DDoS 공격 근원지에 대한 국내외 IP 분류체계 연구

윤성열*, 박석천**

*경원대학교 전자계산학과

Study of Classifying System for DDoS Attack Originations from Domestic and Abroad IP

Sung-Yeol Yun, Seok-Cheon Park

Division of Computer Science, Kyungwon University

E-mail : existmaster@naver.com, scpark@kyungwon.ac.kr

요 약

통신망의 발달로 수많은 인터넷 기반 서비스들이 등장함에 따라 다양한 외부공격이 심화되고 있다. 특히, 시스템 또는 네트워크 자원을 공격 대상으로 하는 서비스 거부 공격(DoS : Denial of Service) 및 분산 서비스 거부 공격(DDoS : Distributed DoS)의 문제가 대두되고 있는데, 본 논문에서는 DDoS 공격 근원지 IP주소의 위치 분류의 필요성을 분석하고 공격 근원지 IP주소 위치의 국내·외 여부를 판별하기 위해 국내 IP분배 할당 체계 현황을 분석한다. 또한 DDoS공격을 포함한 여러 가지 해킹에 빠르게 대응할 수 있고 근원지 IP에 관련된 정보를 알아낼 수 있는 시스템을 위한 분류 기법 정립 방안을 제시한다.

1. 서론

통신망의 발달로 수많은 인터넷기반 서비스들이 등장함에 따라 사용자는 다양한 콘텐츠를 이용할 수 있었다. 그러나 이런 인터넷기반 서비스는 유, 무선 환경에서 다양한 외부공격이 심화됨에 따라 사용자들이 정상서비스를 이용하지 못하거나, 악의적인 공격 등에 노출되는 문제점을 가지고 있다.

이 가운데 일반인들에게 잘 알려져 있으면서 빈번한 해킹사고를 일으키는 것 중의 하나로 분산서비스거부공격(DDoS:Distributed Denial-of-service)을 꼽을 수 있다. 서비스거부공격(DoS: Denial of Service)은 정상적인 사용자가 서비스를 이용하지 못하도록 방해하는 공격 기법이다.

그러나 컴퓨터와 인터넷 환경의 급속한 발전으로 소규모의 DoS 공격으로는 서버나 네트워크를 무력화시키기에 부족함이 많았다. 최근에는 DoS 공격을 극대화시키기 위해서 수 천, 수 만대에 이르는 다수의 컴퓨터를 동원하여 공격을 감행하는 DDoS 공격이 인터넷을 위협하는 이슈로 부상했다.

이에 서비스 공급업체 및 보안관련 업체들은 DoS/DDoS를 막기 위해 백신 또는 악성코드 탐지를 서비스하여 대책마련에 나서고 있지만 각 호스트 중심에서의 문제 해결법은 한계점에 이르고 있다. 신종 봇이 등장하면 백신이나 악성코드 탐지 데이터베이스의 업데이트가 필요해지므로 보안업체는 지속적인 봇 탐지 및 예방에 많은 인력을 쏟아야 하는 문제와, 모든 호스트들에게 이런 악성코드 탐지 관련 프로그램을 설치하여 관리해야하는 어려움 때문이다[1].

** 경원대학교 컴퓨터공학과 교수(교신저자)

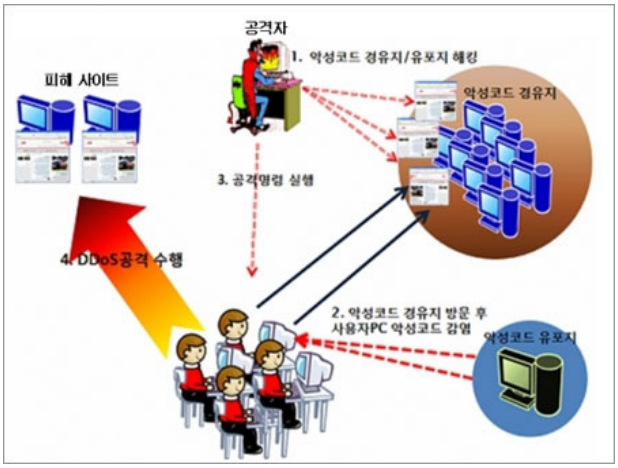
이에 대하여 본 논문에서는 DDoS 공격 근원지 IP주소의 위치 분류의 필요성을 분석하고 공격 근원지 IP주소 위치의 국내·외 여부를 판별하기 위해 국내 IP분배 할당 체계 현황을 분석한다. 또한 DDoS공격을 포함한 여러 가지 해킹에 빠르게 대응할 수 있고 근원지 IP에 관련된 정보를 알아낼 수 있는 공격 IP 근원지 분류 기법 정립 방안을 제시한다.

