분산 서비스 거부 공격 발원지 자동 추적 모델 연구

이만희° 정상길 권윤주 김국한 변옥환
한국과학기술정보연구원
{mhlee°, lovej, yulli, ghkim, ohbyeon}@kisti.re.kr

Study on Automatic Source Tracking of Distributed Denial of Service Attack

Manhee Lee° Sangkil Jung, Youngjoo Kwon, Kookhan Kim, Okhwan Byeon
Korea Institute of Science and Technology Information

요 약

최근 인터넷을 통하여 급속히 확산되고 있는 분산 서비스 거부 공격은 전 세계 웹 사이트들에 큰 피해를 입히면서 세계적인 문제로 부상되었다. 현재 이에 대한 대책으로 방화벽이나 침입 탐지 시스템을 이용하지만, 전 세계에서 동시 다발적으로 일어나는 이 공격을 근본적으로 방지하는 데는 적합지 않다. 이에 본 논문에서는 공격 트래픽의 송신자 주소를 임의의 IP 주소를 사용하여 공격의 발원지를 추적할 수 없는 기존 문제점을 해결할 수 있는 분산 서비스 거부 공격 발원지 자동 추적 모델을 제시하고자 한다.

1. 서 론

최근 인터넷을 통하여 해킹이나 바이러스가 확산되면서 그 피해가 커지고 있다. 특히 분산 서비스 거부(Distributed Denial of Service, DoS) 공격은 2002년 2월 Yahoo, Amazon, CNN에 발생하여 각 웹 사이트들에 큰 피해를 입히면서 세계적인 문제로 부상되었으며, 국내에서는 2003년 1월 25일에는 MS-SQL 웜으로 발생된 DDoS 공격으로 인해 국가 핵심 인터넷이 마비가 되는 심각한 피해를 초래하였다. 이러한 DDoS 공격은 날로 다양해지고 자주 발견되고 있으며 인터넷 정체의 주 요인이 되고 있다.

DDoS를 방지하는 현재의 방법은 주로 방화벽이나 침입 탐지 시스템(Intrusion Detection System, IDS)을 이용한다. 2003년 1월 23일에도 나타났듯이 몇몇 국내·외 방화벽 또는 IDS는 성공적으로 MS-SQL 웜을 방지하는 효과를 보이기도 했다. 하지만 DDoS는 전 세계에서 동시에 발생하며 특정 지역의 시스템으로 트래픽이 집중되기 때문에 IDS로는 DDoS의 발생을 막을 수 없다. 또한 개별 기관으로 유입되는 DDoS 공격을 방화벽 또는 IDS가 방지한다 하더라도 개별 기관이 접속되어 있는 네트워크 자체가 트래픽 폭주로 인터넷을 사용할 수 없는 상태가 되므로 일단 DDoS 공격이 일어나면 방화벽 또는 IDS는 큰 효용성이 없게 된다.

이에 본 논문에서는 개별 기관 차원의 DDoS 방재 대책이 아닌 인터넷 서비스 제공자(ISP) 차원에서 DDoS 트래픽 억제에 사용될 수 있는 DDoS 공격 발원지 자동 추적 모델을 제시하고자 한다. DDoS 공격 방재의 어려움은 공격 트래픽의 송신자 주소를 임의의 IP 주소를 사용(일명, IP Spoofing)함으로써 공격의 발원지를 추적할 수 없다는 데 있다. 본 논문에서 제시하는 DDoS 공격 발원지 추적 모델은 DDoS 공격이 탐지된 특정 라우터에서 해당 DDoS 공격이 유입된 라우터를 추출하고, 다시 해당 DDoS 공격이 유입된 라우터로 접근하여 DDoS 공격 유무를 검사하는 재귀적 방식을 이용하여 최종적으로 DDoS 공격의 발원지 또는 발원지와 연결된 라우터를 찾아냄으로써 IP Spoofing이 된 DDoS 공격의 발원지를 추적할 수 있다. 본 모델은 중소규모 ISP 또는 개별 기관별로도 적용할 수 있으므로 향후 효용성이 높을 것으로 사료된다.

