http://dx.doi.org/10.7236/JIIBC.2014.14.1.203
JIIBC 2014-1-27

플로우 분석을 이용한 분산 서비스 거부 공격 탐지 방법

Detection Method of Distributed Denial-of-Service Flooding Attacks Using Analysis of Flow Information

전재현, 김민준, 조정현, 안철웅, 김승호*

Jae-Hyun Jun, Min-Jun Kim, Jeong-Hyun Cho, Cheol-Woong Ahn, Sung-Ho Kim*

요 약 오늘날 DDoS 공격은 인터넷 안정성에 매우 중요한 위협을 가하고 있다. DDoS 공격은 대량의 트래픽을 네트워크에 전송함으로써 자원을 고갈시키고 정상적인 서비스 제공을 불가능하게 하며 사전 탐지가 힘들고 효율적인 방어가 매우 어렵다. 인터넷과 같은 대규모 망을 대상으로 한 네트워크 공격은 효과적인 탐지 방법이 요구된다. 그러므로 대규모 망에서 침입 탐지 시스템은 효율적인 실시간 탐지가 필요하다. 본 논문에서는 DDoS 공격에 따른 비정상적인 트래픽 범람을 방지하고 합법적인 트래픽 전송을 보장하기 위하여 플로우 정보 분석을 이용한 DDoS 공격 대응 기법을 제안한다. OPNET을 이용해 구현한 결과 DDoS 공격중에 원활한 서비스를 제공할 수 있는 것을 확인하였다.

Abstract Today, Distributed denial of service (DDoS) attack present a very serious threat to the stability of the internet. The DDoS attack, which is consuming all of the computing or communication resources necessary for the service, is known very difficult to protect. The DDoS attack usually transmits heavy traffic data to networks or servers and they cannot handle the normal service requests because of running out of resources. It is very hard to prevent the DDoS attack. Therefore, an intrusion detection system on large network is need to efficient real-time detection. In this paper, we propose the detection mechanism using analysis of flow information against DDoS attacks in order to guarantee the transmission of normal traffic and prevent the flood of abnormal traffic. The OPNET simulation results show that our ideas can provide enough services in DDoS attack.

Key Words : DDoS Attack Detection, Quality-of-Service, Flow Information

Ⅰ. 서 론

오늘날 네트워크는 인프라 구축이 일반화되고 컴퓨터에 저장하고 있는 자료에 대한 접근이 쉬워짐으로 사용자들에게 많은 편이성을 제공하고 있다. 그러나 컴퓨터 시스템에 대한 불법 접근 및 네트워크에 트래픽을 폭주시킴으로 정보 유출 및 제대로 된 서비스를 제공하지 못하게 하여 많은 경제적 피해가 야기되고 있으며 해킹 및 인터넷 침해에 대한 사고 사례가 매년 증가하고 있다.

분산 서비스 거부 (Distributed Denial of Service: DDoS) 공격은 오래 전부터 발생해온 공격 유형이다. 하지만 단순한 공격 기법임에도 불구하고 어디서나 쉽게 구할 수 있는 툴로 인해 인터넷 상에서 발생하는 공격 유형중에서 가장 심각하고 그 발생 횟수도 잦으며 효과적

*정회원, 경북대학교 컴퓨터학부
접수일자 : 2014년 1월 8일, 수정완료 : 2014년 1월 29일
게재확정일자: 2014년 2월 7일

Received: 8 January, 2014 / Revised: 29 January, 2014
Accepted: 7 February, 2014
*Corresponding Author: shkim@knu.ac.kr
School of Computer Science and Engineering, Kyungpook National University, Korea

으로 차단하기도 쉽지 않다[1]. 최근 분산 서비스 거부 공격의 주요 목적은 웹사이트나 서버에 네트워크 장애를 발생시켜 해당 업체에 정치적 또는 금전적인 요구를 하며 주로 실시간 서비스를 제공하는 게임거래사이트나 증권 사이트, 인터넷 포털 사이트 등의 다양한 업체들을 대상으로 공격 목표가 다양화 되고 있다. DDoS 공격은 처음 1990년대 말부터 발생하기 시작하여 지난 2000년 야후, 아마존 등 유명 웹 사이트에 대한 대대적인 DDoS 공격이 발생하였고, 그로인해 몇 시간씩 서비스를 중단하는 사태가 일어나고 막대한 피해가 발생하였으며, 2009년 7월 7일과 2011년 3월 3일 중요 웹사이트에 대한 DDoS 공격이 발생하였다. 그리고 최근 2013년 3월 20일에 각 금융과 방송사에 DDoS 공격이 발생하여 정상적인 서비스를 제공하지 못하는 사태가 발생하였다. DDoS 공격은 최초 발생한지 10년이 지났지만 공격이 아직까지도 시도되고 있고 그로 인한 피해가 지속적으로 발생하고 있는 실정이다.

