情 報 保 護 學 會 誌
第19卷 第5號, 2009. 10

분산서비스거부(DDoS) 공격 통합 대응체계 연구

최 양 서*, 오 진 태*, 장 종 수*, 류 재 철**

요 약

지난 2009년 7월 7일부터 수차례에 걸쳐 청와대 및 다수의 중요 웹 사이트에 대해 분산서비스거부(Distributed Denial of Service, DDoS) 공격이 시도되었다. 이 공격에서 사용된 공격 방법은 공격 트래픽의 형태와, 공격 수행을 위한 공격 네트워크의 구성 방법에 있어서 기존의 방법과는 다른 형태를 띠었고, 이로 인해 공격탐지 및 차단이 쉽게 이루어지지 않아, 피해가 매우 컸다. 이와 같이 최근에는 기존의 DDoS 공격 탐지 및 차단 기술로는 쉽게 탐지 및 차단할 수 없는 고도화된 분산서비스거부 공격이 시도되고 있으며, 그로 인한 피해가 커지고 있는 상황이다. 분산서비스거부 공격은 이미 2000년 이전부터 발생하여온 오래된 공격임에도 불구하고 아직까지 이를 효과적으로 차단하지 못하고 있는 것이다. 이는 전체 정보통신 운영환경과 분산서비스거부 공격의 전체 공격 프로세스에 대한 심도있는 분석을 통해 인터넷 전반에 걸친 거시적인 DDoS 공격 대응 방안을 모색하는 것이 아니라, 개개의 공격 형태를 탐지하고 차단할 수 있는 방법을 모색했기 때문이다. 이에, 본 논문에서는 과거부터 현재까지 DDoS공격이 어떻게 발전해 왔는지를 분석하고, 현재 발생하고 있는 분산서비스 거부 공격의 공격 체계와 공격 기법에 대한 복합적 분석을 통해 현재의 고도화된 분산서비스 거부 공격을 효과적으로 차단할 수 있는 분산서비스거부 공격 통합 대응체계를 제안한다.

Ⅰ. 서 론

분산 서비스 거부(Distributed Denial of Service, DDoS) 공격은 최근에 발생한 신종 공격 기법이 아니다. 이미 1990년대 말부터 발생하기 시작하여 지난 2000년 야후, 아마존 등 유명 웹사이트에 대한 대대적인 DDoS 공격이 발생하였고, 그로인해 막대한 피해가 발생한 과거가 있다. 이러한 DDoS 공격을 탐지하고 차단하기 위해 이미 오래 전부터 관련 연구 및 기술개발이 시도되었고, 현재는 다양한 공격 대응 기법들이 개발되어 운영되고 있다[1,2,3].

그러나, DDoS 공격은 그 공격의 파괴력을 오히려 더욱 더 강화시키면서 현재도 계속 발생하고 있고, 그에 대한 피해 역시 계속되고 있다[4]. 최초 발생한지 10년이 지난 공격이 아직까지도 시도되고 그로 인한 피해가 지속적으로 발생하고 있는 것이다. 이는 DDoS 공격에 대한 전반적인 고찰 없이 시도되는 공격 형태만을 분석하여, 특정 형태의 공격을 탐지하고 차단할 수 있는 방법을 개발해 왔기 때문이다. 즉, 과거에 DDoS 공격에 사용되었던 공격 형태만을 탐지하고 차단할 수 있는 기술을 개발하여 적용하였기 때문인 것이다. 물론 최근에는 보다 다양한 공격 기법을 탐지하고 차단할 수 있는 방법이 연구되고 개발되고 있으나, 개발되는 기법들은 여전히 특정 공격을 탐지하고 차단하는 것을 목표로 개발되고 있다.

문제는 이러한 형태의 대응 기술에 대한 동작 방식이 공개되면 공격자들은 얼마든지 해당 기술을 회피할 수 있는 새로운 공격을 개발할 수 있다는 것이다. 따라서, 기존의 대응기술을 회피할 수 있는 새로운 공격기법은 지속적으로 출현하고 있고, 그에 대한 대응기술 역시 지

본 연구는 지식경제부 및 정보통신연구진흥원의 IT 성장동력기술개발 사업의 일환으로 수행하였음[2009-S-038-01, 분산서비스거부(DDoS) 공격 대응 기술 개발].
본 연구의 네 번째 저자는 지식경제부 및 정보통신연구진흥원의 대학IT연구센터 지원사업의 연구결과로 수행되었음 (IITA-2009-(C1090-0902-0016))
* 한국전자통신연구원 지식정보보안연구부 보안관제기술연구팀 ({yschoi92, showme, jsjang}@etri.re.kr)
** 충남대학교 컴퓨터공학과 (jcryou@home.cnu.ac.kr)

속적으로 개발해야하는 상황이다. 이러한 상황을 극복하고자, 본 논문에서는 DDoS 공격 발생 환경을 전반적으로 분석하여 기존의 공격 대응기법 및 새로운 기술들을 적용하여, 공격발생 이전, 공격 발생 간, 공격발생 이후에 DDoS 공격을 효과적으로 차단하기 위한 DDoS 공격 통합 대응체계를 제시한다.

본 논문은 다음과 같이 구성되어 있다. 먼저 2장에서 DDoS 공격의 발전 형태에 대해 살펴보고, 3장에서는 이러한 DDoS 공격이 어떤 단계를 거쳐 시도되는지에 대해 살펴보고 4장에서 이러한 공격을 효과적으로 방어하기 위해 필요한 DDoS 공격 통한 대응체계를 제시하며, 5장에서 결론과 함께 본 논문을 마치도록 한다.

Ⅱ. DDoS 공격의 발전

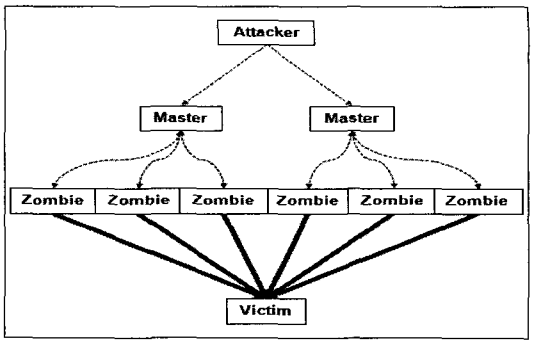
1990년대 중반에 DoS 공격이라는 것이 최초 보고된 이후, 1990년대 말에 들어서면서 다수의 공격 시스템을 이용한 DDoS 공격이 나타나기 시작했다[5]. 본 절에서는 DDoS 공격을 공격 형태와 출현 시기에 초점을 맞춰 총 4개 세대로 세분화하여 정의함으로써 현재까지 DDoS 공격이 어떻게 변화 및 발전되어 왔는지를 기술한다.

