IP 망에서 실시간 유해 트래픽 공격 탐지 및 대응 방법

김은주, 이순석, 김영부
한국전자통신연구원 미래네트워크연구부

A method for Real-time Detecting and Responsing Harmful Traffic in IP Network

Eun Joo Kim, Soon Seok Lee, Young Boo Kim
Future Network Research Department, ETRI
E-mail : ejkim@etri.re.kr, sslee@etri.re.kr, ybkim@etri.re.kr

요 약

인터넷의 빠른 발전과 확산에 따라, 통신은 방송, 통신, 인터넷 등 개별 미디어 융합을 기반으로 IP 기반 융합네트워크로 발전해 나가고 있다. 네트워크의 발전과 함께 보안문제는 네트워크 관리에 있어서 매우 중요시 되고 있는데, 특히 트래픽 폭주를 일으키는 분산공격트래픽 공격에 대한 방어는 필수적이라 할 수 있으며, 분산공격트래픽 공격에서는 알려진 패턴에 대한 유해트래픽의 방어뿐만 아니라 알려지지 않은 새로운 패턴의 유해트래픽에 대한 보안관리가 모두 필요하다. 현재 인터넷에 대한 공격을 차단할 수 있는 방어 기술은 싱크홀(sinkhole) 터널링(tunneling) 기술 등이 제공되고 있으나, 싱크홀 라우터를 따로 만들지 않고 알려지지 않은 패턴의 유해트래픽에 대한 실시간 탐지 및 대응 방법은 정의되고 있지 않다.

본 논문에서는 분산공격트래픽, 바이러스 등을 모두 포함하는 유해트래픽의 실시간 탐지 및 대응 방법에 대하여 제안한다.

1. 서론

인터넷 서비스의 수요가 급증함에 따라 정보통신서비스 제공기업에서도 사용자에게 보장된 네트워크 품질 제공을 할 수 있도록 많은 노력을 하고 있는데, 현재의 보안 시스템으로는 DDoS 공격 시 이에 빠르게 대처하여 사용자에게 보장된 네트워크 서비스를 제공하기에는 많은 문제점을 가지고 있다. 특히 분산화·대규모화 되어가고 있는 네트워크는 이용자들의 생활과 매우 밀접한 위치에 있기에, 이러한 네트워크를 보호해야 할 필요성이 높아지고 있다.

최근 몇 년 동안 인터넷을 통한 각종 피해가 지속적으로 발생하고 있는데, 특히 올해 7월 DDoS

공격으로 DDoS의 심각성이 사회에 크게 대두되어 최근 행정안전부는 분산공격트래픽에 대한 대응방안의 일환으로 올해(2009년) 중 132개 행정· 공공기관에 약 200억원을 투자해 분산서비스거부(DDoS) 공격 대응체계를 긴급 구축할 것이라고 밝혔다. 또한 지난 10월 방송통신위원회로부터 제출받은 자료에 따르면 인터넷전화(VoIP) 전체 사업자 가운데 46%, 별정사업자 73%는 분산서비스거부(DDoS) 공격 발생 시 대응 능력이 매우 미흡한 것으로 드러났다.

이처럼 유해트래픽에 대한 대응은 매우 중요한 사회의 이슈로 부각되고 있으며, 네트워크의 빠른 진화에 맞추어 지속적인 보안 문제의 대응이 필요하다.

2. 관련연구

기존의 DDoS(Distributed Denial of Service) 공격을 탐지하고 예방하는 방법에는 패턴에 기반한 필터링(Pattern-based Filtering) 기술이나 큐 관리(Queue Management)와 같은 방법들이 있다. 이러한 기존의 방법들은 주로 네트워크 상의 트래픽을 관찰하여 DDoS 공격이 있는지를 탐지하는데, 알려진 패턴에 대해서만 공격 탐지와 예방을 한다는 단점이 있다.