2. DDoS공격 관련 기반연구

2.1 DDoS 공격 개요

e비즈니스 환경하의 많은 기업들은 다양한 보안 위협에 노출되어 있다. 이 가운데 일반에게 잘 알려져 있으면서 빈번한 해킹사고를 일으키는 것 중의 하나로 정상적인 사용자가 서비스를 이용하지 못하도록 방해하는 공격인 DoS 공격과 이러한 DoS 공격을 극대화시키기 위해서 수 천, 수 만대에 이르는 다수의 컴퓨터를 동원하여 공격을 감행하는 것이 DDoS 공격이 있다. 실제 공격이 처음으로 나타난 것은 1999년 이전 이었으나 큰 주목을 받게 된 것은 2000년 2월 Yahoo, Buy.com, e-bay, Amazon, E-Trade, CNN등 유명 인터넷 사이트가 공격을 받아 몇 시간 동안 접속할 수 없었던 사건이 발생한 다음부터이다[2].

DDoS 공격이 가능한 것은 현재 인터넷 구조는 정보를 주고받는 두 개체(서버와 클라이언트)가 트래픽을 감시하거나 조정하는 것 보다 네트워크에서 정보전달이 원활하고 빠르게 이뤄질 수 있도록 제공하는데 초점을 맞췄기 때문이라고 볼 수 있다. 따라서 정보를 보내는 송신자 측에서 정보를 받는 수신자 측이 처리를 할 수 없을 정도로 과다한 정보를 전달하면, 수신자 측에서 과다한 정보를 처리하지 못하고 둘 사이에 정보 전달이 원활하게 이루어질 수 없으며, 이러한 상황을 악의적인 목적으로 발생시키는 공격이 바로 DDoS 공격이다[1]. <그림 1>은 DDoS 공격의 개요도를 나타내고 있다[3].



<그림 1> DDoS 공격 개요도

2.2 DDoS 공격 대응관련 현황 분석

현재 DNS 서버를 이용하여 악성 봇의 활동을 막는 기법들이 개발 되었으며 대표적으로 한국정보보호진흥원에서 제공하는 DNS싱크홀이 있다. 이 기술은 호스트중심의 악성코드 탐지/차단이 아닌 DNS 서버에서의 악의적인 공격근원지 차단을 이용하기 때문에 앞서 문제시 되었던 이슈들을 어느 정도 해결할 수 있었다. 그러나 이 서비스를 제공하기 위하여 선행되어야 할 과제로 악의적인 공격을 하는 공격근원지의 탐지문제가 부상하고 있다. 인터넷 기반 서비스를 제공하는 업체들도 어떠한 트래픽이 정상트래픽인지, 악의적인 트래픽인지 구분하기 어렵고, 공격자 탐지를 위하여 근원지 추출기법의 연구가 아직 미흡하기 때문에 이에 따른 기술 및 기법이 절실히 요구되는 상황이다.

또한 국내에서 IP의 지역별 관리가 어려움에 따라 공격 근원지의 위치 탐지 및 관리도 매우 어렵다. 따라서 국내 IP를 관리 하는 한국인터넷진흥원과 협조 체제 방안을 마련하거나 할당된 IP를 관리하는 각 ISP사업자간의 협력을 통한 가이드라인을 마련하는 것이 필요하다.

2.3 공격 근원지 IP의 위치 분류기술의 필요성

사이버테러 위협은 인터넷과 네트워크 관련 기술의 발전에 따라 같이 진화되어 왔다. 1980년대에

는 패스워드 추측이나 패스워드 트래킹과 같은 시스템 자체에 대한 해킹이 주로 이루어졌으며 1980년대 후반부터는 급속한 기술발달과 함께 본격적인 네트워크 시대의 도래에 따라 해킹 기법이 세션하이재킹, 스니핑, 스캔, 서비스거부와 같이 네트워크에 대한 해킹이 주로 이루어졌다. 이와 함께 최근 2000년대에 들어서는 웹 해킹이 본격적으로 시작되었으며 시간이 지날수록 해킹에 대한 전문지식이 요구 되지 않는 다양한 해킹 툴들이 개발되었다. 이로 인하여 관련 지식이 많지 않아도 악의적인 마음만 먹으면 누구든지 쉽게 해킹을 할 수 있는 시대가 되었다. 이에 따라 외부에서 시스템에 침입해서 특정 정보를 유출시키거나 시스템을 마비시키는 등 다양한 공격들이 현재 이루어지고 있으며 보안업체들은 이러한 광범위한 공격들에 대응하기 위해 촉각을 곤두세우고 있다.

