# 유비쿼터스환경에서의 DDoS의 공격과 탐지, 방어시스템에 관한 연구

정창덕, 차주원, 황선일

# A study on DDoS Attack, Detecting and Defence in ubiquitous system

chang-duk Jung , joo-won Cha, sun-il Hwang

< Abstract >

The underlying success of logistics depends on the flow of data and information for effective management. Over the last 30 years, we have seen the power of microprocessors double about every 18months. This continuing trend means that computers will become considerably smaller, cheaper, and more abundant; indeed, they are becoming ubiquitous and are even finding their way into everyday objects, resulting in the creation of smart things. In the long term, ubiquitous technologies will take on great economic significance. Industrial products will become smart because of their integrated information processing capacity, or take on an electronic identity that can be queried remotely, or be equipped with sensors for detecting their environment, enabling the development of innovative products and totally new services. The global marketplace runs on logistics, security, speed, agility and flexibility..In this paper we report that pairing these traditional logistics functions with RFID technology can be a huge value-driver for companies. This winning combination yields increased logistics management effectiveness and more efficient visibility into the supply chain management.

## Ⅰ. 서 론

유비쿼터스환경이 빠르게 변하고 있다, 최근의 해킹·바이러스는 단일 시스템을 대상으로 한 공격에서 발전하여 네트워크 인프라를 위협할 수 있는 대규모 공격으로 발전하고 있다. Yahoo, 아마존, CNN 등 굴지의 인터넷 관련한 기업들이 대규모 DDoS 공격으로 막대한 피해를 입었으며, 국내에서도 지난 1.25 인터넷 침해사고로 인해 전국적인 규모의 인터넷 장애가 발생되기도 하였다. 또한, 최근에는 개인 PC를 공격한 후 원격 제어가 가능한 bot을 설치하여 수천~수만개의 zombie 시스템들을 거느린 botnet을 형성하고 이를 이용한 대규모 공격도 커다란 위협으로 등장하고 있다.

이처럼 대규모 피해를 유발시키는 주된 원인은 분산서비스거부공격(DDoS)과 인터넷 웜이 라는 2개의 파괴적인 공격에서 찾아볼 수 있다. 이 두 공격의 공통점은 한 대의 컴퓨터만을 이용하지 않고 수십~수만대의 컴퓨터를 공격에 이용하거나 감염시킨다는 점이다. 이로인해 네트워크 사업자 입장에서도 기존의 단순한 한 해커에 의한

시스템 침입의 경우 ISP 망에 아무런 영향을 주지 않지만 DDoS와 인터넷 웜은 ISP 망의 품질이나 건전성을 떨어뜨리고, 고객 서비스에 막대한 지장을 초래하는 주요 원인이 되고 있다. 2000년 대규모 DDoS 공격의 여파로 인해 미국 정부에서는 정부기관, CERT, ISP 등의 전문가가 참가하는 워크샵을 개최하여 이러한 대규모 DDoS 공격에 대응할 수 있는 방안을 강구하는 등의 노력을 하였다. 이러한 노력들의 일환으로 망 운영 경험이 풍부한 ISP 운영자와 네트워크 장비 개발자들이 낸 아이디어가 본 문서에서 소개하고자 하는 원격구동 블랙홀 라우팅 (Remote Triggered Blackhole Routing) 기술과 DDoS 공격을 추적할 수 있는 Sinkhole 기술이다.
원격구동 블랙홀 라우팅 기술은 관리 하에 있는 다수의 edge 라우터들을 원격에서 제어하여 특정 목적지로 향하거나 특정한 IP 주소로부터 발생된 대규모 패킷들을 효과적으로 차단시킬 수 있는 기술이다. 이 기술의 장점은 기존의 네트워크 환경하에서 추가적인 보안장비의 도입이 필요 없고, 네트워크 장비의 성능에도 많은 영향을 주지 않으면서 손쉽게 다수의 공격 블랙리스트를 관리할 수 있다는 것이다. 또한 Sinkhole 기술 역시 비용을 효과적으로 DDoS 공격 근원지를 추적하고 공격 내용을 분석할 수 있는 기술이다.