2.1 1세대 DDoS 공격

2000년대 초반까지 주로 발견된 1세대 DDoS 공격에는 TFN, TFN2K, Trinoo, Stacheldracht 등의 DDoS 공격 도구들이 주로 사용되었으며, 이 시기에 사용된 공격은 [그림 1]과 같은 구조를 띄고 있었다. 즉, 실제 공격을 수행하는 공격 agent가 공격 시스템에 설치되고, 공격 agent는 공격자에 의해 개발된 독자적 통신 프로토콜을 통해 제어되었다[6].

1세대 DDoS 공격은 가능한 많은 양의 공격 트래픽을 생성하여 공격 대상 시스템으로 전송하는 트래픽 폭주 형태의 공격이 주류를 이루었다. 가장 유명한 것은 2000년에 발생한 아마존, 야후 등의 대형 웹 사이트에 대한 DDoS 공격이었다. 이 공격으로 트래픽 폭주 형태의 DDoS 공격에 대한 대응 기술을 본격적으로 연구하게 되었다.

이 시기에 개발된 공격 탐지기법은 DDoS 공격에 사용되는 네트워크 패킷들의 특징을 이용하거나, 다량의 네트워크 트래픽이 짧은 시간 내에 발생함을 탐지하는 것에 초점이 맞춰져 있었다.



[그림 1] 1세대 DDoS 공격 구조. 공격자는 Master를 통해 Zombie들에게 공격 명령을 하달함.

이 시기의 대응 기법은 공격 트래픽만을 선별하여 차단하는 것이 아니라 특정 대상으로 전송되는 네트워크 트래픽의 양이 급격히 증가하는 경우, 해당 트래픽의 대역폭을 제한(Rate Limit)하는 방법이 주로 사용되었다.

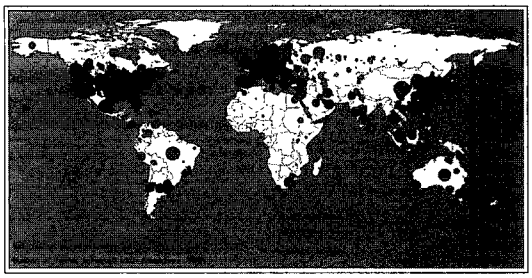
2.2 2세대 DDoS 공격

2세대 DDoS 공격은 주로 2000년대 초/중반에 나타난 공격으로 특정 공격 대상에 대한 DDoS 공격이 아니라, 자동 전파 기능을 가지고 있는 완전 자동화된 인터넷 웜이 스스로를 타 시스템으로 전파시키기 위해 다량의 네트워크 트래픽을 생성함으로써 네트워크의 가용성을 떨어뜨려 발생하는 DDoS 공격을 의미한다.

이러한 DDoS 공격은 인터넷 웜이 타 시스템의 취약점을 찾기 위해 생성하는 트래픽, 해당 취약점을 공격하는 트래픽, 해당 피해 시스템 내로 웜 자체를 전파하기 위해 웜 본체를 전달하는 트래픽 등이 동시에 막대한 양으로 생성되면서 네트워크의 가용성을 떨어뜨려 발생한 경우와, 상기한 일련의 과정에서 특정 시스템의 IP주소를 획득하기 위해 DNS에 전송하는 DNS Query트래픽의 양이 순간적으로 폭증하여 DNS 자체가 마비되어 발생한 경우, 그리고, DNS가 속한 네트워크의 대역폭이 고갈되어 발생한 경우 등이었다.

2세대 공격 형태의 가장 대표적인 예가 1.25 인터넷 대란으로 불려진 2003년 1월 25일에 발생한 Slammer 웜이다. Slammer웜은 Root DNS에 대한 DNS Query를 급격히 증가시켜 국제 관문국으로 통하는 네트워크 트래픽이 처리 가능한 용량을 넘게 만들었고, 이로 인해

인터넷 전체를 마비시켰다([그림 2]참조). 이 시기에는 Slammer웜 Blaster웜, Sasser웜 등이 있었다.



〔그림 2〕 슬래머 웜 발생 10분 후 감염 시스템 분포도. 전체 감염대상의 90%가 10분만에 감염되었음.

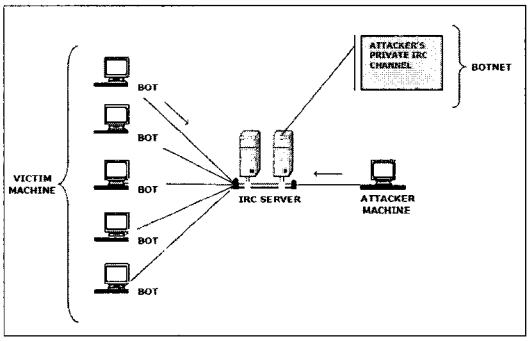
이러한 형태의 공격을 차단하기 위해 이 시기에는 악성프로그램 전파 트래픽뿐만 아니라 악성프로그램 자체를 탐지하고 차단하는 방법에 대한 연구가 진행되었다.

2.3 3세대 DDoS 공격

3세대 DDoS 공격은 봇넷을 이용한 DDoS 공격을 의미한다. 봇넷의 가장 큰 특징은 공격을 수행하는 공격 agent를 제어하기 위해 공격자에 의해 개발된 독자적 프로토콜을 사용한 것이 아니라, 일반 사용자들이 널리 사용하는 정상적인 응용서비스 들을 이용했다는 점이다. 봇넷 관리에 가장 널리 사용된 서비스는 IRC였으며, 이 외에도 P2P, HTTP 등 다양한 프로토콜들이 사용되었다.

2000년대 중반에 들어서면서 악성프로그램의 전파는 특정 취약점을 이용하는 것보다는 일반 사용자들이 널리 사용하는 정상 응용서비스를 이용하여 시도되었다. 예를 들면, 특정 웹사이트에 악성 프로그램을 숨겨 저장하고, 일반사용자들이 접근하면 해당 사용자들의 시스템으로 자동적으로 저장되게 하는 등의 방법을 주로 사용한 것이다. 이 외에도 e메일이나 메신저 등을 이용하여 전파하기도 하였다. 이러한 방법은 기존의 악성프로그램이 전파 단계에서 다량의 트래픽을 발생함으로써, 실제 악성 프로그램의 제작 의도는 이루지도 못한 채 탐지되고 제거되는 것을 막기 위한 것이다.