이러한 단점을 해결하기 위해 데이터가 목적지 주소의 다음 홉 주소를 변경하지 않고 정해진 터널을 지나가게 하고, 이 터널에서 ACL(Access Control List), Rate-Limit, 분석 등의 필요한 작업을 한 후에 정상적인 트래픽일 경우, 터널을 빠져나가 원래의 목적지로 전송될 수 있도록 내보내는 싱크홀 터널링(Sinkhole Tunneling) 기술이 제안되었다. 이러한 공격 차단 방법은 먼저 분석 장비들이 연결되어 있는 싱크홀 라우터를 준비해야 하고, 라우터에서 패킷들을 싱크홀 라우터로 들어가게 하는 터널을 생성해야 한다.

하지만, 종래의 싱크홀 터널링 기술에서, 싱크홀 라우터를 따로 만들지 않고 알려지지 않은 패턴의 유해트래픽에 대한 실시간 탐지 및 대응 방법은 정의되고 있지 않다.

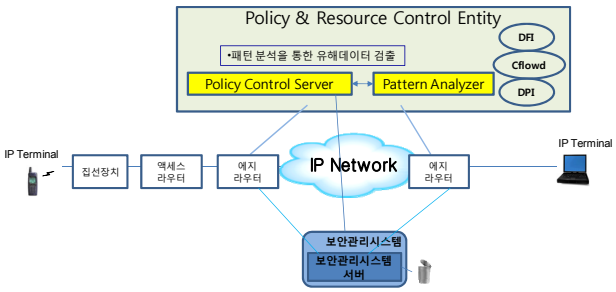
본 논문에서는 유해트래픽을 4가지로 종류로 분류하고, 각각의 특징 분석을 통하여, 효과적인 유해트래픽 탐지법을 알아보고 진단한다.

3. 본론

본 장에서는 유해트래픽의 분류, 탐지 및 대응 방법에 대하여 살펴본다.

3.1. 유해트래픽 탐지 대응 시스템

유해트래픽 탐지 대응 시스템은 싱크홀 라우터를 따로 만들지 않고, (그림1)과 같이 패턴분석기와 정책제어서버가 포함된 정책자원제어장치(Policy & Resource Control Entity)와, 정책라우팅 기능을 가지는 라우터, 그리고 보안관리서버로 구성된다.



(그림 1) 유해트래픽 탐지/대응 시스템

송신단말과 수신단말은 휴대폰, PDA 등을 포함하는 IP 주소를 가진 단말기로서 VoIP, MMOIP 서비스 등을 제공할 수 있다.

■ 정책자원제어장치

정책자원제어장치는 전송계층(Transport Stratum)에 존재하며 정책제어서버와 패턴분석기를 포함한다.

정책제어서버는 라우터의 DFI(Dynamic Flow Identification) 기능 및 DPI(Deep Packet Inspection) 기능 수행을 위한 DFI 정보 및 DPI 정보를 라우터로 전송한다. DFI 정보는 존속기간, 평균패킷크기, 평균 전송률 및 바이트 카운트 등의 범위를 포함하고, 라우터는 이 범위를 벗어나면 해당 데이터를 유해트래픽으로 간주하게 된다.

패턴분석기는 라우터로부터 수신한 Cflowd 정보를 이용하여 수신된 데이터가 알려지지 않은 패턴 또는 시그니처를 포함하는 유해트래픽인지 여부를 판정한 후, 판정 결과를 라우터로 전송한다.

유해트래픽 검출을 위한 정책자원제어장치는 다음의 기능과 정보를 가지고 있어야 한다.

- ➢ 패턴분석을 통한 유해데이터 검출 기능
- ➢ DFI, DPI, Cflowd 정보

■ 라우터

라우터는 정책라우팅 기능을 가지는데, DFI 기능 및 DPI 기능을 이용하여 수신된 데이터가 알려진 패턴 또는 시그니처를 포함하는 유해트래픽인지 여부를 판정하게 된다.