본 논문은 다음과 같이 구성되어 있다. 2장에서는 DoS, DDoS의 소개와 플로우 기반 DoS 공격 탐지 연구에 대해서 기술하고, 3장에서는 서비스 거부 공격 발원지 추적 알고리즘을 기술하고, 마지막으로 결론과 향후 계획에 대하여 기술할 것이다.

2. 관련 연구

2.1 DDoS(Distributed Denial of Service)

DDoS 공격은 인터넷에 연결된 일단의 시스템들을 이용해 단일 사이트에 대한 플러딩 공격을 시도하는 것이다[1][4]. DDoS 공격은 그림 1과 같은 구조로 하나의 시스템을 공격한다.

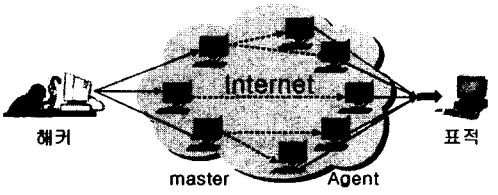

그림 1 DDoS 공격의 구조

그림 1에서 보는 바와 같이 DDoS 공격은 Attacker, Master, Agent로 구성된다. 여기서 Agent들은 DDoS 공격을 위한 침해호스트로서, Master에서 전송된 공격 메시지를 받아 특정 시간에 표적 시스템으로 폭주 트래픽을 발생시킨다. Master는 침해된 호스트들인 Agent를 관리하면서 Attacker로부터의 명령이 오면 자신이 관리하고 있는 Agent들에 공격 메시지를 전달하여 모든 Agent들이 하나의 표적 시스템을 공격하도록 한다[5]. 이러한 DDoS를 방어하는 데 있어서 문제점은 다음과 같다.

· DDoS 공격에는 필터링하거나 탐지할 수 있는 일반적인 특성이 없다. 결국 DDoS 공격으로 전송되는 네트

워크 트래픽은 서비스의 합법적인 사용을 위한 트래픽과 구분되지 않는다.

- DDoS 공격 발원지간의 협동은 DDoS 공격을 trace back 하기 어렵게 한다. 따라서 분산된 근원지에 대처할 수 있도록 관리 도메인간 협력이 필요한 반면 관리 도메인 간의 협력이 부족하다.
- Attacker는 attacking machine의 신분를 숨기기 위해 IP Spoofing을 사용하기 때문에 공격하는 시스템의 신분을 알아내기 어렵다[1][2][3][5].

2.2 플로우 기반 서비스 거부 공격 탐지(Flow-based DDoS Detection System, FDDS) 연구

전술한 바와 같이 DDoS 탐지는 방화벽이나 IDS 시스템도 수행 중이다. 하지만 많은 라우터를 관리하고 있는 ISP 입장에서는 모든 라우터와 링크에 대해서 IDS와 같은 탐지 시스템을 설치할 수 없다. FDDS는 라우터로부터 플로우 정보를 수신받아 DDoS를 탐지할 수 있는 시스템이다. 본절에서는 분산 서비스 공격 발원지 추적 모델이 기반으로 하는 권윤주가 [5]에서 제안한 FDDS의 원리와 작동 모델을 기술한다.

일반적으로 네트워크 트래픽은 Service 요청/응답으로 이루어지기 때문에 inbound 트래픽과 outbound 트래픽의 비율은 비슷하다. 그러나 플러드형 공격이 시작되면 그러한 트래픽간 균형이 깨져서 어느 한 쪽으로 트래픽이 몰리는 경향을 볼 수가 있다.