공격 agent들은 좀비PC에 설치되고 나면, 사전에 정의되어 있는 IRC서버의 특정 채널에 접속하여 명령을 수신하기 위해 대기한다. 또한 공격자는 IRC서버를 통해 공격 agent에 공격 명령을 내리거나 특정 기능을 갱신하기도 했다. 이러한 형태의 공격구조는 [그림 3]과 같았다.



〔그림 3〕 3세대 DDoS 공격 구조. 공격자는 일반 응용 서비스를 이용하여 좀비PC들에게 공격 명령을 하달함[1]

이 시기에는 공격 agent의 모든 성능을 이용하여 다량의 공격 트래픽을 생성하는 트래픽 폭주 형태의 공격이 아니라, 특정 서버의 특정 서비스만을 마비시키기 위한 공격이 주류를 이루었는데, 이런 형태의 공격 트래픽은 급격한 트래픽 양의 변화를 감지하여 공격을 탐지하거나, 네트워크 패킷의 이상 유무 혹은 프로토콜 규약 위반 등을 확인하여 공격을 탐지하는 과거의 DDoS 공격 탐지 기법으로는 탐지하기가 어려운 공격이었다. 왜냐하면, 공격 트래픽의 양이 정상 트래픽 양에 비해 크게 많지 않았을 뿐만 아니라, 네트워크상에 실제로 존재하는 좀비PC를 이용하여 공격 대상 서비스의 프로토콜 규약을 지키며 공격했기 때문에 패킷 단위의 분석으로는 정상트래픽과 구분할 수 없었기 때문이다.

이러한 상황을 극복하고자 이 시기의 공격 대응기술 개발은 공격 트래픽을 탐지하기 위한 기술개발 보다는 공격을 위해 필요한 공격구조를 와해하고자 하는 방향으로 진행되었다.

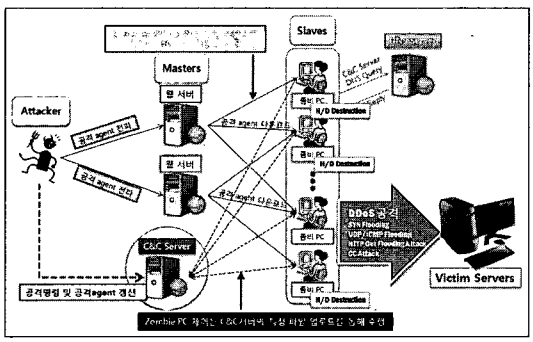
공격 구조를 와해하여 공격을 차단하는 방법은 대부분의 DDoS 공격이 봇넷을 이용함에 근거하여, 봇넷 자체를 탐지하고, 봇넷을 통한 공격명령 전달을 차단하는데 그 목표를 두었다. 실제로 KISA[7]에서 이에 관련된 과제를 수행하고 있다. 공격 명령을 차단하는 가장 간단한 방법은 명령제어(Command & Control, C&C)서버를 탐지하여 해당 서버로의 접속을 차단하는 것이다. 이렇게 되면, 좀비PC에 설치되어 있는 공격 agent는 공격자로부터 공격 명령을 전달받지 못하기 때문에 비록 특정 좀비PC라고 하더라도 결과적으로 공격을 시도하지

않게 되기 때문이다.

2.4 4세대 DDoS 공격

3세대 DDoS 공격이 지속되던 가운데, 2009년 7월 7일 미국 및 한국 내 다수의 중요 웹사이트에 대한 DDoS 공격이 발생하였다. 7.7DDoS 공격은 기존의 공격 방법 및 구조와는 여러 가지 면에서 다른 모습을 보였다. 본 논문에서는 7.7DDoS와 같은 구조의 공격을 4세대 DDoS 공격으로 정의한다.

7.7DDoS는 기존의 공격과는 달리, 비록 C&C서버가 존재하기는 하였으나, 공격 agent가 C&C 서버에 지속적으로 접근을 시도하지 않았고, 공격 대상 웹 서버 목록 및 공격 시간이 공격 agent의 실행코드와 관련 파일에 포함되어 있었기 때문에, 기존에 C&C 서버를 탐지하는 방법으로는 7.7DDoS 공격에 사용된 C&C서버를 탐지할 수 없었다. 이로 인해 C&C서버 탐지를 통해 공격을 차단하는 방법은 사용할 수가 없었다. 이러한 7.7 DDoS 공격 구조는 [그림 4]와 같다.



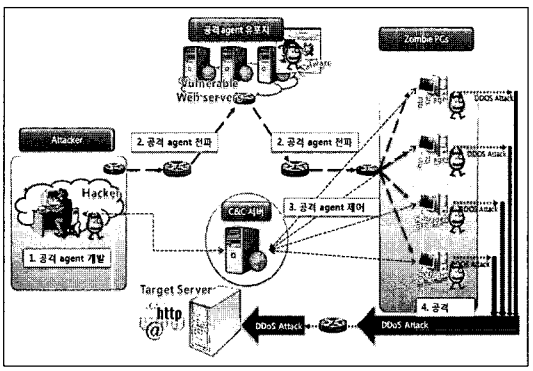
[그림 4] 4세대 DDoS 공격 구조. 7.7DDoS 공격에서는 기존의 C&C서버 운영방법과는 전혀 다른 형태로 C&C서버가 운영되었음

또한 공격 트래픽을 네트워크 패킷 단위로 분석해 보면 이는 정상트래픽과 구분이 불가능한 형태였고, 트래픽 양의 변화를 이용하여 분석하더라도, 특정 시스템에서 발생되는 네트워크 트래픽의 양은 정상 상황에서의 트래픽의 양에 비해 많지 않은 정도였기 때문에, 공격자를 정확히 판단하여 차단하기가 매우 어려웠다. 그리고, 비록 개개의 공격 시스템에서 전송하는 공격 트래픽의 양은 그 양이 많지 않았으나, 20만 여대의 다수의 좀비 PC가 동시에 생성하는 공격 트래픽의 양은 공격 대상 시스템이 속한 네트워크의 전체 대역폭을 모두 고갈시킬 수 있을 만큼 많은 양의 트래픽이었기 때문에, 쉽게 대응할 수 없었다[8]. 추가적으로 7.7DDoS 공격의 경우에는 최종 공격을 마치고 나서는 하드디스크 자체를 파괴하는 자기파괴(Self-destruction) 기능을 가지고 있었다. 이는 공격 agent가 분석되어 공격자를 추적하는데 사용되지 않도록 하기 위한 것으로 예상된다.