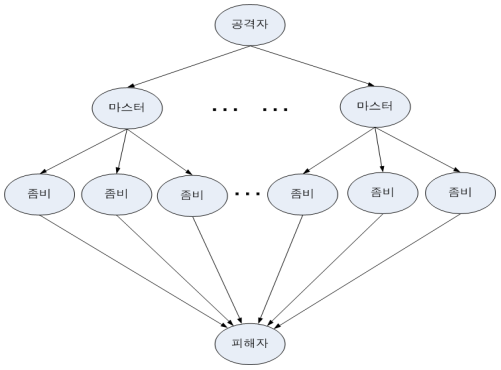

그림 1. DDoS 공격의 구조
Fig. 1. The structure of DDoS attack

표 1. 분산 서비스 거부 공격 노드의 역할
Table 1. Role of DDoS Node

이 름	역 할
공격자	모든 공격을 주도하는 공격자로서 DDoS 도구들을 원격으로 제어하고 직접 명령을 전달한다.
마스터	공격자로부터의 명령을 받아서 자신이 관리하는 좀비들에게 공격을 지시하는 역할을 한다.
좀 비	공격 프로그램은 각 마스터로부터 받은 명령을 수행하며 최종적으로 피해자에게 DoS 공격을 수행하는 역할을 한다.
피해자	공격의 최종적인 피해자로 여러 호스트로부터 동시에 DoS 공격을 받게 된다.

그림 1은 분산 서비스 거부 공격의 구조를 타낸다[3]. DDoS공격은 공격자, 마스터, 좀비, 피해자로 구성되어 있으며 각 역할은 표 1과 같다.

II. DDoS 검출/방어를 위한 기존 연구

DDoS 공격을 위험이 계속되는 가운데 DDoS 공격을 검출/방어하기 위해 여러 연구가 진행되고 있다[2,11,12,13]. 이러한 방법의 분류는 여러 가지 기준으로 이루어질 수 있다[3]. 본 논문에서는 네트워크 계층, 전송 계층, 응용 프로그램 계층에서 각각 검출/방어하는 방법을 소개한다.

첫 번째로, 패킷 전송률, 헤더 정보 등의 특징을 조사하여 검출/방어하는 네트워크 계층에서의 방법은 가장 많은 연구가 진행 중이다. MIB (Management Information Base) 정보를 이용하는 방법[4], 상호 상관 관계를 이용하여 어디서부터 언제 공격이 시작됐는지 결정하는 방법[5], 양방향 패킷 전송률의 비대칭성을 이용하는 방법[6] 등이 존재한다. 네트워크 계층에서의 검출/방어 방법은 반응 속도가 빠른 반면, IP (Internet Protocol) 헤더 등의 한정된 자료로 인해 정확도에서 손실이 있다.

전송 계층에서의 검출/방어 방법은 MIB를 이용하여 ICMP(Internet Control Message Protocol), UDP (User Datagram Protocl), TCP (Transmission Control Protocol) 패킷의 통계적인 유해성을 조사하는 방법[4], 폭주 공격을 방어하기 위해 TCP SYN/FIN 패킷을 이용하는 방법[7], 수신하는 SYN, FIN, RST, PSH, ACK, URG 등의 TCP 플래그 (flag)의 비율을 계산하는 방법[8] 등이 존재한다. 일반적으로 전송 계층의 프로토콜은 호스트 단위에서 수행되기 때문에, 공격이 목적지에 도달한 후에 검출되는 경우가 많다. 따라서, 수초 내에 이루어지는 DDoS 공격을 방어하기에 반응이 늦다는 문제점을 가진다.

