 연결 설치한다. 라우터 과부하 발생 가능성으로 대용량 장비에만 사용한다.
- ACL(Access Control List): 라우터 접근 목록을 이용하여 실시간 소스/목적지 IP, 포토, 프로토콜만 확인한다. 라우터 과부하 주의가 필요하며, 백본이나 게이트웨이 라우터 자체 기능으로 설치 가능하다.
- MRTG(Multi Router Traffic Grapher)/RRD (Round Robin Database): 라우터의 SNMP MIB를 수집, 분석하여 트래픽 급증, 급감 여부를 보고 징후를 판단한다. MRTG는 모든 ISP가 운용중이며, MRTG 서버를 백본 네트워크에 연결 설치한다.
- DNS 서버: DNS query 패킷 분석을 통해 과도한 질의 패킷을 탐지하고, DNS 서버 로그 실시간 모니터링을 한다. 주요 네트워크에 DNS 캐싱 서버가 설치된다.
- L7 스위치(IPS): Query 임계치를 미리 설정해 놓고 초과시 경보를 발생한다. 상위 랭크 DNS query URL을 표시하여 주는 기능이 없다. DNS 서버와 게이트웨이 등에 설치된다.

2.3 DDoS 공격 차단 기술

공격 차단 기술은 아래와 같이 구분된다.

- URL 차단: 과도한 DNS 질의 패킷 발생에 의한 DNS 기능 마비 방지와 특정 URL로 발생되는 DDoS 패킷을 차단하는 것이 목적이다. 차단방법으로는 DNS 싱크홀 방법, DNS 캐싱 서버에서 차단하고자 하는 특정 URL에 대하여 루프백 IP 주소 선언을 하거나 임의의 서버 IP를 설정하는 방법, 해당 사업자에 할당되지 않은 IP에서 DNS query를 받을 시 차단하도록 캐싱서버에서 차단설정 하는 방법(IP 스푸핑 차단 효과), L7 스위치, DNS 앞단에서 특정 URL에 대한 DNS query 패킷 차단 설정 방법 등이 있다. DNS 서버에 필터링

적용 시에는 용량대비 부하를 고려할 필요가 있다.

· IP 차단: DDoS 공격 IP를 차단하여 네트워크를 보호함이 목적이다. 차단 방법은 아래와 같다.
  - Blackhole 처리
  - 차단하고자 하는 목적지 IP를 blackhole 라우팅으로 처리하여 차단(소스 차단 불가)
  - ACL 처리
  - 소스 IP, 목적지 IP, 포토별 차단
  - 과부하로 라우터 최대 처리 용량 제한으로 소극적 사용 권장
  - uRPF(unicast Reverse Path Forwarding)
  - 게이트웨이 라우터나 가입자 접속용 라우터에 uRPF 적용
  - 율 제한(Rate Limit)
  - Sync 플러딩 등 특정 패턴의 대역폭 제한
  - 라우터에 부하를 줌
  - PBR(Policy Base Routing)
  - 특정 사이즈 별로 패킷을 ACL 처리, Null 0으로 차단

소스 IP 차단은 ACL 및 라우팅 갱신(AS별, prefix별) 등으로 처리 가능하다.

· 포트, 프로토콜 차단: DDoS 공격하는 특정 포트, 프로토콜 등을 차단하여 네트워크를 보호함이 목적이다. L7 스위치; 포트, 프로토콜별 및 TCP/UDP 플러딩, 페이로드 패턴 등 설정; ACL 처리; 라우터에서 포트, 프로토콜 등을 ACL로 설정하여 차단하는 방법 등이 있다. L7 스위치는 게이트웨이, DNS 등에 제한적으로 설치 운용하고 있다.

Ⅲ. DDoS 공격의 분류 기준

DDoS 공격을 분류하기 위하여, [2]에서는 공격을 준비하고 수행하는데 사용된 수단, 공격의 특성 및 희생자에 대한 영향 등을 고려하였다.

3.1 자동화 정도(Degree of Automation)

자동화 정도에 따라서 *수동, 반자동, 자동*으로 구분된다. 초창기의 DDoS 공격이 단지 수동 공격의 범주에 포함되었지만, 그 후로 곧 자동화 되었다. 반자동 공격 유형에서는 DDoS 네트워크는 핸들러(마스터)와 에이전트(슬레이브, 데몬, 좀비) 머신으로 이루어진다. 에이전트들을 모집하고, 이용하고 감염하는 단계는 자동적으로 이루어진다. 실제 사용단계에서, 공격자는 핸들러를 경유하여 에이전트에게 공격 유형, 개시, 기간 및 희생자를 명시하며, 에이전트는 희생자에게 패킷들을 전송한다. 에이전트와 핸들러 머신 사이의 통신 메커니즘에 따라, 반자동 공격은 다시 직접 통신을 하는 공격과 간접 통신을 하는 공격으로 구분된다.

직접 통신을 위하여 에이전트와 핸들러 머신은 서로의 신원을 알 필요가 있으며, 이 때문에 이런 유형의 DDoS 네트워크는 쉽게 탐지될 수 있다. 간접 통신을 하는 공격의 예로는 IRC(Internet Relay Chat)를 이용하는 공격이 있다[4]. 이런 유형의 공격 식별은 IRC 서버에 현재 연결된 에이전트들을 추적할 수 있는 능력에 달려 있다.

자동 공격에서는 공격 코드 내에 자동적인 DDoS 공격을 위한 모든 것이 사전 프로그램 되어 공격자가 쉽게 노출되지 않는다.