이 기술들은 북미네트워크운영자그룹(NANOG) 등에도 소개되었으며, 국내 ISP, IDC 등 대규모 네트워크를 관리하는 기관에서도 이 기술들을 적용함으로써, 보다 신속하고 경제적으로 대규모 DDoS 공격 차단 및 추적이 가능할 것으로 생각된다. 본 문서의 제2장에서는 최근 분산화·대규모화 되어 가고 있는 인터넷 공격기술의 변화를 살펴보고 이에 대응하기 위한 기존의 방어기술의 종류와 그 한계를 분석해 본다.
제3장에서는 대규모 공격을 차단할 수 있는 원격구동 블랙홀 라우팅 기술의 개념과 목적지 기반 원격구동 블랙홀 라우팅 기술 및 출발지 기반 원격구동 블랙홀 라우팅 기술의 구현 방법을 구체적으로 살펴보도록 한다.
제4장에서는 공격자를 추적하고 공격패킷을 분석할 수 있는 싱크홀 기술에 대해 살펴보고 제5장에서 결론을 맺기로 한다. 그리고, 분산서비스거부공격이 발생하였을 경우 국제 관문국, ISP 백본, edge 라우터, 가입자 라우터 등 각 지점에서 대응할 수 있는 시나리오와 Blackhall, CAR, uRPF, PBR, EACL 의 부하 발생에 대한 자체 분석결과를 부록으로 첨부하였다.

# Ⅱ. 본론

## 2. 인터넷 공격기술의 변화와 기존 방어기술의 한계

가. 인터넷 공격기술의 변화
최근 공격방법의 변화에 대해서 한마디로 이야기하라면 “분산 공격의 일반화”라고 할 수
있을 것이다. 분산공격이라고 하면 한 대의 시스템을 이용한 공격이 아닌 다수의 시스템 을 공격에 이용한 공격으로써 공격의 효과나 파괴력이 대단히 강력하다. 가장 대표적인 예가 DDoS 공격으로써 공격에 이용되는 master 시스템이나 slave 시스템들이 모두 이미 exploit된 시스템들로써 한 번의 공격에 수십~수천대의 시스템들이 동원되기도 한다. 공격에 이처럼 다수의 시스템들을 이용하는 이유는 여러 가지가 있을 수 있다.
첫째, 공격에 이용할 수 있는 취약한 서버들을 쉽게 구할 수 있는 환경 때문이다. 인터넷 웜에 의해 이미 공격당한 서버들은 일반적으로 특정한 포트를 백도어로 열어놓고 있어 이용이 용이하고, 신규 취약점을 이용하는 웜을 퍼뜨려 다수의 시스템들을 일시에 장악하는 것도 어렵지 않다. 실제 인터넷 웜 감염 시 DDoS agent가 설치되는 경우를 흔히 볼 수 있다.
둘째, 보다 강력한 공격을 위해 공격 자원(컴퓨팅 파워, 네트워크 대역폭 등)을 최대한 많이 확보하기 위해 분산된 다수의 시스템들을 이용한다. 공격을 받는 사이트뿐만 아니라 공격을 하는 사이트도 많은 자원을 소진해야 하므로 가능하면 많은 사이트를 이용하게 된다.
DDoS 공격도 시간의 흐름에 따라 많은 변화를 거듭하고 있다. DDoS 공격의 초창기인 1999년, 2000년 당시의 대표적인 DDoS 공격 도구들은 다음 표와 같다.

초창기의 DDoS 도구들은 대부분 SUN 또는 리눅스 시스템들을 해킹한 후, DDoS를 위한 Zombie 시스템으로 활용하고, 특정한 포트를 이용하여 Zombie

[표 1] 초창기의 DDoS 공격 도구들

| DDoS 도구 | 특징 |
|---|---|
| trinoo | 1524/tcp, 27665/tcp, 27444/tcp, 31335/udp 사용 |
| TFN | ICMP ECHO, ICMP ECHO REPLY 사용 |
| stacheldraft | 16660/tcp, 65000/tcp, ICMP ECHO, ICMP ECHO REPLY 사용 |
| Shaft | 20432/tcp, 18753/udp, 20433/udp 사용. 포트번호 변경 기능 사용 |
| TFN2K | 정해진 포트 사용치 않음. 포트번호 변경 기능 사용 |