특히 분산된 호스트에 봇을 설치하여 공격을 시도하는 DDoS 공격의 경우, 최초 공격 근원지의 IP를 알아내기도 어렵지만 설령 해킹에 쓰이는 근원지 IP를 역추적 하여 알아냈다고 해도 빠른 시간 안에 공격자의 물리적 위치를 파악하기가 쉽지 않은 상황이다. 해당 정보를 얻기 위해서는 수사기관에 협조를 요청하고 ISP업체에 의뢰를 하는 등의 많은 절차가 있기 때문에 절차에 따른 시간적 제약이 존재한다. 우리나라에 할당된 IP주소를 재 할당 하는 기관인 한국인터넷진흥원에서는 IP할당에 관련된 업무를 처리함에도 불구하고 IP주소에 따른 IP주소 사용자의 물리적 위치에 대한 데이터는 가지고 있지 않다[4]. 따라서 IP주소를 이용해 IP 소유자의 물리적인 위치정보에 누구나 손쉽게 접근할 수 있다면 문제가 되지만 사이버테러 방지차원에서의 물리적 위치 추적은 필요하다고 할 수 있다.

3. 국내 IP의 기초 자치단체 수준의 지역 분류 방안 제시

IP주소를 이용해 지역 정보를 추적하는 것은 단순히 특정 툴이나 서비스를 이용한다고 해서 가능한 것이 아니다. 인터넷과 IP주소의 할당체계에 대한 이해와 그로 인해 얻어낸 정보의 해석 및 확장 능력이 필요하지만, 이를 모두 동원하더라도 반드시 정보를 얻을 수 있는 것도 아니다.

DDoS 공격뿐만 아니라 여러 가지 해킹 범죄에 대해서 해킹의 근원지가 국내라면 해킹을 시도한 IP에 대한 정보를 얻는 것이 해킹 범죄 수사에 첫 번째 일이 된다. 근원지 IP의 물리적인 위치를 추적하고자 할 때 현재의 시스템으로는 정부기관에 공문을 요청하고 IP를 개인에게 분배한 ISP 업체에 협조를 요청하는 등의 까다로운 절차가 필요하다. IP주소 사용자의 개인정보 보호 차원에서 이 같은 정보를 쉽게 얻을 수 없게 만드는 것은 당연한 일이지만 해킹 범죄에 대한 수사 지원 측면에서 IP주소에 대한 기본적인 지역분류정보 등을 제공하는 것은 필요하다. 본 논문에서 IP주소에 따른 지역분류 방안 제시를 위한 항목은 다음과 같다.

3.1 기존 IP의 지역 분류 체계 현황분석

국내의 경우 최종 사용자에게 IP주소를 분배하는 일은 ISP업체별로 IP할당을 해주는데 공식적인 지역 분류 체계나 자료는 없는 현실이다.

IP주소는 할당방법에 따라 '고정IP'와 '유동IP'로 나뉜다. IP주소는 특정 기관 및 사업자에게 할당되어 사용되며 이것은 고정IP와 유동IP 모두 마찬가지이다. 기술적인 의미로 볼 때 고정IP와 유동IP의 차이는 DHCP서버(동적 주소 할당 서버)의 사용여부에 따라 나뉘게 된다. 일반적인 경우 기업/PC방/관공서/학교 등에서는 할당받은 IP주소를 정적으로 할당하여 사용하고(DHCP서버를 사용하지 않고) 가정용 인터넷을 서비스하는 ISP(인터넷 서비스 업체: KT, SK브로드밴드 등)에서는 IP주소를 유동적으로 배분한다(DHCP 서버 사용). 유동IP는 HELPER - IP(DHCP)를 경유함으로 대부분의 상위 웹 접속에서는 찾기 힘들다.

따라서 흔히 사용되는 고정IP와 유동IP의 의미는 가정용 회선이냐 아니냐를 뜻하며 모든 IP주소의 할당정보는 공개되어 있다. 할당정보는 Whois 서비스로 조회가 가능하다. 하지만 공개된 정보는 IP주소를 할당받은 기관 및 사업자까지이며 해당 기관이 IP주소를 재 할당 하는 경우에는 기관의 정보공개 방침에 따르게 된다. 국내 대부분의 인터

넷 서비스 업체에서는 고정IP 등록자(기업/PC방/관공서/학교)의 정보만을 공개하고 있으며 따라서 고정IP 등록자의 정보는 손쉽게 얻을 수 있다.