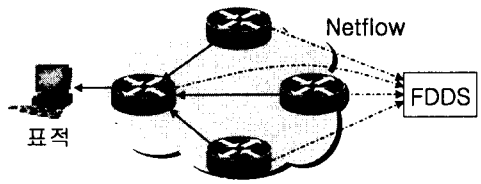

그림 2. FDDS의 구성

FDDS는 각 네트워크 트래픽을 조율하는 라우터로부터 하나의 네트워크로 유입 또는 유출되는 트래픽의 정보를 받는다. 이때 라우터로부터 전송되어지는 트래픽 정보가 'Netflow'이다[6]. Netflow의 세부 요소로는 근원지 주소, 목적지 주소, 프로토콜 번호, 서비스 포트 번호, 라우터 주소, 플로우당 packet량, 플로우당 byte량 등이 있다. FDDS는 각 플로우에 대한 inbound와 outbound 트래픽을 계산한다. 이 트래픽 분석을 바탕으로 기존의 평균값과 표준편차를 구하여 신뢰구간 95%로 트래픽의 normal과 abnormal 트래픽을 구분한다. 만약 현 트래픽이 abnormal 트래픽으로 판정되면, DDoS 공격여부를 재차 검사하기 위해서 해당 분류단위별로 근원지 주소/목적지 주소의 top10을 구한다. 플로우 개수를 기준으로 정렬된 목적지 주소별 1위가 전체 트래픽의 90%이상이 되면 DDoS 공격으로 간주한다.

FDDS는 현 트래픽에 대해서 DDoS 공격 판정이 나오면 FDDS 내부 state는 Normal에서 Abnormal로 변경되며 플로우 개수를 기준으로 정렬한 목적지 주소를 이용하여 라우터에 적용할 AccessList를 작성하고 해당 라우터 직접 적용한다. 이후 라우터가 정상적인 트래픽을 발생시키면 일단 Transient State로 이동 후, 재차 DDoS 공격 검사를 하고 다시 정상적인 트래픽으로 간주되면 Normal State로 천이된다.

3. 서비스 거부 공격 발원지 자동 추적 알고리즘

DDoS를 방재하기 위해서는 2.1절에서 기술한 DDoS 방어 문제점을 해결하여야 효과적으로 DDoS를 방어할 수 있다. 첫 번째로, DDoS 공격에는 필터링하거나 탐지할 수 있는 일반적인 특성이 없는 문제점은 2.2절에서 설명한 FDDS를 이용한다. FDDS는 트래픽의 특성과 관계없이 트래픽의 유·출입의 양의 변화로 DDoS를 판별할 수 있기 때문에 효과적으로 DDoS를 판별할 수 있다.

두 번째로, DDoS의 발원지는 대부분 다양한 도메인에 위치하기 때문에 일괄적인 정책을 가지고 DDoS를 방지하기 어렵다. 따라서 본 논문에서는 단일 도메인, 즉 하나의 ISP에서 관리하고 있는 전체 네트워크를 대상으로 한다. 한 ISP의 관리자는 전체 네트워크를 구성하는 모든 라우터의 접근 권한을 가지고 동일한 정책을 적용할 수 있다. 따라서 DDoS 방지 대책을 한 ISP에 속한 전체 네트워크에 적용하는 것이 매우 용이하다. 이는 다른 도메인에 위치한 DDoS 발원지를 직접 추적할 수 없는 한계가 존재하지만, 본 논문에서 제시하는 방안을 많은 도메인에서 동시에 적용할 경우, 근본적인 DDoS 발원지 추적이 가능할 것이다.

세 번째로, DDoS 공격의 Machine의 신분을 숨기기 위해 IP Spoofing을 사용하는 것이다. IP Spoofing된 트래픽은 피해 시스템에서 발견하더라도 발원지에 대한 어떠한 정보도 알 수 없다. 이를 해결하는 방법은 DDoS와 연관된 모든 라우터에서 해당 DDoS 공격이 어떤 라우터로부터 들어와서 어떤 라우터로 나갔다는 플로우 정보를 추출할 수 있는 기능을 이용한다. 이 기능을 이용하면 DDoS 공격이 들어온 라우터를 알 수 있고 이 라우터에 대해서 재귀적으로 같은 검사를 실시하면 최종적으로 DDoS 발원지 라우터를 찾을 수 있고, 발원지가 현재 도메인에 존재하지 않는다면 발원지와 가장 가까운 말단 라우터를 찾을 수 있다.