또한 라우터는 유해트래픽 데이터를 IP 캡슐화 기능을 이용하여 캡슐화하고, 캡슐화된 데이터에 보안관리버서의 IP 주소를 수신자로 지정한 헤더를 추가하여 보안관리서버로 전송한다.

유해트래픽 검출을 위한 라우터의 주요 기능을 살펴보면 다음과 같다.

- ➢ DFI(Dynamic flow identification)
- ➢ DPI(Deep Packet Inspection)
- ➢ Cflowd
- ➢ Policy Routing
- ➢ IP Encapsulation 기능

■ 보안관리서버

보안관리서버는 캡슐화된 데이터를 라우터로부터 수신하고, 캡슐화된 데이터가 유해트래픽인지 여부를 재확인하며, 캡슐화된 데이터가 유해트래픽이 아닌 경우, IP 역캡슐화(Decapsulation) 기능을 이용하여 보안관리서버의 IP 주소를 포함하는 헤더를 제거한 후 라우터로 전송한다.

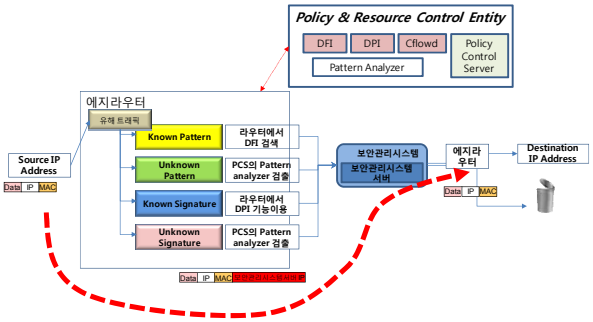
보안관리서버는 캡슐화된 데이터가 유해트래인 경우, 캡슐화된 데이터의 근원지 IP 주소를 저장하고, 캡슐화된 데이터를 삭제하며, 근원지 IP 주소 관련 정보들을 정책제어서버로 전송한다.

3.2. 유해트래픽 분류

유해트래픽은 분산공격트래픽, 바이러스 등을 모두 포함하는데, 유해트래픽의 종류는 알려진 패턴/시그니처를 포함하는 경우와 알려지지 않은 패턴/시그니처를 포함하는 경우로 나누어볼 수 있다.

■ 유해트래픽의 종류

- ➢ 알려진 패턴
- ➢ 알려지지 않은 패턴
- ➢ 알려진 시그니처
- ➢ 알려지지 않은 시그니처



(그림 2) 유해트래픽의 분류 및 검출방법

패턴검색과 시그니처 검색은 다음과 같이 유해트래픽 검출에 이용된다.

■ 패턴검색

- ➢ 분산공격트래픽에 대한 유해트래픽 검출

■ 시그니처 검색

➢ 바이러스에 대한 유해트래픽 검출

(그림 2)를 참조하면, 라우터는 DFI 기능을 이용하여 이미 알려진 패턴의 분산공격에 대한 유해트래픽을 검출하고, DPI 기능을 통해 이미 알려진 바이러스에 대한 유해트래픽을 검출하게 된다.

패턴 분석기는 라우터로부터 수신된 데이터의 Cflowd 정보를 수신하고, 수신한 Cflowd 정보를 이용하여 수신된 데이터가 알려지지 않은 패턴 또는 시그니처를 포함하는 유해트래픽인지 여부를 판정한다. 이때 해당 데이터가 유해트래픽인 경우 패턴분석기는 판정결과를 라우터로 전송하고, 라우터는 데이터를 IP 캡슐화 기능을 이용하여 보안관리서버의 IP 주소를 수신자로 지정한 헤더를 추가하여 캡슐화하며, 보안관리서버로 전송한다.