에이전트 머신을 모집하기 위하여 반자동 및 자동 공격에 사용되는 호스트 스캐닝 전략은 아래와 같이 분류하고 있다:
- 랜덤 스캐닝
- 히트 목록 스캐닝
- Signpost 스캐닝
- 순열(permutation) 스캐닝
- 지역 서브넷 스캐닝

취약성 스캐닝 전략에 따른 분류는 다음과 같다:
- 수평(horizontal) 스캐닝
- 수직(vertical) 스캐닝
- 조정된(coordinated) 스캐닝
- 비밀 스캐닝

감염 단계에서의 공격 코드 전파 메커니즘에 따라 다시 아래와 같이 분류 한다:
- 중앙 근원지 전파
- 역-체이닝 전파
- 자동 전파

3.2 서비스 거부에 사용된 약점

*semantic 공격*과 *전수(brute-force) 공격*으로 구분된다. 시맨틱 공격은 희생 머신에 설치된 어떤 프로토콜이나 응용의 구체적인 특징이나 구현 버그를 이용한다. 예로써 TCP SYN 공격이 있다. 전수 공격은 엄청난 양의

합법적으로 보이는 거래를 개시하여 수행된다. 중간 네트워크가 희생 네트워크가 다룰 수 있는 양보다 더 많은 트래픽을 보통 전달함으로써 희생자의 자원을 소모해 버린다. 설치된 프로토콜이나 응용을 수정함으로써 시맨틱 공격에 대응하게 되면 해당 공격은 전수-공격 범주로 넘어오게 된다. 그러므로 전수 공격은 시맨틱 공격보다 더 많은 양의 공격 패킷을 생성할 필요가 있게 된다.

3.3 소스 주소의 유효성

IP 스푸핑 공격에 따른 소스 주소의 유효성을 기초로, *spoofed 소스 공격*과 *유효 소스 주소 공격*으로 구분된다. spoofed 소스 공격은 주소의 경로 가능성(routability)에 따라 다시 경로-가능한 소스 주소 공격과 경로-불가능한 소스 주소 공격으로 구분된다. 경로-가능한 공격의 예로는 reflector 공격으로 Smurf 공격이 있다. 경로-불가능한 공격은 예약된 주소 집합이나 사용되지 않은 주소 공간을 이용한다.

스푸핑 기술에 따라서 spoofed 소스 공격은 다시 아래와 같이 구분 된다:

- 임의(random) spoofed 소스 주소 공격
- 서브넷 spoofed 소스 주소 공격
- 경로 내(en route) spoofed 소스 주소 공격
- 고정 spoofed 소스 주소 공격

만약 공격 메커니즘이 에이전트와 희생 머신 사이에 여러 개의 요구/응답 교환이 필요하다면 특정한 응용이나 프로토콜 특징을 목표로 하는 공격은 유효한 소스 주소를 사용하여야 한다. 이런 공격의 예로는 Naptha[5]가 있다.

3.4 공격 율의 역동성

에이전트 머신의 공격 율 역동성에 의하여, *항등 율(constant rate) 공격*과 *가변 율(variable rate) 공격*으로 구분된다. 대부분의 알려진 공격들은 항등율 메커니즘을 전개한다. 그러나 지속적인 대규모의 트래픽은 비정상 트래픽으로 쉽게 탐지될 수 있다. 탐지와 대응을 지연시키거나 우회하기 위하여 가변 율 공격은 에이전트 머신의 공격 율을 변화시킨다. 율 변화 메커니즘에 따라 다시 증가 율 공격과 진동(fluctuating) 율 공격으로 구분된다. 증가 율 공격은 희생자의 자원을 천천히 고갈시키기 위하여 점진적으로 율을 증가시킨다. 장시간에 걸쳐 서비스가 저하되기 때문에, 공격 탐지를 상당히 지연시킬 수 있다. 진동 율 공격은 희생자의 행위나 사전 프로그램 된 타이밍에 따라 공격 율을 조정함으로써, 탐지를 피하려고 노력한다.

3.5 특성화의 가능성

공격 패킷의 콘텐츠와 헤더 필드를 봄으로써 때로는 공격을 특성화 할 수 있다. 그리하여 특성화를 통하여 필터링 규칙을 만들 수 있다. 이런 특성화 가능성에 따라서, 다시 특성화 가능 공격과 특성화 불가능 공격으로 구분된다. 특성화 가능 공격의 예로는 TCP SYN 공격(TCP 헤더에 SYN 비트 설정된 패킷), ICMP ECHO 공격, DNS 요구 공격 등이 있다. 특성화 가능 공격은 희생 서비스와의 연관성에 따라 다시 여과-가능(filterable) 공격과 여과-불가능(non-filterable) 공격으로 구분된다. 여과-가능 공격은 방화벽에 의하여 여과될 수 있는 패킷들을 사용하는 공격이다. 예로는 UDP 플러드 공격이나 웹 서버 상의 ICMP ECHO 플러드 공격이 있다.

여과-불가능 공격은 합법적인 서비스를 요구하는 정상 형태의 패킷들을 이용하여 공격한다. 이에 대한 여과는 합법적인 서비스들에 대하여 서비스 거부를 초래하기 때문에 수행할 수 없게 된다. 예로는 웹 서버를 범람시키는 HTTP 요구나 네임 서버를 목표로 하는 DNS 요구 플러딩 공격 등이 있다.