DDoS 공격에 관련된 라우터로부터 해당 공격이 흘러들어온 라우터를 추출하는 방법은 라우터에 트래픽의 플로우 정보를 축적하도록 Enable 함으로써 가능하다. 라우터에서 sh ip cache flow 명령을 수행하면 축적된 플로우 정보를 추출할 수 있다(표 1). 아래 표에서 출발지 IP 주소 213.230.8.57, 목적지 IP 주소 153.155.235.43인 트래픽이 Fa0/1/0로 유입되어 AT4/0/0.1을 통하여 흘러간다는 것을 알 수 있다.

표 1 라우터 플로우 정보 추출 예

SrcIf	SrcIPaddress	DstIf	DstIPaddress
Fa0/1/0	213.230.8.57	AT4/0/0.1	153.155.235.43
AT4/0/0.1	213.230.8.249	NULL	224.0.0.22

만약 이 트래픽이 DDoS 공격 트래픽이고 213.230.8.57이 IP Spoofing 되어서 무의미한 IP 주소라고 할지라도, 해당 트래픽이 Fa0/1/0으로 들어왔기 때문에 라우터

정보에서 Fa0/1/0의 연결 정보를 알 수 있다. Fa0/1/0이 특정 시스템 또는 LAN에 연결되어 있다면 이 DDoS 공격을 발생시키는 시스템을 금방 찾을 수 있고, 만약 Fa0/1/00이 다른 라우터와 연결되어 있다면 그 라우터에서 같은 절차로 플로우 정보를 이용하여 DDoS 트래픽이 유입되는 인터페이스를 찾을 수 있기 때문에 최종적으로는 DDoS 공격을 발생시키는 시스템을 찾을 수 있다.

따라서 DDoS를 방어하기 어려운 세가지 문제점은 위의 방법을 이용하여 해결될 수 있으며, 이를 자동으로 추적하는 모델은 그래프 탐색 방법을 이용해 해결할 수 있다. 한 ISP가 관리하고 있는 모든 라우터들은 주변 라우터들과 서로 연결되어 있으므로, 네트워크 T는 그래프 G(V,E)(V는 라우터, E는 라우터간 링크)로 표현할 수 있다. T에서 DDoS 공격이 발생하면, 발원지 라우터 v_s로부터 목적지 라우터 v_d 까지 트래픽이 발생하며, 이 때 DDoS 트래픽이 흐르는 라우터의 집합 V'이 생성된다.

$V'=\{v_s, v_0, .., v_k, v_d\}$ $(v_i \in V, 0 \le i \le k)$

새로운 집합 V'는 DDoS 공격에 참여하게 된 라우터의 집합으로써, DDoS 트래픽이 흐르는 E에 방향성 특성이 첨가된 새로운 네트워크인 그래프 T'를 정의할 수 있다.

$T' = G(V',E')$ $(E'=\{(v_i, v_j)\}, (v_i, v_j \in V'))$

T'의 특성은 DDoS 공격 특성과 라우팅 특성을 따르는데, 첫째 라우팅 된 트래픽은 순환되지 않는 라우팅 특성상 T'에는 순환이 생성되지 않는다. 둘째, 목적지는 하나이므로 라우팅 정책이 변하지 않는 동안은, 다음 라우터는 변하지 않는다. 세째, 여러 라우터에서 시발된 DDoS 공격 트래픽이 하나의 라우터에서 모이면, 이후 이 트래픽은 같은 라우팅 정책에 의해 같은 경로를 따른다. 이 세 특성을 종합하면, T'는 T'에 포함된 모든 V'가 |V'|-1개의 E'로 연결되는 신장 트리가 된다. 따라서 DDoS 공격 발원지 자동 추적은 T의 특정 라우터 v에서 신장 트리 T'에 대한 검색을 통해 v_s를 찾는 문제로 변형될 수 있다(그림 3).