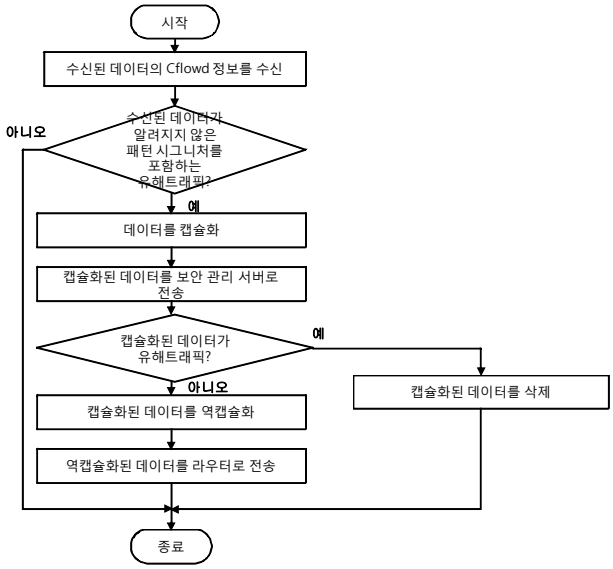
보안관리서버는 캡슐화된 데이터가 유해트래픽인지 여부를 재확인하고, 캡슐화된 데이터가 유해트래픽인 경우 캡슐화된 데이터를 삭제한다.

3.3. 유해트래픽 탐지/대응 방법

유해트래픽 탐지 및 대응 방법을 살펴보면, 크게 라우터에서는 유해트래픽 탐지를 하고, 보안관리서버에서 유해트래픽 대응을 한다고 볼 수 있다.

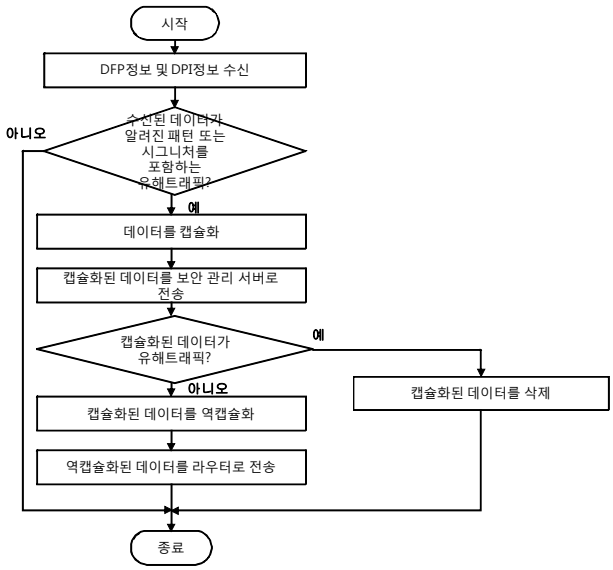
유해트래픽 탐지를 위하여 라우터는 여러 추가 기능을 가져야 하며, 향후 All-IP 통합망에서는 이러한 라우터의 역할이 더욱 커질 것으로 기대된다.

(그림 3)은 알려지지 않은 패턴/시그니처에 탐지 방법으로서, 패턴분석기로부터 Cflowd 판정결과를 전달받은 라우터는 수신된 데이터가 유해트래픽인 경우 데이터를 캡슐화하여 보안관리서버로 전송한다. 이때 보안관리서버는 캡슐화된 데이터를 다시 검사하여 유해트래픽인경우 데이터를 삭제하고, 유해트래픽이 아닌경우, 다시 데이터를 라우터로 전송하여 사용자가 제공받던 통신서비스에 지장을 주지 않아야 한다.