특성화 불가능 공격은 다른 응용이나 프로토콜을 포함하는 다양한 패킷들을 사용하여 네트워크 대역폭 소모를 시도한다. 그러나 공격의 특성화 가능 여부는 특성화에 부과된 자원과 특성화 수준에 강하게 의존된다.

3.6 에이전트 집합의 지속성

탐지를 방지하고 추적을 방해하기 위하여 한 순간에 활동하는 에이전트 머신의 집합이 변하는 공격이 있다. 이에 따라 다시 *고정 에이전트 집합 공격*과 *가변 에이전트 집합 공격*으로 구분된다. 고정 공격은 모든 에이전트 머신이 자원 제약을 고려하여 비슷한 방법으로 동작한다. 같은 집합의 명령을 받으며 공격동안 동시에 동원된다. 가변 공격에선 공격자는 모든 사용가능한 에이전트들을 여러 그룹으로 나누어 한 순간에 단지 하나의

그룹만 종사케 한다.

3.7 희생 유형

희생 유형에 따라, *응용, 호스트, 자원, 네트워크 및 인프라 공격*으로 구분된다. 응용 공격은 희생 호스트의 어떤 응용을 목표로 하며 합법적인 사용자가 그 응용을 못 쓰도록 한다. 공격당한 호스트 상의 다른 응용들은 동작을 방해받지 않고 지속해야 하고, 공격 양이 비정상으로 나타나지 않을 만큼 보통 작기 때문에 응용 공격의 탐지는 어렵다. 호스트 공격은 타깃 머신에 대하여 완전하게 접근을 못하도록 하는 것이다. 호스트 공격은 많은 양의 공격 트래픽을 생성하므로 탐지가 쉽게 된다. 자원 공격은 특정 DNS 서버, 라우터 혹은 병목 링크와 같은 희생 네트워크 내의 중요한 자원을 타깃으로 한다. 중요 서비스들을 이중화하고 견고한 네트워크 토폴로지를 설계함으로써 방지할 수 있다. 네트워크 공격은 타깃 네트워크의 입력 대역폭을 소모하는 공격이다. 대량의 트래픽 발생으로 보통 쉽게 탐지된다. 하부 공격은 전역 인터넷 운용에 중요한 어떤 분산 서비스를 타깃으로 한다. 예로써 도메인 네임 서버, 대규모 코어 라우터, 라우팅 프로토콜, 인증 서버 등에 대한 공격이 있다.

3.8 희생자에 대한 영향

희생자에 대한 DDoS 공격의 영향에 따라서, *파괴적(disruptive)* 및 *저하성(degrading) 공격*으로 구분된다. 파괴적 공격은 타깃 머신의 서비스를 완전하게 거부하도록 하는 것이다. 이 공격은 역동적 복구 가능성에 따라 다시 *자기-복구가능, 인간-복구가능* 및 *복구-불가능 공격*으로 구분된다. 자기-복구가능 공격의 경우에는, 공격 패킷의 유입이 정지되자마자 인간의 개입 없이 희생 머신은 복구된다. 인간-복구가능 공격은 공격이 멈춘 후 복구를 위하여 사람의 개입이 필요하다. 복구 불가능 공격은 희생 머신의 하드웨어에 대하여 영구적인 손상을 끼치는 공격이다.

저하성 공격의 목적은 희생자 자원의 상당 부분을 소모하여 합법적인 사용자에 대한 서비스를 심각하게 저하시키는 것이다. 이러한 공격은 총체적인 서비스 단절을 초래하지 않기 때문에 상당기간 동안 탐지되지 않고 남아 있을 수 있다.

Ⅳ. Mirkovic의 DDoS 대응 기법 분류

[2]에서는 대응 기법을 활동 수준, 협동 정도 혹은 설치 위치 등에 따라 다음과 같이 분류하고 있다.

4.1 활동 수준에 따른 분류

방어 메커니즘의 활동 수준에 따라, *예방(preventive)*과 *반응(reactive)* 메커니즘으로 구분된다.

4.1.1 예방 메커니즘 대응 기법

예방 메커니즘은 예방 목적에 따라 다시 *공격 예방*과 *서비스-거부 예방* 메커니즘으로 구분된다. 공격 예방 메커니즘은 침해의 가능성이나 DDoS 공격 수행 가능성을 없애기 위하여 인터넷상의 시스템과 프로토콜을 수정하는 것이다. 보안 타깃에 따라, 공격 예방 메커니즘을 다시 *시스템 보안*과 *프로토콜 보안* 메커니즘으로 구분한다.

DoS 예방 메커니즘은 합법적인 사용자에 대한 서비스 거부 없이 공격 시도를 견디도록 한다. 이것은 자원 소비에 대한 정책을 집행하든지 혹은 합법적인 사용자가 공격에 의하여 영향을 받지 않도록 충분한 자원이 있도록 보장함으로써 행하여진다. 예방 방법에 따라, DoS 예방 메커니즘을 다시 *자원 계정*(accounting)과 *자원 번식*(multiplication) 메커니즘으로 구분한다. 자원 계정 메커니즘은 모든 사용자의 자원에 대한 접근을 사용자의 권한과 행위에 기반 하여 감시한다. 따라서 합법적인 정상-행위 사용자에게는 공평한 서비스가 보장된다. 자원 번식 메커니즘은 DDoS 위협에 대처하기 위하여 풍부한 자원을 제공한다. 예로써, 로드 밸런서(load balancer)를 가진 서버 풀을 설치하고 업 스트림 라우터 사이에 고 대역폭 링크를 설치하는 시스템이 있다.