이와 같이 4세대 DDoS 공격은 매우 지능화된 공격 방법을 사용하고 있다. 이러한 공격을 효과적으로 탐지하고 차단하기 위해서는 응용계층 서비스에 대한 일반 사용자들의 접근 양식을 분석하여 행위기반의 공격탐지 기술이 개발되어야 한다.

Ⅲ. DDoS 공격 프로세스

현재의 DDoS 공격은 공격을 시도하기 위해 공격 전에 DDoS 공격 환경을 구축해야 한다. 이러한 사전 준비과정을 포함하여 DDoS 공격 프로세스를 [그림 5]와 같이 크게 1) 공격자에 의한 공격 agent개발 단계, 2) 다양한 취약점을 이용한 공격 agent의 전파 단계, 3) 공격 agent 제어 단계, 그리고, 4) 공격 단계로 분류할 수 있다. 본 절에서는 DDoS 공격 프로세스의 각 단계별 특징에 대해 설명한다.



[그림 5] DDoS 공격 프로세스

3.1 공격 agent 개발

최근의 공격 agent는 다양한 기능이 동시에 포함되어 있는 형태로 개발되며, 공격자에 의해 수시로 갱신되어, 공격 명령을 실시간으로 수신할 뿐만 아니라, 보유 기능을 추가하거나 삭제할 수도 있으며, 기존의 악성 프로그

램들이 가지고 있었던 거의 모든 기능을 동시에 가지고 있는 형태로 개발된다. 또한, 보안 전문가에 의해 쉽게 분석되지 않게 하기 위해 다양한 분석 방해(Anti-Reversing) 기법이 적용되게 된다.

3.2 공격 agent 전파

과거에는 공격 agent 전파를 위해 시스템의 취약점을 이용하였으나, 최근에는 일반 사용자들이 널리 사용하고 있는 응용 프로그램을 통해 사용자에 의해 다운로드 되도록 운영되고 있다. 이러한 과정은 정상 상황에서 계속해서 나타나는 현상이기 때문에 최근에는 공격 agent를 전파단계에서 탐지하기가 매우 어려워 졌다. 그러나, DDoS 공격을 사전에 효과적으로 차단하기 위해서는 공격 agent의 전파를 사전에 탐지하여, 일반 PC의 좀비화를 막고, 숙주서버, 즉 공격 agent가 심어져 있는 서버를 조기에 탐지하여 제거 할 수 있어야 한다.

3.3 공격 agent 제어

과거에는 공격 agent 제어를 위해 공격자가 개발한 독자적 통신 프로토콜을 사용하였으나, 최근에는 일반 응용서비스인 IRC, P2P, HTTP 등을 이용하고 있으며, 과거에는 지속적으로 연결을 유지하거나 지속적으로 C&C서버로 접속을 시도하는 형태로 운영되었으나 C&C서버에 지속적으로 접속을 시도하거나 연결 상태를 유지하는 것이 아니라, 최소한의 접속 시도를 통해 명령을 내려 받는 형태를 띠고 있다.

따라서, C&C서버를 탐지하여 DDoS 공격을 차단하기 위해서는 새로운 형태의 C&C접속 방법에 대한 연구를 통해 새로운 C&C서버 탐지 기술을 개발해야 한다.

3.4 공격

최근의 DDoS 공격은 매우 고도화 되어 있다. 즉, 1가지 특정 공격을 시도하는 것이 아니라, 지정된 공격 목표에 대해 다양한 공격을 동시에 시도하며, 공격 트래픽의 양 또한 많지 않기 때문에 특정 시스템에서 발생하는 트래픽이 공격인지를 판단하기가 쉽게 않은 특징을 가지고 있다. 추가적으로 매우 많은 좀비PC를 이용하여 공격을 시도하기 때문에, 특정 공격 목표로 전달되는 전체 공격 트래픽의 양은 매우 커서, 공격 목표가 속해 있는 네트워크 전체가 마비될 수 있을 만큼의 공격이 발생한다.

Ⅳ. 공격 대응 체계

III장에서 설명한 바와 같이, DDoS 공격은 크게 4단계를 통해 시도되는데, 이때 각 단계가 공격자가 의도한 바 대로 진행되지 않게 하면 DDoS 공격은 차단될 수 있다. 즉, 공격자가 공격 agent자체를 개발할 수 없게 하거나, 공격자에 의하여 공격 agent가 전파될 수 없게 하거나, 공격자에 의해 공격 agent가 제어될 수 없게 하거나, 실제 발생하는 공격을 탐지하고 차단하면 되는 것이다.

물론 상기 대응 방식들이 간단하게 해결되지는 않는다. 이를 위해서는 다양한 공격분석/탐지/대응기법들에 대한 연구가 필요하며, 또한 기술적인 측면 외에 법적, 도덕적 대응 방법 역시 강구되어져야 하는 것이다.

그러나, 현재까지는 특정 공격 방법별로 해당 공격을 탐지하고 차단할 수 있는 방법을 찾는데 연구의 초점이 맞춰져 있었다. 예를 들면, TCP SYN Flooding 공격을 어떻게 탐지할 것인가만을 연구하였고, 근본적으로 이러한 공격이 발생하지 않도록 하는 방법에 대한 연구는 미흡하였던 것이다. 근본적인 대책이 강구되지 않으면, 새로운 대응기술을 개발하더라도 짧은 시간 내에 해당 기술을 회피할 수 있는 공격이 다시 출현하게 된다.

이러한 상황을 극복하고자 본 논문에서는 공격 프로세스를 공격발생이전/공격간/공격발생이후의 3단계로 구분하고, 각 단계별 DDoS 대응 요구사항과 정보통신망 환경 전체를 고려한 DDoS 공격 대응 요구사항을 제시함으로써 DDoS공격 통합 대응체계를 제안한다. 본 논문에서 제시하는 개개의 대응 기술들은 최종적으로는 전체가 통합적으로 동작하여, 유기적인 대응을 수행할 수 있어야만 DDoS 공격을 효과적으로 차단할 수 있게 된다([그림 6] 참조).