(그림 3) 알려지지 않은 패턴 또는 시그니처를 포함하는 유해트래픽 탐지/대응 방법

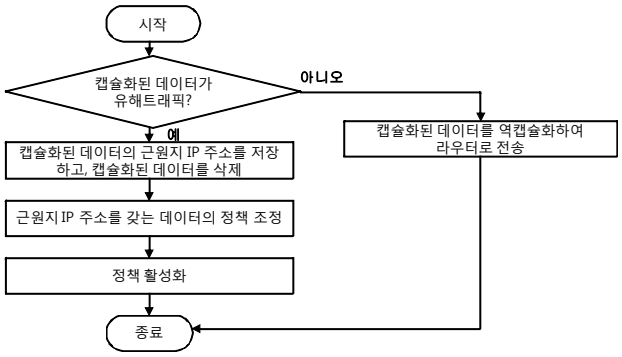
(그림 4)는 알려진 패턴/시그니처를 포함하는 유해트래픽 탐지 방법으로서, 라우터는 DFI 기능 및 DPI 기능을 수행하기 위해 정책제어서버로부터 DFI 정보 및 DPI 정보를 수신하고, DFI 기능 및 DPI 기능을 이용하여 수신된 데이터가 알려진 패턴 또는 시그니처를 포함하는 유해트래픽인지 여부를 판정한다.



(그림 4) 알려진 패턴 또는 시그니처를 포함하는 유해트래픽 탐지/대응 방법

(그림 5)는 유해트래픽 대응 방법의 예로서, 보안관리서버 입장에서의 흐름 순서도를 나타낸다.

보안관리서버는 캡슐화된 데이터가 유해트래픽인 경우, 캡슐화된 데이터의 근원지 IP 주소를 저장하고, 캡슐화된 데이터를 삭제한다. 이어서 보안관리서버는 근원지 IP 주소를 정책제어서버로 전송하고, 정책제어서버는 근원지 IP 주소를 갖는 데이터의 정책을 조정하며, 해당 정책을 라우터로 전송하여 활성화한다. 즉, 정책제어서버는 라우터로 하여금 근원지 IP 주소를 갖는 데이터의 QoS(Quality of Service)를 관리하고(예를들면 Rate limit 등), 근원지 IP 주소를 사용하는 사용자의 플로우를 제어하도록 한다.



(그림 5) 유해트래픽 대응 방법의 예

4. 결론

최근 몇 년 동안 인터넷을 통한 각종 피해가 지속적으로 발생하고 있는데, 특히 트래픽 폭주를 일으키는 분산공격트래픽(DDoS) 공격의 심각성이 사회에 크게 대두되고 있다.

기존의 DDoS(Distributed Denial of Service) 공격예방 방법으로 패턴에 기반한 필터링(Pattern-based Filtering) 기술이나 큐 관리(Queue Management)와 같은 방법들은 주로 네트워크 상의 트래픽을 관찰하여 알려진 패턴에 대해서만 공격 탐지와 예방을 한다는 단점이 있다. 이러한 단점을 해결하기 위해 싱크홀 터널링(Sinkhole Tunneling) 기술이 제안되었는데, 이러한 공격 차단 방법은 먼저 분석 장비들이 연결되어 있는 싱크홀 라우터를 준비해야 하고, 라우터에서 패킷들을 싱크홀 라우터로 들어가게 하는 터널을 생성해야 하는 단점이 있다.

하지만, 종래의 싱크홀 터널링 기술에서, 싱크홀 라우터를 따로 만들지 않고 알려지지 않은 패턴의 유해트래픽에 대한 실시간 탐지 및 대응 방법은 정의되고 있지 않다.

본 논문에서는 싱크홀 라우터를 따로 만들지 않고, 알려지지 않은 패턴/시그니처를 포함하는 유해트래픽에 대한 실시간 탐지 및 대응을 위하여, 라우터의 기능 확장과 정책자원제어장치를 추가하였다. 이러한 라우터와 정책자원제어장치는 향후 All IP 통합망에서 네트워크관리를 위하여 사용될 수 있을 것이다.

[참고문헌]

[1] Internet Security System (ISS) White Paper “Distributed Denial of Service Mitigation”, 2002

[2] 패킷 필터링을 이용한 DDoS 공격 대응구조

[3] 송병학 외 4명, “BcN상에서의 DDoS에 대한 Anmaly Detection 연구”, 인터넷정보학회논문지 제 8권 제 2호, 2007.4

[4] 황찬규 외 3명,”비정상 트래픽 실시간 탐지/분석시스템 설계 및 구현”, KNOW Review, Vol. 10, No.1, August 2007