시스템들에게 공격 명령을 내렸다.
초창기의 DDoS 공격에 비해 현재의 DDoS 공격이 가지는 가장 큰 차이점은 다음 두 가지에서 찾아 볼 수 있다.
첫째, 윈도우즈 시스템을 Zombie 시스템으로 사용한다.
초창기의 DDoS 공격은 대부분 리눅스 시스템을 Zombie로 이용하고 있으나 최근에는 윈도우즈 시스템을 DDoS 공격에 이용하고 있다. 이는 개인용 PC의 컴퓨팅 성능이 서버급 못지않게 향상되었고, 가정마다 초고속 인터넷이 설치되어 공격에 필요한 네트워크대역폭이 확보되었으며, 서버에 비해 상대적으로 보안이 취약해 DDoS 공격에 이용하기 에는 최적의 조건을 갖추고 있기 때문이다. 공격에 이용하는 시스템이 서버급 시스템에서 광범위하게 사용하는 가정용 PC로 바뀐 공격 패러다임의 변화는 DDoS 공격의 파괴력을 한층 높이고 피해 범위도 광범위해 질 수 있다는 것을 의미한다.
둘째, 제어를 위해 IRC(Internet Relay Chat) 채널을 사용한다.
초창기의 DDoS 공격은 특정한 포트를 이용하여 명령을 전달하여서 이 포트를 모니터링 함으로써 쉽게 공격을 탐지하고 차단할 수 있었다. 하지만 최근에는 명령하달을 위한 채널을 IRC를 이용하는 경우가 많다. IRC는 다수의 사용자들이 인터넷상에서 서로 채팅을 할 수 있는 프로그램으로 최근의 DDoS 공격 툴들은 IRC 채널을 활용하여 명령을 전달함으로써 탐지와 차단을 어렵게 하고 있다.
최근 이러한 특성을 가진 DDoS 공격은 윈도우즈 시스템을 해킹한 후 설치되는 Bot에 DDoS 공격기능이 내재되어 있어 이루어지는 경우가 많다. Bot은 MS 윈도우 취약점, 웜·바이러스에 의한 백도어, 패스워드 설정 미비 등으로 인해 감염되고 있으며, 이 Bot들은 분산서비스거부공격, 스팸발송, 와레즈 사이트 개설 등에 사용된다. Rbot, Phatbot, Agobot, Sdbot 등 2,000여종 이상의 변종 bot이 존재하며, 국내에서도 수십만대의 PC가 감염된 것으로 추정하고 있어 국내 네트워크 인프라에도 엄청난 잠재적인 위협으로 작용 할 수 있을 것으로 보인다.

나. 기존 방어기술의 종류와 한계

대규모 인터넷 공격이 증가함에 따라 각 ISP에서도 각종 네트워크 장비나 보안솔루션을 동원하여 네트워크 모니터링과 유해 트래픽 차단 등의 조치를 취하고 있지만 광대역 네트워킹 환경하에서 장비의 성능이나 기능이 만족할 만한 수준은 아니다. 네트워크 차원에서 서비스거부공격에 대한 기존의 방어기술로써 대표적인 것은 ACL, null0 라우팅, uRPF, Rate-Limit 등이 있으며, 공격에 대한 추적을 위해서는 트래픽 흐름을 분석할 수 있는 Netflow 기술 등이 있다.

□ ACL(Access Control List)
가장 일반적인 유해 트래픽 차단 기술로써 IP주소, 서비스 포트 그리고 컨텐츠를 기반으로 한 차단이 가능하다. 하지만 이 방법은 접근통제를 위한 별도의 ASIC화된 모듈이 없을 경우 네트워크 장비에 많은 부담을 주어 성능저하의 원인이 될 수 있다. 또한 ISP와 같이 많은 네트워크 장비를 보유하고 있는 기관의 경우, 이들 장비들에 접근통제 정책을 업데이트하기 위해서 별도의 스크립트를 작성하거나, 그렇지 않은 경우 개별적으로 로그인하여 설정을 변경하여야 하는 어려움이 있다.

1.25 인터넷 침해사고시에도 많은 ISP들이 1434 포트에 대한 접근통제를 수동으로 행하여 대응이 신속하게 이루어지지 않았으며, 일부 노후화된 장비에서는 접근통제 설정에 따른 과부하로 인해 설정하지 못한 경우도 있었다.
□ Null0 라우팅
특정한 목적지로 향하는 패킷들을 Null0라는 가상 인터페이스에 포워딩함으로써 drop 시킬 수 있는 기술이다. 이 기술은 국외에서는 블랙홀 라우팅 또는 블랙홀 필터링이라고 불리고 있지만, 국내에서는 대부분 Null0 라우팅이라고 한다. 이 기술은 네트워크 장비의 기본 기능인 포워딩 기능을 이용하므로 ACL 기술에 비해 장비의 과부하가 거의 없으나, IP 기반(L3)의 필터링만 제공할 수 있고, 서비스 포트(L4)나 컨텐츠(L7)에 의한 필터링은 불가능한 단점을 가지고 있다.
□ uRPF(unicast Reverse Path Forwarding)
출발지 IP주소를 위장(IP Spoofing)한 공격을 차단해 줄 수 있는 기술로써, 라우터가 패킷을 받으면 출발지 IP 주소를 확인하여 해당 IP로 갈 수 있는 역경로(Reverse Path)가 존재하는지 확인함으로써 출발지 IP 주소의 신뢰한다.
대부분의 DoS 또는 DDoS 공격이 자신의 출발지 주

소를 위장하므로 uRPF는 상당히 효과적인 서비스거부공격 차단 수단이 될 수 있다. 하지만, 이 기술 역시 다수의 라우팅 경로가 존재하는 비대칭 망구조를 가지고 있을 경우 적용의 한계(strict 모드 사용 못함)가 있으며, Spoofing을 방지하는 것 이외에 다양한 서비스거부공격에 대한 대응 기능이 존재
하지 않는다.