반응 메커니즘은 희생자에 대한 공격의 영향을 완화하기 위하여 노력한다. 이를 위하여 공격을 탐지하고 대응할 필요가 있다. 가능한 빨리 시도된 DDoS 공격을 탐지하고 낮은 오탐(false positive) 레벨을 가지는 것이다. 반응 메커니즘은 공격 탐지 전략에 따라 다시 *패턴 탐지, 어노멀리(anomaly) 탐지* 및 *제3자(third-party) 탐지*로 구분된다.

패턴 탐지 메커니즘은 데이터베이스 내에 알려진 공격들의 시그니처를 저장하고 이러한 패턴들의 존재에

대하여 모든 통신을 감시하는 것이다. 알려진 공격들은 쉽게 탐지되는 반면에, 새로운 공격이나 폴리모픽 형태의 공격은 탐지되지 않을 수 있다는 결점이 있다.

어노멀리 탐지 메커니즘은 정상적 트래픽 역동성이나 예상 시스템 성능과 같은 정상 시스템 행위 모델을 가지고 있고, 시스템의 현재 상태를 모델과 주기적으로 비교하여 비정상을 탐지하는 방법이다. 이전에 알려지지 않은 공격을 발견할 수 있는 장점이 있지만, 정상적 행위를 공격으로 잘 못 식별하는 문제도 있다. 정상 행위의 명세화에 따라 다시 *표준 및 훈련(trained)* 메커니즘으로 구분한다.

정상 행위의 표준 명세서를 사용하는 메커니즘은 어떤 프로토콜 표준이나 규칙 집합에 근거한다. 예를 들어, TCP 프로토콜 명세서는 3-방향 핸드세이크를 기술하는데, 공격 탐지 메커니즘은 이 명세서를 이용하여 반-개방 TCP 연결을 탐지하여 큐로부터 삭제할 수 있다. 오탐을 생성하지 않는다는 장점이 있고, 표면적으로 표준을 준수하는 것처럼 보이는 정교한 공격에 대하여는 탐지되지 않은 결점이 있다.

정상 행위의 훈련 명세서를 사용하는 메커니즘은 네트워크 트래픽과 시스템 행위를 감시하여 다른 파라미터들에 대하여 경계 값을 생성한다. 한개 혹은 그 이상의 값을 초과하는 모든 통신은 비정상으로 간주된다. 광범위하게 공격을 잡을 수 있으나, 두 가지의 단점을 가지고 있다: 경계치 설정과 모델 갱신. 경계치를 낮게 잡으면 많은 오탐을 초래하고, 높게 잡으면 미탐을 가져온다. 자동적 모델 갱신 훈련 메커니즘은 장기간에 걸쳐 서서히 증가하는 율 공격에 대하여 취약할 수 있다.

제3자 탐지 메커니즘은 스스로 탐지 과정을 다루지 않고, 공격 발생을 보내고 공격 특성화를 제공하는 메시지에 의존한다.

4.1.2 반응 메커니즘 대응 기법

반응 메커니즘은 대응 전략에 따라 다시 *에이전트 식별, 율-제한(rate-limiting), 여과(filtering)* 및 *재구성(reconfiguration)*을 설치하는 메커니즘으로 분류된다.

에이전트 식별 메커니즘은 희생자에게 공격을 수행하는 머신의 신원에 대한 정보를 제공해 준다. 이 정보를 공격의 영향을 감소시키기 위하여 다른 방법에 의하여 사용할 수 있다.

율-제한 메커니즘은 탐지 메커니즘에 의하여 악성으로 특성화된 패킷의 집합에 대하여 율-제한을 부과한다. 탐지 메커니즘이 공격 스트림을 정확히 특성화할 수 없거나 많은 오탐이 있을 때 흔히 사용될 수 있는 대응 기술이다. 공격 트래픽의 일부가 통과될 수 있는 단점이 있다.

여과 메커니즘은 공격 스트림을 완전하게 여과하기 위하여 탐지 메커니즘에 의하여 제공되는 특성화를 이용한다. 특성화가 매우 정확하지 않으면 여과 메커니즘은 합법적인 트래픽에 대하여 우발적으로 서비스를 거부하는 위험을 가지고 있다. 예로써 역동적으로 설치된 방화벽이 있다.

재구성 메커니즘은 희생자에 대하여 더 많은 자원을 추가하거나 공격 머신을 고립시키기 위하여 희생자나 중간 네트워크의 토폴로지를 변화시킨다. 예로는 재구성 가능한 오브레이 네트워크, 자원 번식 서비스, 공격 고립 전략 등이 있다.

4.2 협동 정도에 따른 분류

DDoS 방어 기법의 협동 정도에 따라, *자율적(autonomous), 협동적(cooperative)* 및 *상호의존적(interdependent)* 메커니즘으로 구분된다.

4.2.1 자율적 대응 기법

자율적 메커니즘은 설치된 호스트나 네트워크 지점에서 독립적인 방어를 수행한다. 방화벽이나 침입탐지 시스템이 그 예이다. 방어 시스템이 분산 방법으로 기능을 수행할 지라도 자신이 보호하는 네트워크 내에 완전히 설치된다면 자율적으로 간주된다.