4.1 공격 발생 이전 단계

공격 발생 이전 단계에서 가장 중요한 것은 DDoS 공격에 필요한 사전 준비과정을 공격발생 이전에 탐지하여 제거함으로써 공격 발생 이전에 대응을 먼저 시작해야 한다는 것이다. 공격 발생 이전 단계에는 III장에서 언급한 프로세스의 단계들 중에서, 공격 agent 개발 단

계, 공격 agent 전파 단계, 공격 agent 제어 단계가 속한다고 할 수 있다. 상기 단계들에 대한 대응은 각 단계별로 독단적으로 이루어지는 것이 아니라, 각 단계에서 생성 가능한 정보들이 통합적으로 수집 분석될 수 있는 대응 체계가 확보되어야 한다.

4.1.1 공격 agent 개발 단계 대응

개개의 공격자가 공격 agent를 개발하지 못하도록 하기는 매우 어렵다. 다만 법적 대응을 강화하는 방법은 가능할 것이다. 즉, 공격 agent를 개발/배포하는 공격자에 대해서는 검거 시 중형의 형량을 부과하도록 법안을 개정하여 공격자들이 공격 agent를 개발하는 것을 주저하도록 만들 수 있어야 한다.

4.1.2 공격 agent 전파 단계 대응

공격 agent 전파 단계에서의 대응 방안으로는 네트워크상에서 송수신되는 실행파일들을 탐지하고 재구성하고, 이를 분석하여 재구성된 실행파일이 공격 agent 인지를 판단함으로써 가능할 수 있다. 공격 agent 전달을 탐지하면 공격 agent의 전파 경로를 추적할 수 있게 되며, 또한 좀비PC가 되었을 것으로 예상되는 시스템 목록과 공격 agent를 전파하는 숙주 서버의 목록을 획득할 수 있게 된다.

여기서 가장 중요한 것은 다양한 프로토콜을 사용하여 전송되는 실행파일을 오류 없이 재구성하는 것과 알려지지 않은, 즉, 시그니처가 존재하지 않는 악성 프로그램을 분석하여, 악성으로 판단하는 기술이다. 이를 위해 동적 악성 프로그램 분석기술 개발이 시급하다.

또한, 이렇게 수집된 악성 프로그램 송수신 정보는 타 관리망간에 서로 공유될 수 있어야 하며, 이를 통해 국가 차원의 효과적인 DDoS 조기 경보 체계를 구축해야 한다.

다른 대응 방안으로는 객체 인증(Object Authentication) 기술을 개발하는 것이다. 즉, 인터넷을 통해 전달하고자 하는 실행파일들을 신뢰할 수 있는 제3기관에 등록하도록 하여, 특정 실행파일이 신뢰할 수 있는 파일인지를 실행파일 다운로드 이전에 일반 사용자가 확인할 수 있도록 함으로써, 정상 사용자가 안전한 실행 파일만을 내려 받을 수 있는 환경을 구성해 주는 것이다.

또한 개별 시스템 내에 사용자의 의도와는 상관없이 설치되는 실행파일을 탐지하여 보고하는 기술을 개발하고, 본 기술을 이용하여 사용자의 의도와 관계없이 설치되는 실행파일을 제거할 수 있도록 하는 기술을 개발하는 것이다.

마지막으로, 허니넷을 활용하여 공격 agent를 수집하는 것이다. 비록 최근에는 사용자에 의해 직접 다운로드되는 형태로 악성 프로그램들이 전파되어 허니넷의 활용도가 예전보다 떨어지긴 했으나, 공격자가 악성프로그램 배포 사이트를 선정하고, 해당 사이트에 악성프로그램을 은닉하는 과정이 웹사이트의 취약점을 이용한 자동화된 방식을 사용할 수 있고, 이런 경우에는 취약한 웹사이트를 허니넷 내에 위치시켜, 악성프로그램이 널리 전파되기 이전에 악성프로그램을 수집할 수 있게 되기 때문이다.

4.1.3 공격 agent 제어 단계 대응

공격 agent들은 일반적으로 C&C서버에 접속하여 명령 수령을 위해 대기한다. 이러한 방식의 C&C서버를 탐지하고, 탐지된 C&C서버로의 접속을 차단하는 기술이 개발되고 있다.

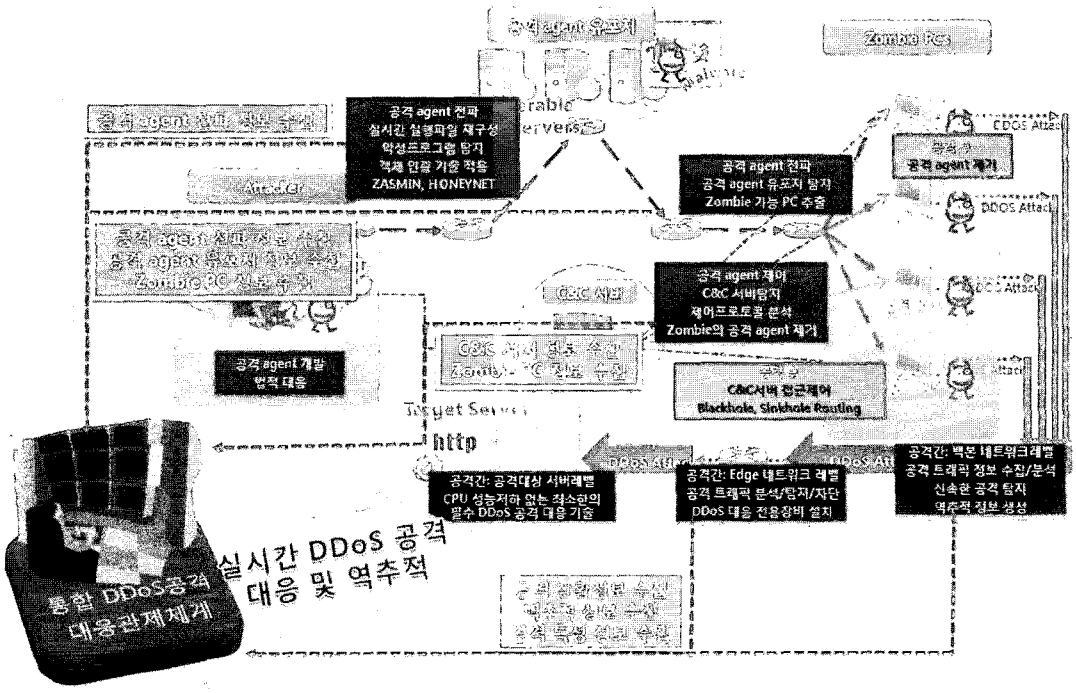
그러나, 7.7DDoS 공격에서 볼 수 있었듯이 공격 agent는 동일한 C&C 서버로 장시간 연결을 유지하지 않고, 서로 다른 C&C 서버에 접속하여 공격 프로그램 및 공격 대상 등을 업데이트할 수도 있다. 따라서, 다양한 형태의 C&C 서버 접근 방식을 분석하고, 이를 탐지할 수 있는 기술을 개발해야 한다.