□ Rate-Limit 기술
특정 서비스 또는 패턴을 가진 패킷이 단위시간 동안 일정량 이상 초과할 경우 그 이상의 패킷을 통과시키지 않도록 하는 기술을 Rate-Limit 기술이라고 한다. 이 기술은 rate filtering이라고도 하며, Cisco에서는 CAR(Commit Access Rate)로 구현하고 있다. 이 기술은 Syn flooding 공격시 Syn 패킷의 Bandwidth 제한, Smurf 공격시 ICMP 패킷의 Bandwidth 제한 등에 유용하게 사용될 수 있다. 하지만, 비정상적인 패킷뿐만 아니라 정상적인 패킷도 차단될 수 있으며, 해당 기능을 수행하는 전용 모듈이 없을 경우 라우터에 과부하를 유발시킬 수 있는 단점이 있다.

□ Netflow
트래픽 흐름 분석(Traffic Flow Analysis)을 통해 소스 및 대상 주소, 각 flow의 바이트 수 및 패킷 수, 트래픽 유입 인터페이스 및 업스트림 피어 정보 등을 모니터링할 수 있다. Cisco에서 개발한
NetFlow는 트래픽 flow를 측정할 수 있는 대표적인 것으로써 이를 이용하여 Spoofing된 유해 트래픽이 어떤 인터페이스에서 유입되고 있는지 확인할 수 있다. 하지만, 이 기능을 이용한 공격자 추적은 공격로 상의 모든 네트워크 장비에 대한 접근권한이 주어져야 하고, 공격이 이루어지고 있을 동안 분석이 완료되어야 된다는 단점이 있다. Netflow는 공격자를 추적하는 것 이외에 실시간으로 네트워크를 모니터링하여 이상 징후를 탐지하는 용도로도 사용될 수 있다.지금까지 살펴본 기존의 기술들은 성능, 기능, 비용 등 많은 제약사항을 가지고 있어 실제 이를 이용한 대규모 공격에 대한 차단과 추적에는 한계가 있다. 또한, Firewall, IPS(Intrusion Prevention System), L7 스위치 등 기존의 보안장비도 DDoS, 웜 등에 대한 차단과 추적기능을 가지고 있지만, 성능과 비용의 문제점들을 가지고 있으며, 특정 사이트가 아닌 전체 ISP망을 제어하기에는 역부족이다.

[표 2] 원격구동 블랙홀 라우팅 기술과 기존 기술의 비교

| 구분 | Null0 라우팅 | ACL | 원격구동 블랙홀 |
|---|---|---|---|
| 제어 수준 | L3 레벨 | L3, L4, L7 레벨 | L3 레벨 |
| 적용시 성능 문제 | 성능저하 거의 없음 | 성능저하 발생 가능 | 성능저하 거의 없음 |
| 원격구동 가능성 | 불가능 | 불가능 | 가능 |
| 다수장비 동시제어 | 불가능 | 불가능 | 가능 |
| 핵심 기술 | 포워딩 기술 | 필터링 기술 | 포워딩 기술 + iBGP |

앞으로 살펴볼 원격 구동 블랙홀 라우팅 기술은 기존에 존재하는 몇 가지 기술을 조합하여 대규모 공격에 효과적으로 대응할 수 있는 기술로써 기존의 기술과 비교해 보면 다음과 같은 차이점이 있다.

원격구동 블랙홀 라우팅 기술은 L4, L7 수준의 정교한 제어는 불가능하지만 원격에서 다수의 장비를 동시에 제어할 수 있고, 장비의 성능에도 거의 영향을 미치지 않아 ISP와 같은 대규모 네트워크 관리기관에서 적용하기에는 상당히 효과적인 기술이라고 할 수 있다.