4.2.2 협동적 대응 기법

협동적 메커니즘은 자율적 탐지 및 대응이 가능하나, 다른 개체들과 협동 할 수 있고 합동 운영에서 훨씬 더 좋은 성능을 가진다. 예로써 푸시백 메커니즘을 설치한 집합 혼잡 제어(ACC: aggregate congestion control)[6] 시스템이 있다.

4.2.3 상호의존적 대응 기법

상호의존적 메커니즘은 단일 설치 지점에서 자율적

으로 운용될 수 없다. 복수의 네트워크에 설치하거나, 공격 방지, 공격 탐지나 효율적인 대응을 위하여 다른 개체들에 의존한다.

4.3 설치 위치에 따른 분류

설치 위치에 따라 *희생자, 중간, 혹은 소스 네트워크*에 설치된 메커니즘으로 구분한다.

4.3.1 희생자 네트워크

희생자 네트워크에 설치된 DDoS 방어 메커니즘은 네트워크를 DDoS 공격으로부터 보호하며 희생자에 대한 영향을 감소시킴으로써 탐지된 공격에 대응한다. 전통적으로 대부분의 방어 시스템은 희생자에 설치되었다. 예로써 자원 계정, 프로토콜 보안 메커니즘 등이 있다.

4.3.2 중간 네트워크

중간 네트워크에 설치된 DDoS 방어 메커니즘은 많은 수의 인터넷 호스트에 대한 하부구조적 DDoS 방어 서비스를 제공한다. 예로써 푸시백 및 역추적 기법 등이 있다.

4.3.3 소스 네트워크

이 메커니즘의 목적은 네트워크 고객들이 DDoS 공격을 생성하는 것을 방지하는 데 있다. 그러나 이 방법은 이 서비스와 관련된 비용을 누가 지불할 것인가가 불분명하기 때문에 설치 동기가 낮다.

V. Champagne의 DDoS 대응 기법 분류

[3]에서는 DDoS 대응 기법을 DDoS 공격에 의한 손상을 완화시키기 위한 방법, DDoS 공격 발생을 예방하는 방법, 미래의 DDoS 공격을 억제하기 위한 방법으로 구분하고 있다.

5.1 DDoS 완화(mitigation)

제안된 DDoS 대응 기법의 주요 범주는 진행 중인 공격의 영향을 완화시키는 것이다. 이것은 다시 서버, 네트워크 혹은 클라이언트 기반 완화를 위한 별개의 기술로 분류될 수 있다.

5.1.1 네트워크 기반 완화 기술

가) 혼잡 제어

어떤 부분의 트래픽을 다른 것으로부터 고립시키는 정책을 적용함으로써 공격 탐지 메커니즘에 대한 필요 없이 악성 행위의 영향을 제한시킬 수 있는 방법이다. 적용되는 함축 레벨에 따라서 링크, 플로 혹은 통합(aggregate) 레벨로 다시 분류될 수 있다.

- 링크: 각 입력 링크에 대하여 버퍼를 라우터가 유지하고, 패킷을 라운드-로빈 기반으로 각 버퍼로부터 순서대로 전달하는 방식이다.
- 플로: 패킷을 네트워크 근원지와 목적지에 따른 플로로 분류하여, 과부하 라우터가 특정 입력 링크가 아닌 어떤 플로의 유입을 억제하도록 구성하는 방식이다. 이런 라우팅 정책은 정상적으로 동작하는 플로에 대하여는 영향을 미치지 않게 된다.
- 통합: 통합이란 패킷의 근원지와 목적지뿐만 아니라, 응용이나 프로토콜 유형과 같은 공통 특성을 가지는 패킷들의 그룹으로 정의된다. 특정 통합 트래픽을 나머지로부터 고립함으로써 관련되지 않은 트래픽에 대한 DDoS 공격의 영향을 감소시킬 수 있는 더 정확한 필터링이 가능하게 된다.

나) 네트워크 구성

이 방식은 DDoS 공격으로부터 보호를 하기 위하여 네트워크나 서버의 물리적 혹은 논리적 구성을 변경하는 것이다.

- 중복성: 서버 처리 용량을 증가시키기 위하여 중복성(redundancy)을 도입하는 기법이다. 서버 로드의 증가가 어떤 클라이언트에게도 영향을 미치지 않도록 항상 모든 입력 트래픽을 처리하도록 하는 것이다. 서버가 Flashcrowds뿐만 아니라 DDoS 공격에 견디도록 도와주는 기법이다. Flashcrowds는 합법적인 사용자로부터 다량의 콘텐츠 요구로 인한 갑작스런 트래픽 버스트를 의미한다.
- 오브레이: 기본 인프라 위에 다른 계층의 네트워킹 컴포넌트를 추가하거나 이미 존재하는 노드들의 기능을 확장하는 방식이다. 예를 들어, Secure Overlay Service(SOS)[7]에서는 패킷을 어떤 서버

로 경로 배정하기 위하여 해시-기반 알고리즘을 사용하는 라우터의 오브레이 네트워크를 제공한다. 해당 서버에 통신을 원하는 외부 호스트는 Secure Overlay Access Point(SOAP)를 먼저 접촉하여야 하며, 그 지정된 라우터가 근원지를 인증한 후 오브레이에 패킷을 들어올 수 있게 한다.

- 로밍: 많은 알려진 공격 도구들이 DNS 룩업없이 공격을 수행한다는 사실을 이용하여, 공격 하에 있는 서버가 자신의 IP 주소를 변경하는 방식이다.

다) 시그니처 필터

반응 활동에 따라, 시그니처-기반 메커니즘은 다시 지역 필터링과 추적 메커니즘으로 구분된다.