또한, 공격 agent는 공격 명령을 실시간으로 받지 않고, 사전에 정의된 공격 방법과 목표 그리고 시간을 이용하여 공격을 시도할 수 있다. 따라서, C&C 서버를 탐지하고 차단하는 기술만으로는 DDoS 공격을 효과적으로 차단할 수 없음을 간과해서는 안된다.

추가적으로 공격 agent가 어떤 접속규격에 의해 C&C 서버로 접근하는지를 분석하여 C&C 서버로 접근하는 연결 요청을 특정한 대응 시스템으로 유도하고, 해당 접속규격에 맞춰 공격 agent 자체를 제거하도록 명령을 내릴 수 있는 관련 기술을 개발해야 한다.

4.2 공격 발생 단계

공격 발생 단계는 DDoS 공격 프로세스에서 공격 단계를 의미한다. DDoS 공격이 시작되면 가장 시급한 것



〔그림 6〕 전역 정보통신망 보호를 위한 통합 DDoS공격 대응관제체계. 전체 네트워크가 통합관리될 수 있는 통합 DDoS공격 대응 관제체계가 통합보안제어센터를 중심으로 구축되어야 함.

은 공격 트래픽 자체를 차단하여, 공격 대상 시스템의 서비스가 정상적으로 동작되도록 하는 것이다. 이때 중요한 것은 가능하다면 오직 공격 트래픽만을 차단할 수 있어야 한다는 것이다. 이를 위해서는 네트워크상의 위치에 따라 수행할 수 있는 대응 방법이 서로 다르다. 이에, 본 논문에서는 각 네트워크 레벨별로 대응 방안을 제시한다.

4.2.1 백본 네트워크 레벨 대응

DDoS 공격은 다수의 좀비PC에서 공격 트래픽이 생성되어 공격 대상 시스템으로 전송됨에 따라 발생한다. 이때, 좀비PC는 전 세계에 널리 분포되어 있기 때문에, DDoS 공격 발생 시, 공격 트래픽은 공격 대상 시스템이 속한 국가의 백본 네트워크를 거쳐 전달될 가능성이 매우 높다. 따라서, 백본 네트워크를 모니터링하고 공격의 징후를 탐지할 수 있다면, 공격 대상 시스템이 속해 있는 네트워크에서 대응하는 것에 비해 보다 신속하게 대처할 수 있어, 피해를 최소화할 수 있으며, IP주소가 변형된 네트워크 패킷을 이용한 DDoS 공격의 근원지를 추적하는 데도 보다 효과적일 수 있다. 공격 근원지를 추적할 수 있게 되면 공격 트래픽이 백본 네트워크로 유입되지 않도록 차단할 수 있기 때문에 공격을 효과적으로 차단할 수 있게 된다.

이를 위해서는 수십 Gbps 대역폭의 백본 네트워크상에서 송수신되는 모든 네트워크 트래픽을 수집하여 분석할 수 있는 성능을 갖는 DDoS 장비를 개발하여야 한다.

4.2.2 Edge 네트워크 레벨 대응

Edge 네트워크는 공격 대상 시스템으로 전달되는 모든 공격 트래픽이 통합되는 곳이기 때문에, 트래픽 양의 변화를 가장 신속히 그리고 가장 정확하게 측정할 수 있는 위치이다. 또한 Edge 네트워크는 네트워크상에서 공격 트래픽이 서버에 전달되기 이전에 공격 트래픽을 탐지하고 차단할 수 있는 마지막 위치이기도 하다. 이런 이유 때문에 현재 개발되고 있는 거의 모든 DDoS 공격 대응 시스템이 이 위치에서 설치 운영되고 있다.

그러므로, 공격 트래픽이 공격 대상 서버로 전달되는 것을 막기 위해서는 이 위치에서 DDoS 공격을 탐지하

고 차단할 수 있어야 한다. 다시 말하면, 과거에 발생했던 트래픽 폭주 형태의 공격 및 특정 취약점을 이용한 DDoS 공격뿐만 아니라, 응용 서비스에 대한 DDoS 공격 역시 탐지하고 차단해야 하는 것이다.

그러나, 현재의 DDoS 대응 장비들은 네트워크 패킷의 특징만을 이용하여 탐지 가능한 간단한 공격과 트래픽 폭주 형태의 공격에 대해서는 일정 수준 이상의 대응 성능을 보이지만, 응용 계층에 대한 DDoS 공격에 대해서는 아직까지 만족할만한 성능을 보이고 있지 않다. 이는 과거 트래픽 폭주형태의 공격을 탐지하던 방식을 그대로 응용 계층의 DDoS 공격에 적용하고 있기 때문이다.

트래픽 폭주류의 DDoS 공격은 공격 트래픽의 양이 정상 상황에서의 네트워크 트래픽에 비해 매우 급격히 증가하기 때문에 트래픽양의 변화 정도를 다양한 방법으로 탐지하고, 탐지 결과에 기반하여 공격여부를 판단하는데, 응용 계층 DDoS 공격은 공격 트래픽의 양이 정상 상황에 비해 크게 변하지 않는 수준에서도 공격이 가능하기 때문에 단순히 공격 트래픽의 양만을 이용하여 공격 여부를 판단하는 방법은 응용 계층의 DDoS 공격 탐지에는 비효율적인 것이다.