# Ⅲ. 결론

5. 결론
DDoS나 인터넷 웜 공격에 대한 대응은 대단히 어려운 과제이다.
본 문서에서 소개한 많은 기술들도 완벽하게 DDoS 공격을 차단하고 제거하지는 못한다. 원격구동 블랙홀 라우팅 기술도 공격자가 공격 목표 설정시 IP 주소가 아닌 도메인 네임을 사용하거나, 피해기관의 DNS 엔트리 변경을 쫓아서 공격 대상 IP를 바꾸어서 공격할 경우 대응의 한계를 가진다. 하지만, 본 문서에서 소개된 기술들은 일반적인 DDoS 공격에 대해 상당히 비용 효율적이며, 효과적인 차단과 추적을 가능하게 한다.
이 기술들은 UUNet과 같은 거대 ISP망에서 이미 적용하여 그 안정성이 입증되었으며, 국내 ISP망에서도 네트워크 보안을 위해 이러한 기술들을 채택하는 것이 바람직하리라 생각된다. 물론 일부 국내 ISP에서는 이 기술을 이미 적용하고 있는 것으로 안다. 원격구동 블랙홀 라우팅 기술을 처음 제안한 미국 통신회사 UUNet은 2004년 초 고객 대상 DoS 공격을 15분 이내에 대응하겠다는 서비스수준협약서(SLA)를 발표하여 공격 차단에 대한 자신감을 보여주었다. 이 자신감은 본 문서에서 소개한 다양한 기술과 운용경험, 그리고 시스템화된 보안정책을 배경으로 하고 있는 듯 하다.
본 문서에서 소개한 기술들은 특별히 새로운 기술을 요하지는 않는다. 기존에 각기 다른 목적으로 사용되었던

null0 라우팅, iBGP 광고, uRPF, syslog logging 등을 조합하여, 새로운 대응방안을 마련한 것이다. 이러한 기술의 발상은 ISP 사업자, 통신장비 판매회사, 보안 전문가 등이 각자 서로의 아이디어를 교환하는 과정에서 얻어질 수 있었고, 지금도 새로운 기술들이 나오고 있으며, 이 기술에서 착안한 보안솔루션들도 만들어지고 있다.

우리나라는 자타가 인정하는 인터넷 강국이지만, 보안 측면에서는 부족한 면이 많다.

국내에서도 미국의 NANOG 처럼 서로의 망 운영 경험과 보안관리 경험을 나눌 수 있는 장을 보다 활성화시키고, 1.25 인터넷 침해사고와 같은 대규모 사건이 발생하기 이전에 미리 다양한 공격 가능성에 대해 검토하고 사전 훈련을 실시할 필요가 있다. 1.25 당침해도 많은 ISP 망 관리자들이 네트워크 장비에 대한 보안설정시 장비와 서비스에 미칠 수 있는  미리 정확히 몰라 설정을 망설였었다. 충분한 사전훈련이 있었다면 이러한 일은 없었을 것이다. 본 문서에서 소개한 기술들도 ISP망에서 미리 적용하고 각 ISP 환경에 맞도록 커스터마이징함으로써 실제 대규모 사고 발생시 신속하게 대응할 수 있을 것이다.

## 참고문헌


트래픽 분석을 통한 서비스거부공격 추적 :
http://www.krcert.or.kr/report/download.jsp?no=TR2003001&seq=0

Dissemination of flow specification rules, draft-marques-idr-flow-spec-00.txt :
http://www.tcb.net/draft-marques-idr-flow-spec-00.txt

Configuring BGP to Block Denial-of-Service Attacks :
http://www.watersprings.org/pub/id/draft-turk-bgp-dos-01.txt

How to Get Rid of Denial of Service Attacks :
http://www.bgpexpert.com/antidos.php

BlackHole Route Server and Tracking Traffic on an IP Network :
http://www.secsup.org/Tracking/

Unicast Reverse Path Forwarding (uRPF) Enhancements for the ISP-ISP Edge :
ftp://ftp-eng.cisco.com/cons/isp/security/URPF-ISP.pdf

Phase 1 Prepare the Tools and Techniques, Using IP Routing as a Security Tool :
ftp://ftp-eng.cisco.com/cons/isp/security/ISP-Security-Bootcamp-Singapore-2003/H-Preparation-Tools-v3-0.pdf

INTERNET PROTOCOL V4 ADDRESS SPACE :
http://www.iana.org/assignments/ipv4-address-space

MPLS Architecture and Applications :
http://mmlab.snu.ac.kr/research/hsn/workshop/hsn2001/data/jbc.pdf

MPLS-Based Synchronous Traffic Shunt :
http://www.nanog.org/mtg-0306/afek.html

MPLS-based Traffic Shunt :
http://www.securite.org/presentations/ripe46/COLT-RIPE46-NF-MPLS-TrafficShunt-v1.ppt

MCI To Offer New Protection Against Denial-Of-Service Attacks : http://informationweek.securitypipeline.com/news/18201396