- 지역 필터링: 특정 시그니처를 가진 패킷들이 악성으로 결정되면, 같은 시그니처를 가진 후속적인 입력 패킷들은 폐기되든지 혹은 율-제한된다.
- IP 추적: 공격 패킷 스트링의 근원지를 찾아내려고 하는 DDoS 대응 메커니즘이다. 경로 데이터를 수집하는 방법에 따라 다시 능동적 추적 메커니즘과 수동적 메커니즘으로 구분된다. 능동 메커니즘은 악성 스트림에 대한 정보를 얻기 위하여 상류의 라우터들에게 반복적으로 질의를 보낸다. 수동 메커니즘은 중간 네트워크가 자동으로 경로 정보를 희생자에게 전송한다.

능동 메커니즘은 다시 Memoryless와 히스토리-기반 방법으로 구분된다. 앞의 방법은 중간 네트워크 내의 라우터에게 전달된 패킷에 대한 정보 저장을 요구하지 않는 반면에, 뒤의 방법은 요구하는 방법이다. 수동 메커니즘은 메시지-기반과 헤더 마킹 방법으로 다시 구분된다. 메시지-기반 방법은 패킷의 경로 상에 있는 노드들이 추적 정보를 포함하는 여분의 패킷을 생성하는 것이고, 헤더 마킹 기법에선 라우터가 IP 패킷의 헤더 내에 경로 정보를 포함시킨다.

라) **QoS**

네트워크 대역폭 고갈을 목표로 하는 공격에 대처하는 한 가지 가능한 방법은 어떤 범주의 트래픽에게 대역폭의 몫을 예약해주는 서비스 차등 메커니즘을 도입하는 것이다. 이런 등급 메커니즘을 도입하여 네트워크에 의하여 다르게 패킷들을 처리한다.

5.1.2 서버

서버에 대한 DDoS 공격에 대응하기 위한 전략으로 주로 소프트웨어로 처리된다.

가) **DDoS-**인지 알고리즘

운영체제가 DDoS 공격의 영향을 완화시키기 위하여 사용하는 방식이다. 예를 들어, TCP 연결 큐를 주기적으로 스캔하여 반-개방 연결을 탈락시키는 방법, Lazy Receiver Processing(LRP)[8] 등이 있다.

나) 자원 계정

CPU 시간이나 네트워크 대역폭 같은 시간-다중화 자원의 할당을 제어하는 정책을 실행하는 방식이다. 예를 들어, Escort[9]가 있다.

5.1.3 클라이언트

클라이언트 트래픽에 대한 조절을 강제하기 위하여 클라이언트 호스트의 제한된 계산 자원과 금전적 자원을 이용하는 방식이다.

5.2 DDoS 예방

DDoS 공격의 발생을 사전에 예방하기 위하여 구현되는 능동적 대처 방식이다.

- 필터링: 유효하지 않은 정보나 해로운 정보를 가진 패킷들을 필터링을 통하여 잡아내는 방식이다.
- 프로토콜: DDoS 공격 기회를 제공하지 않는 프로토콜을 설계하는 방법은 아직도 해결되지 않은 연구 문제이다. 예를 들어, TCP SYN 공격을 방지하기 위하여 상태를 유지하는 부담을 서버로부터 클라이언트로 전가시키는 무-상태(stateless) 프로토콜을 설계할 수 있다. SYN 쿠키 방법이 한 예이다.
- 좀비 예방: DDoS 공격자가 좀비 컴퓨터를 구성하지 못하도록 사전에 방지하는 방식이다. 이를 위하여 인터넷에 연결된 호스트의 통제를 얻기 위하여 공격자가 이용할 수 있는 취약점을 없앨 필요가 있다. 예를 들어, 공격자들이 많이 이용하는 버퍼 오브플로 취약점이 소프트웨어나 하드웨어 메커니즘으로 완화될 수 있다.

5.3 억제

DDoS 공격을 억제하는 방식으로 하니팟과 포렌식이 있다

- 하니팟: 정상적인 운영체제에서, 루트킷이 공격자 추적을 포함하기 위하여 사용될 수 있다. 진보된 하니팟 시스템에서는 OS가 로깅 프레임워크 내에 캡슐화되어 모든 공격자 활동이 기록된다.
- 포렌식: 포렌식 활동을 통하여 공격자의 신원을 찾아내는 것이 가능하다.

VI. DDoS 대응 기법 과제와 설계 목표

DDoS 문제의 심각성과 증가된 빈도로 여러 가지의 대응 기법들이 제안되었다. 그러나 많은 솔루션들이 개발되었음에도 불구하고, 아직 문제는 제대로 다루어지지 않고 있으며, 해결되지 않은 상태이다. DDoS 대응 연구의 진보를 방해되는 여러 가지 심각한 요인을 아래와 같이 지적한다[2]:

- 인터넷상의 많은 지점에서 분산된 대응 필요: DDoS 공격에 효과적인 대응을 위하여 분산 협동 대응 시스템을 가질 필요가 있다. 현재 인터넷의 관리 방법 상 이것이 쉽지 않다는 것이 문제이다.
- 경제적 · 사회적 요인: 분산 대응 시스템이 DDoS 공격으로부터 직접적인 손해를 보지 않는 소스나 중간 네트워크에 의해서도 설치되어야 한다는 것이다. 따라서 대응 솔루션들이 드물게 설치되어, 매우 제한된 효과만 가져올 수 있다.
- 상세 공격 정보의 부족: 여러 가지의 공격 유형에 대한 정보와 공격 율, 기간, 패킷 크기, 에이전트 머신의 수, 시도된 대응 및 유효성, 피해 규모 등에 대한 정보가 부족하다.
- 대응 시스템 벤치마크의 부족: 현재까지 대응 시스템 사이의 비교를 할 수 있는 공격 시나리오나 확립된 평가 방법론의 벤치마크 suite가 없다는 지적이다.
- 대규모 시험의 어려움: DDoS 대응이 실제적인 환경에서 시험될 필요가 있는데, 인터넷상에서 실제 분산 실험을 수행할 수 있는 대규모 테스트 베드나 안전한 방법이 없다는 것이다. 대응 시스템의 성능이 소규모 실험과 시뮬레이션 기반이라 신뢰적이지 못하다는 지적이다.

[3]에서는 DDoS 대응 기법에 대한 분류를 기초로 DDoS 대응 기법의 과제를 해결하기 위하여 다음과 같은 설계 목표를 제시 한다:

- 저가 솔루션의 제공: ISP와 DDoS 공격의 잠재적인 희생자에 의한 광범위한 채택을 위하여 저가로 솔루션을 제공해야 한다. 또한 낮은 계산 오버헤드와 작은 메모리 자원을 요구해야 한다.
- 진행 중인 공격이 없을 때는 성능을 저하시키지 않아야 한다: ISP 네트워크의 고-대역폭 라우터에 대한 수정이 필요한 경우 특히 중요하다.
- 확장성: 추가 자원에 대한 보호가 필요할 때 방어 시스템을 확장하는 것이 가능해야 한다.
- 합법 · 악성 트래픽의 통합을 고려: 공격자와 합법적인 클라이언트로부터의 패킷들이 같은 서브넷을 향하여 통합되고 링크를 공유함에 따라, 방어 시스템은 업 스트림 필터링이나 정확한 다운스트림 패킷 분류를 수행할 수 있어야 한다.
- 다수의 개별 정상-행위 플로로 이루어진 공격 처리: 봇넷을 구성한 교모하게 공격하는 공격자를 저지할 필요가 있다.
- 빠르게 변하는 특성을 가진 공격과 간헐적 공격에 적응해야 한다.
- 희생자의 부하에 방어 메커니즘의 반응을 조절할 수 있어야 한다.
- Flashcrowds와는 최소한의 간섭이 있어야 한다.
- 위조 정보의 경우에도 유효해야 한다.
- 점진적인 설치를 허용해야 한다: 네트워크, 클라이언트나 서버에서의 변경 작업이 즉시에 같이 수행될 수 없기 때문에, 아직 완전하게 설치되기 전이라도 어떤 보호를 제공해야 한다.

위와 같은 설계 목표를 달성하기 위하여 다음과 같은 설계 원칙을 제시한다:

- 분산 방어 메커니즘: 확장성이 있고, 악성 집단이 메커니즘 공격을 하는 것을 더욱 어렵게 만들고, 합법 · 악성 트래픽의 통합을 제한하는 방어 조처를 가능하게 한다.
- 협동 메커니즘: 전역적인 정보를 제공함으로써 분산 대응 방법의 효율성을 증가시킨다.
- 정보 요구의 최소화: 대응을 위하여 많은 정보가 필요 할수록, 계산적, 메모리, 네트워크 대역폭 오브헤드가 많이 요구된다.

· 독립적으로 유용한 메커니즘: 다른 노드의 간섭 없이 모든 노드는 독립적으로 기능이 가능해야 한다.

VII. 맺음말

DDoS 공격이 인터넷의 안정성과 신뢰성에 심각한 위협을 제공하고 있다. 공격은 점점 더 정교화되고 조직화 되고 있으며, 이러한 공격에 대응하기 위하여 많은 대응 기법도 제안되었다. 이처럼 DDoS 공격이 다양화되고 복잡화됨에 따라, 기존의 대응 기법들이 DDoS에 얼마나 효과적인지에 대하여도 아는 것이 쉽지 않게 되었다. 따라서 본 논문에서는 DDoS 공격과 대응 기법의 분류를 통하여 유사성과 차이점을 알아보고, 효과적인 대응책의 수립을 위한 기초 자료를 제공하고자 하였다.

DDoS 공격 및 대응 기법의 분류가 사용될 수 있는 용도는 아래와 같다[2].

· DDoS 연구 분야 지도: DDoS 분야의 빠른 소개를 위한 보편적인 개관을 제공한다.
· 신규 공격 전략 조사: 알려진 위협 이외의 새로운 공격 방법을 소개한다.
· DDoS 벤치마크 생성: DDoS 방어 평가를 위한 공격 벤치마크 생성을 제공한다.
· 공통 어휘: 공격 메커니즘과 솔루션의 서술적인 설명에 필요한 공통 어휘를 제공한다.
· 공격 등급-특정 솔루션의 설계: 모든 가능한 공격을 위한 만능의 DDoS 방어는 비현실적이다. 분류는 DDoS 위협의 부분집합 식별과 맞춤식 솔루션의 설계를 쉽게 한다.
· 솔루션 제한의 이해: 대응 기법에 따른 공통적인 성능 제한과 약점을 이해함으로써, 문제 해결을 위한 노력에 초점을 맞출 수 있다.
· 신규 연구 분야 조사: 다른 종류의 공격에 대한 다른 방어 메커니즘들의 효율성을 조사함으로써 신규 연구 분야에 대한 제시를 한다.