따라서, 응용 계층에 대한 DDoS 공격은 공격 트래픽의 양으로 탐지하는 것이 아니라, 해당 응용 프로그램의 전형적인 트래픽 특성을 분석하여 분석한 내용에 비해 얼마나 다르게 동작하는 지를 판단할 수 있어야 한다. 그러나, 아직까지 이러한 방식의 응용 계층 DDoS 공격 탐지 기술 연구는 부족한 상황이다.

추가적으로 Edge 네트워크 레벨에서는 해당 네트워크에 속해있는 좀비PC가 확인되면, 해당 좀비PC를 네트워크에서 분리시킬 수 있는 방안이 동시에 강구되어야 한다.

4.2.3 공격 대상 서버 레벨 대응

공격 대상 서버는 네트워크를 구성하는 마지막 단계라고 볼 수 있어, 본 절에 포함한다. 공격 대상 서버는 공격 트래픽을 높은 성능으로 분석하고 차단할 수 없다. 이는 서버의 본래 기능, 즉 특정 서비스를 제공하는데, 서버의 CPU 및 메모리 자원을 우선적으로 사용해야 하기 때문이다. 따라서, 공격 대상 서버에서는 고도의 DDoS 공격 탐지 및 차단 기법을 적용하는 것이 아니라 서버에 특화된 최소한의 공격 차단 기능이 포함되어야 한다.

DDoS의 공격 탐지가 서버단에서 수행되면, 서버의 현재 상황, 즉 CPU 점유율 및 다양한 정보 등을 이용하여 서버가 현재 DDoS 공격을 받고 있다는 것을 판단할 수 있게 된다. 따라서, 정상 상황과 공격 상황에서의 공격 탐지 임계치를 서로 다르게 적용할 수 있으므로, DDoS 공격 상황에 따른 적응적 대응이 가능하도록 할 수 있다.

그러나, 앞서 언급한 바와 같이 서버 자체의 CPU 및 메모리를 사용하게 되면, 공격 발생 시 서버의 성능 저하를 야기 시킬 수 있기 때문에, 서버의 성능 저하는 발생하지 않으면서 공격을 차단할 수 있는 기술을 개발해야 한다. 이는 네트워크 인터페이스 카드 내에 H/W로 구현되어, 자체 CPU를 이용한 공격 탐지 및 차단을 수행해야 한다.

4.2.4 통합 분석 레벨 대응

통합 분석 레벨이란, 공격 발생 시 전역 네트워크상에서 발생하는 다양한 보안 이벤트들을 수집하여 통합 분석하고, 그에 대한 분석 결과를 공격 탐지 및 차단에 활용할 수 있는 대응을 의미한다. 이러한 위치는 관리 영역이 다른 전역 네트워크의 각종 정보들을 모두 수집할 수 있는 위치여야 한다. 즉, 국가차원의 통합관제시스템 등이 이에 해당될 것이다. 현재 국내에는 통합 보안 관제 시스템이 구축되어 있으나, 이는 수동적 보안상황 분석 및 일부 시각화 기술이 적용된 수준이다.

DDoS 공격에 대해 효과적으로 대응하기 위해서는 DDoS 공격 관련 정보들을 수집하고, 이를 자동화된 방법으로 통합 분석하여 신속히 공격을 탐지하고, 그에 대한 대응 방안을 모색하며, 기존에 설치되어 있는 다양한 보안 장비들에게 현재의 공격 상황에 대한 정보를 전달할 수 있어야 한다. 또한, 수집되는 정보들을 이용하여 좀비PC, 공격 agent 유포시스템, C&C서버 그리고 공격자의 위치를 추적할 수 있는 방안에 대해서도 연구되어야 한다. 이를 위해서는 국가차원의 통합관제시스템이 법적 제도적 지원 하에 정부기관에 의해 관리 운영되어야 한다.

4.3 공격 발생 이후 단계

공격 발생 이후에는 공격이 종료되었다고 하더라도, 향후에 제거되지 않은 공격 agent를 통해 반복적으로 공격이 시도될 수 있으므로, 공격에 사용된 시스템들을

추출하여 해당 시스템에서 공격 agent를 제거하고, 취약점이 존재하는 경우, 이를 제거하는 과정을 거쳐야 한다. 또한 수집된 공격 agent를 상세하게 분석하여, C&C 서버 및 공격 agent 유포지를 알아내어, 해당 서버 및 유포지로 접근을 시도하는 네트워크 트래픽에 대해 블랙홀 라우팅(Blackhole Routing) 혹은 싱크홀 라우팅(Sinkhole Routing) 등의 기법을 적용하여, 접근제어 및 공격 agent의 자동 삭제 등이 가능하도록 기술개발을 수행해야 한다.

마지막으로, 시도된 공격의 핵심 특징을 추출하여 향후, 동일한 공격이 발생하는 경우에는 신속히 탐지 및 차단할 수 있는 시그니처를 생성하고 이를 배포하여야 한다.

4.4 기타

상기한 각 단계별 대응 방안은 [그림 6]에서와 같이 전체가 하나의 유기적 대응 체계로서 동작해야만 DDoS 공격을 효과적으로 탐지하고 차단할 수 있다. 그러나, 제시한 대응체계를 구현하기 위해서는 기술적인 문제뿐만 아니라, 법적 제도적 문제가 해결되어야 한다. 제시한 대응체계에서는 다수의 서로 다른 관리망 내의 다양한 데이터들이 통합 DDoS공격 대응관제체계 하에 수집되어 동시에 분석되어져야 하는데, 이를 위해서는 다수의 관리망들이 동일한 인터페이스 또는 프로토콜을 이용하여 정보를 제공할 수 있어야 한다. 이를 위해서는 제공하는 정보의 형태 및 내용 등에 대한 규정과 실제 정보 전달을 위해 필요한 프로토콜의 표준화 등 법적 제도적으로 해당 정보들을 제공하도록 해야만 통합 대응이 가능해 지는 것이다. 따라서, 이를 위해서는 국가 차원의 대응체계 구축이 진행되어야 한다.

현재, 본 논문에서 제시한 대응체계를 구축하여 DDoS 공격을 탐지하고 차단하기 위해 한국전자통신연구원[11]에서는 DDoS 공격 대응 기술개발 과제를 수행하고 있다. 본 과제에서는 네트워크상에 송수신되는 실행파일을 수집/분석하고, 악성 여부를 판단하기 위한 기술과, 다양한 정보들을 수집하고 통합분석하여 DDoS 공격을 효과적으로 차단하는 기술, 응용계층의 DDoS 공격을 탐지하고 차단하기 위한 응용프로그램 네트워크 행위기반 공격 탐지 기술 그리고 서버단에서 DDoS 공격을 방어하기 위한 보안네트워크카드 개발이 진행되고 있다.