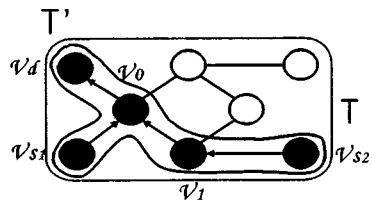

그림 3 DDoS 공격 참여 라우터 신장 트리

DDoS_check(v,$\mathcal{A}$)는 라우터 v에 DDoS 공격 $\mathcal{A}$ 트래픽을 유입시키는 인접 라우터 집합을 리턴한다. 공격 $\mathcal{A}$를 유입시키는 인접 라우터가 없다면, 공격 $\mathcal{A}$ 발원 시스템이 현재 라우터 v에 직접 연결된 것을 의미한다. 공격 $\mathcal{A}$를 유입시키는 인접 라우터가 있다면, 각 인접 라우터에 대해서 같은 방법으로 공격 $\mathcal{A}$를 검색하면 최종적으로 공격 $\mathcal{A}$ 발원 시스템을 모두 검색할 수 있다. 상기 알고리즘 DAT(DDoS_Automatic_Tracking)를 의사코드로 나타내면 다음과 같다.

```
DAT(v,A)
    vA=DDoS_check(v,A)
    if vA={} then
        print v and return
    else for each router v'∈vA
        DAT(v',A)
    return
```

그림 4 DDoS 공격 발원지 자동 추적 의사 알고리즘

위 알고리즘을 그림 3의 T'에 적용하면, 즉 DAT(v_d,$\mathcal{A}$)를 수행하면 v_d->v_0->v_{s1}->v_1->v_{s2}의 순서로 탐색되고 그 결과 값으로 v_{s1},v_{s2}이 출력되므로 위 DAT 알고리즘이 효과적으로 발원지 라우터를 찾아낼 수 있음이 입증된다.

4. 결론

본 논문에서는 인터넷에서 최근 극심한 피해를 입히고 있는 DDoS 공격을 방지할 수 있는 요소 기술인 DDoS 공격 발원지 추적 알고리즘을 설명하였다. DDoS 공격의 탐지는 플로우 기반 DDoS 탐지 시스템인 FDDS를 이용하였다. 그리고 한 ISP가 운영하는 전체 네트워크를 그래프로 보고, DDoS 공격이 일어나고 있는 라우터를 그래프로 나타내면 그래프의 신장 트리와 같음을 보였다. 마지막으로 이 신장 트리에서 DDoS 공격 발원지를 자동으로 추적할 수 있는 알고리즘을 제안하였다.

본 논문에서 제시한 자동 추적 알고리즘은 많은 가정을 기반으로 하고 있으며, 이를 실제로 구현하기 위해서는 많은 변수를 감안해야 한다. 예를 들면, 라우터가 발원지 시스템이 직접 연결되어 있고, 동시에 인접 라우터에서 DDoS 공격 트래픽이 흐르는 경우, 발원지 시스템이 타 도메인에 위치하여 더 이상 검색을 못하는 경우, 본 알고리즘의 분산형 또는 중앙 집중형 구현 여부 등이 있으며 현재 연구 또는 구현 중이다.

참고 문헌

[1]Felix Lau, et al., "Distributed Denial of Service Attacks," *Systems, Man, and Cybernetics, 2000 IEEE International Conference* on, Vol. 3, pp 2275-2280, 2000

[2]Jelena Mirkovic, "D-WARD : DDoS Network Attack Recognition and Defense," PhD Proposal, 2002

[3]Jelena Mirkovic, "Source Router Approach to DDoS Defence," *Usenix Security Symposium 2001*, 2001

[4]Dan Sterne, et al., "Active Network Based DDoS Defense," *DANCE02(DARPA Active Network Conference and Exposition)*, pp. 193-203, 2002

[5]권윤주, "DDoS 공격 탐지와 대응에 관한 연구 : FDDS(Flow-based DDoS Detection System)", *2002 정보보호학회 추계학술대회*, 2002

[6]"Netflow services and applications," http://www.cisco.com/warp/public/cc/pd/iosw/ioft/neflct/tech/napps_wp.htm, 2000, Cisco white paper