국내에서도 정보통신 환경 전반을 보호할 수 있는 국가 차원의 DDoS 공격에 대한 종합 대응 체계 개발이 필요하다고 사료된다.

참고문헌

[1] Jelena Mirkovic, D-WARD: Source-End Defense Against Distributed Denial-of-Service-Attacks, Ph. D. dissertation, Computer Science, UCLA. 2003.

[2] Jelena Mirkovic and Peter Reiher, "A Taxonomy of DDoS Attack and DDoS Defense Mechanisms", Computer Communication Review, Vol. 34(2), pp. 39-53, 2004.

[3] David Champagne and Ruby B. Lee, "Scope of DDoS Countermeasures: Taxonomy of Proposed Solutions and Design Goals for Real-World Deployment", http://palms.ee.princeton.edu/ PALMSopen/champagne06DDoS.pdf.

[4] 전용희, "봇넷 기술 개요 및 분석", 한국정보보호학회지 제18권 3호, pp. 101-108, 2008년 6월.

[5] SANS Institute, NAPTHA: A new type of Denial of Service Attack, Dec. 2000. http://rr.sans.org/threats/naptha2.php.

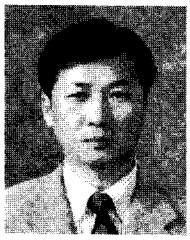
[6] J. Ioannidis and S. M. Bellovin, "Pushback: Router-Based Defense Against DDoS Attacks", In Proceedings of NDSS, Feb. 2002.

[7] D. K. Angelos, et al., "SOS: secure overlay services," in Proc. of the 2002 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications, pp. 61-72, Aug. 2002.

[8] P. Druschel and G. Banga, "Lazy receiver processing(LRP): a network subsystem for server systems," in Proc. of the 2nd USENIX Symposium on Operating System Design and Implementation (OSDI), pp. 261-275, Oct. 1996.

[9] O. Spatscheck and L. L. Peterson, "Defending against denial of service attacks in Scout," in Proc. of the 3rd USENIX Symposium on Operating System Design and Implementation (OSDI), pp. 59-72, Feb. 1999.

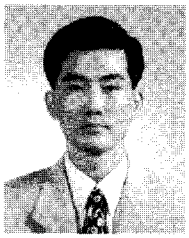
〈著者紹介〉



전 용 희 (Yong-Hee Jeon)

종신회원

1971년 3월~1978년 2월: 고려대학교 전기전자전파공학부
1985년 8월~1987년 8월: 미국 플로리다 공대 대학원 컴퓨터공학과
1987년 8월~1992년 12월: 미국 노스캐롤라이나주립 대학원 Elec. and Comp. Eng. 석사, 박사
1978년 1월~1978년 11월: 삼성중공업(주)
1978년 11월~1985년 7월: 한국전력기술(주)
1979년 6월~1980년 6월: 벨기에 벨가톰사 연수
1989년 1월~1989년 6월: 미국 노스캐롤라이나주립대 Dept of Elec. and Comp. Eng. TA
1989년 7월~1992년 9월: 미국 노스캐롤라이나주립대 부설 CCSP (Center For Comm. & Signal Processing) RA
1992년 10월~1994년 2월: 한국전자통신연구원 광대역통신망연구부 선임연구원
1994년 3월~현재: 대구가톨릭대학교 컴퓨터 · 정보통신공학부 교수
2001년 3월~2003년 2월: 대구가톨릭대학교 공과대학장 역임
2004년 2월~2005년 2월: 한국전자통신연구원 정보보호연구단 초빙연구원
2007년 1월~2007년 12월: 한국정보보호학회 학회지 편집위원장
2008년 1월~현재: 한국정보보호학회 부회장
2009년 1월~현재: 한국정보과학회 정보보호연구회 위원장
<관심분야> 네트워크 보안, 웜 모델링 및 대응 기술, 통신망 성능분석



장 종 수(Jong-Soo Jang)

종신회원

1984년: 경북대학교 전자공학과 학사
1986년: 경북대학교 대학원 전자공학과 석사
2000년: 충북대학교 대학원 컴퓨터공학과 박사
1989년 7월~현재: 한국전자통신연구원 지식정보보안연구부 책임연구원
2008년 1월~현재: 한국정보보호학회 부회장, 학회지 편집위원
2008년 1월~현재: 한국정보처리학회 이사, 논문지 편집위원
2009년 1월~현재: 대한전자공학회 통신소사이티 이사
<관심분야> Network Security, 정책기반보안관리, 비정상트래픽탐지, 유해정보차단

오 진 태(Jintae Oh)

정회원

1990년 2월: 경북대학교 전자공학과 공학사
1992년 2월: 경북대학교 전자공학과 석사
1992년 2월~1998년 2월: 한국전자통신연구원 책임연구원
1998년 3월~1999년 1월: 미국 Min Max Tech. 연구원
1999년 2월~2001년 10월: 미국 Engedi Networks. Director
2001년 10월~2003년 1월: 미국 Winnow Tech. Co-founder, CTO 부사장
2003년 3월~현재: 한국전자통신연구원 지식정보보안연구부 책임연구원
2008년 1월~현재: 한국정보보호학회 학회지 편집위원(간사)
<관심분야> 네트워크보안, 비정상행위탐지기술, 공격 시그니처 자동생성기술, 보안하드웨어기술