V. 결 론

DDoS 공격은 매우 넓은 영역에 걸쳐 퍼져있는 다양한 형태의 공격 시스템으로부터 다양한 공격 트래픽이 특정 사이트로 전송되는 형태의 공격이다. 이러한 공격은 공격을 탐지하는 위치에 따라 공격인지 여부를 판단하는데 사용할 수 있는 가용한 방법이 다르기 때문에 한 곳에서 모든 공격을 효과적으로 차단하기 매우 어려운 공격이다.

과거에도 이와 같은 DDoS 공격 탐지의 어려움을 인지하고는 있었으나, 이를 해결하기 위한 적극적인 방안을 제시하지는 못했다. 왜냐하면, 대부분의 DDoS 공격 대응 기술은 DDoS 공격 대응 장비에 탑재되어 설치 운영되게 되는데, 한 두 장치를 통해 광역 정보를 효과적으로 수집하고 이를 분석하여 차단할 수 없을 뿐만 아니라, DDoS 공격 대응 장비를 개발하고 판매하는 정보보호 업체의 입장에서는 다양한 정보를 획득할 방법 자체가 없었기 때문이다.

그러나, 과거부터 현재까지 발생한 DDoS 공격을 살펴보면 특정 위치에서 모든 공격을 효과적으로 차단한다는 것은 매우 어렵다는 것을 알 수 있다. 또한, 최근에 발생하는 DDoS 공격이 주로 특정 서버의 특정 서비스를 대상으로 하고 있으나, 공격의 대상은 언제든지 전체 네트워크로 바뀔 수 있으며, 이런 경우, 전체 네트워크에 대한 총체적 대응체계가 사전에 구축되어 있지 않다면, 전체 인터넷의 마비뿐만 아니라 정보통신환경의 마비를 유발하게 되어, 천문학적인 피해가 발생하게 될 것이다.

이와 같은 상황을 극복하기 위해서는 전체 네트워크를 지속적으로 감시하여, 신속한 공격의 탐지 및 차단을 수행하는 것뿐만 아니라, DDoS 공격발생 이전부터 공격을 시도하기 위한 행위들을 탐지하여 이를 사전에 차단함으로써, 공격 자체가 불가능하도록 해야 한다. 이를 위해 본 논문에서는 DDoS 공격 통합 대응체계를 제안하였다. 본 논문에서 제시한 DDoS 공격대응체계 관련 연구 내용이 DDoS 공격을 효과적으로 차단하는데 도움이 되길 바란다.

참고문헌

[1] Peng, T., Leckie, C., and Ramamohanarao, K., "Survey of Network-based Defense Mechanisms

Countering the DoS and DDoS Problems", *ACM Comput. Surv.* 39, 1, Article 3, April 2007.

[2] Jelena Mirkovic, Peter Reiher, "A Taxonomy of DDoS Attack and DDoS Defense Mechanisms", *ACM SIGCOMM Computer Communication Review*, Volume 34, Issue 2, pp. 39-53, April 2004.

[3] Arbor Networks. The Peakflow Platform. http://www.arbornetworks.com.

[4] 구자현, "서비스 거부 공격(Denical of Service)의 유형 및 대응", *주간기술동향*, 통권 1377호, 2008. 12.

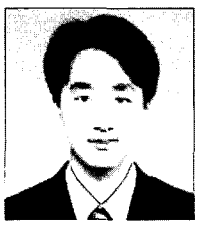
[5] 한국침해사고대응협의회, "All about DDoS 기술세미나", *2008*

[6] 유황빈, 김경탁, 윤창표, "해킹바이러스연구 최종보고서 - 서비스거부공격 위협분석 및 대응체계 연구", *한국정보보호센터*, 2000. 12. http://register.itfind.or.kr/Report/200201/KISA/KISA-0086/KISA-0086.pdf.

[7] 한국인터넷진흥원 ((구)한국정보보호진흥원), KISA, http://www.kisa.or.kr

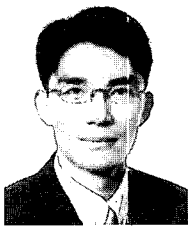
[8] 인터넷침해사고대응지원센터, "국내 주요 사이트 대상 분산서비스거부공격 분석보고서", *한국정보보호진흥원*, 2009. 7.

〈著者紹介〉



최 양 서 (Choi, Yang-Seo)

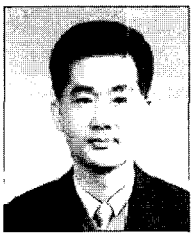
1996년 2월: 강원대학교 전자계산학과 졸업
2000년 8월: 서강대학교 컴퓨터공학과 석사
2000년 6월~현재: 한국전자통신연구원 선임연구원
<관심분야> 정보보호, 네트워크보안, 시스템보안



오 진 태 (Oh, Jin-Tae)

정회원

1990년 2월: 경북대학교 전자공학과 졸업
1992년 2월: 경북대학교 전자공학과 석사
1992년 2월~1998년 2월: 한국전자통신연구원 선임연구원
1998년 2월~1999년 1월: MinMax Tech. 연구원
1999년 2월~2001년 10월: Engedi Networks Inc. Director
2001년 10월~2003년 1월: Winnow Networks Inc. CTO, 부사장, Cofounder
2003년 3월~현재: 한국전자통신연구원 책임연구원
<관심분야> 정보보호, 네트워크보안, 보안 하드웨어



장 종 수 (Jang, Jong-Soo)

정회원

1984년 2월: 경북대학교 전자공학과 졸업
1986년 2월: 경북대학교 전자공학과 석사
2000년 2월: 충북대학교 컴퓨터공학과 박사
1989년 3월~현재: 한국전자통신연구원 책임연구원
<관심분야> 정보보호, 네트워크보안, 시스템보안

류 재 철 (Ryu, Jae-Cheol)

정회원

1988년 5월: Iowa State University 전산학과 석사
1990년 12월: Northwestern University 전산학과 박사
1991년~현재: 충남대학교 정보통신공학부 교수
1997년~현재: 한국정보보호학회 이사
2003년~현재: 인터넷침해대응기술연구센터장
<관심분야> 정보보호, 네트워크보안, 암호학, 보안프로토콜