반면, 유동IP는 그 사용자가 수시로 바뀔 수 있고, 또 개인정보 및 사생활보호의 차원에서 공개하지 않고 있다. 하지만 유동IP의 시간대별 할당기록을 보유하고 있기 때문에 정확한 할당시간을 알고 있다면 가입자의 정보를 확인할 수 있다. 그러나 현재 유동IP의 할당기록은 사법기관의 요청에 의해서만 공개가 가능하여, 유동IP의 등록정보는 쉽게 확보하기기 어려운 것이 현실이다.

3.2 국내에 적용 가능한 IP 지역 분류 방안

IP주소들은 인터넷 서비스업체인 ISP가 할당을 받아서 사용을 하는데 업체가 일련번호중의 어느 부분만을 가진 것이 아니라 서로 섞여 있어서 일괄적인 보유IP를 파악하기가 쉽지 않다. 또한, 각 ISP들은 고정IP주소를 고객에게 제공하는 경우도 있고(기업체, PC방 등) 일정 IP주소는 유동IP용으로 보유하고만 있다가 고객의 요청 시에(ADSL, VDSL 사용자의 접속)만 IP주소를 분배해서 사용하는 경우도 있기 때문에 IP만으로 지역을 뚜렷하게 구분하기는 힘든 실정이다.

이러한 IP주소의 사용은 그 IP주소의 소유권자인 ISP들의 권한이므로 각 ISP회사마다 그 회사 고유의 내부적인 사용규칙에 따라 운용되며, 회사마다 각각 다 다른 방침을 갖고 있을 것이다. 또한, 한 ISP에서 사용하고 있는 지역적 IP주소 할당 규칙은 어떻게 보면 회사의 내부 비밀에 해당될 수 있으므로 이것을 아는 것은 거의 불가능 하다고 볼 수 있다. 그렇기 때문에 이에 대한 책임을 ISP 사업자에게 두어 ISP업자가 분배한 IP주소에 대한 간략한 지역정보를 ISP 업자 스스로 국가가 관리하는 DB에 업데이트 하도록 하고 이를 성실히 시행할 경우에는 세제감면 등의 혜택을 두어 ISP 사업자가 이를 따르게 만드는 방안이 있다.

또한 ISP 사업자들 간의 소유하고 있는 데이터베이스를 통합시키는 등의 정책적, 제도적인 개선 방안이 필요하다. 그러나 기존 ISP 사업자들 간의 이해관계를 고려하고 고객정보 보호 등의 이슈들을 해결하기 위하여 즉각적인 데이터베이스 통합은 기대하기 어렵다. 따라서 점진적인 데이터베이스 통합과 제도적 보안을 마련해야 할 것이다. 그리고 국가와 ISP 사업자들 간의 유동IP 등록정보 열람에 있어 필요한 제약사항들을 마련함으로써 제도화된 정책적 방안을 마련해야 할 것이다.

이 같은 정보 열람은 물론 개인이 접근해선 안되며 IP주소의 지역 정보에 접근할 수 있는 기관을 한정지어(예: DDoS 대응기관) 해당되는 기관만 접근 할 수 있도록 해야 하며, 해당 정보가 유출되었을 때에는 문제가 발생할 수 있기 때문에 이에 대한 철저한 보안이 이루어져야 한다는 전제가 필요하다.

4. 결론

결론적으로 현재 일정 규칙에 의해 IP주소로 지역을 파악한다는 것은 불가능하며 이를 가능하게 하기 위해서는 ISP사업자들의 적극적인 협력이 필요하다. 실제적으로 이것을 DDoS 대응기관이 파악하여 열람할 수 있게 하려면 각 ISP 사업자에게 의뢰를 하고, 정보를 받고, DB에 등록하고, DB를 관리하는 등 여러 가지 절차에 따라 복잡하고 어려운 측면이 있다. 따라서 국가와 ISP 사업자들 간의 필요한 제약사항들을 마련하고, ISP 사업자들 간의 데이터베이스를 통합시킴으로써 제도적 보안을 마련해야 하겠다.

본 논문에서는 DDoS 공격 근원지 IP에 관련된 정보를 알아낼 수 있는 시스템을 위한 분류 기법 정립 방안을 제시하였다. 향후에는 DDoS공격을 포함한 여러 가지 해킹에 빠르게 대응할 수 있는 체계적인 방안이 마련되어야 할 것이다.

[참고문헌]

[1] 이희조, “DDoS를 통한 네트워크 마비 협박과 공격 대응”, 경영과컴퓨터, 2008.6

[2] 김현준, “분산서비스거부공격(DDoS)의 이해와 대응 방안 제시”, DBguide.net, 2003.4

[3] “http://www.kisa.or.kr”

[4] “https://ip.nic.or.kr/main.html”