마지막으로, 응용 프로그램 계층에서의 검출 방어 방법이 있다. HTTP 세션 (session)의 특징을 조사하여 통계적으로 공격 트래픽을 검출하는 방법[9], 특징 벡터와 기계 학습을 이용하여 DDoS 공격과 혼잡 상황을 구분하여 처리하는 방법[1] 등이 존재한다. 응용 프로그램 계층에서의 검출/방어 방법은 적용 대상에의 정확도는 높은 편이지만, 수많은 응용 프로그램이 존재하고 개발되고 있기 때문에 지속적인 통계 정보와 기계 학습이 이루어져야 한다는 단점이 있다.

Ⅲ. 플로우 분석을 이용한 DDoS 공격 탐지 방법

엔트로피의 개념은 1865년에 독일의 물리학자인 루돌프 클라지우스(Rudolf Julius Emanuel Clausius)에 의해 처음 제안되었다. 엔트로피는 불확실성(Uncertainty)을 야기시키기 때문에 엔트로피적인 상황에서는 다음에 어떤 일이 일어날 것인가의 예측이 전혀 불가능하다. 하지만 엔트로피가 감소하면 그에 따라 불확실성도 감소되어 부분적인 예측이 가능하게 된다.

엔트로피 H는 다음과 같이 정의된다.

$$H = -\sum_{i=1}^{n} P_i \log_2 P_i \qquad (1)$$

식 1에서 P_i 는 임의의 시간 동안 관찰한 것 중에 특정한 이벤트(패킷 수, 목적지 IP 주소. 송신지 포트 넘버)가 몇 번 관찰되었는지를 나타내는 확률이다.

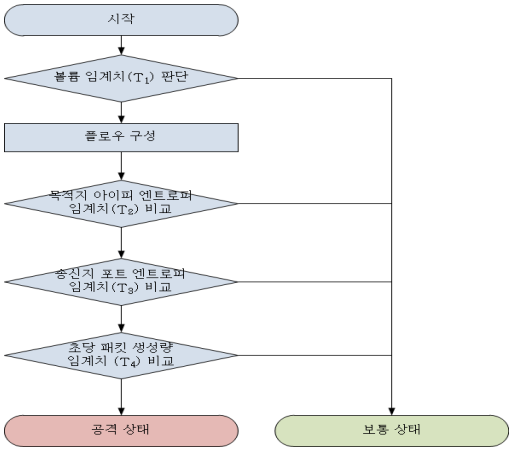

그림 2. 제안한 DDoS 공격 탐지 방법
Fig. 2. Proposed DDoS attack detection method

그림 2은 DDoS 공격을 탐지하기 위해 제안한 방법의 순서도이다. 처음에는 라우터로 들어오는 패킷량을 고려한다. 유입되는 트래픽량이 작다면 라우터가 배치된 네트워크에 큰 영향을 미치지 못하기 때문에 이것을 판단하는 부분이 필요하다. 그러므로 라우터로 유입되는 트래픽 Volume을 고려한다. 이때 이용되는 파라미터는 Volume 임계치(T_1)이다. 타임 윈도우를 정의하고, 이 타임 윈도우 동안 라우터로 들어오는 트래픽량을 측정한다. 만약 타임 윈도우 동안 수집한 트래픽량이 Volume 임계치(T_1)를 넘으면 다음 검출 단계로 보낸다. 만약 Volume 임계치(T_1)를 넘지 못한다면 아무 위험이 없는 상태로 판단한다.

위에서 Volume 임계치(T_1)를 넘었다면 수집한 트래픽을 5-투플(tuple)정보가 같은 3계층 패킷의 흐름으로 정의된다. 즉 일정 한도 이하의 공백 시간을 가지고 전송되는 송신지/목적지 주소,. 송신지/수신 포트, 프로토콜(Protocol) 필드의 값이 동일한 패킷들의 모임을 말한다. 플로우는 다음 수식 (2)을 통해서 정의될 수 있다.

$$f = \{p_0, p_1, p_2, ..., p_i\}, \ \text{if } T_{p_{i+1}} - T_{p_i} > T \qquad (2)$$

위의 수식에서 p_i는 5-투플 정보가 동일한 패킷, T_{p_i}는 패킷 p_i의 도착 시간, T는 패킷 간의 임계치 시간을 나타낸다. 플로우 f는 패킷 p_i의 연속된 집합이며, 만약 p_i와 p_{i+1}의 도착 시간 간격이 임계치 시간 T 보다 크면 p_{i+1} 패킷을 포함한 이후의 패킷은 다른 플로우로 구별된다.

플로우를 구성한 후 목적지 IP 주소에 대한 엔트로피를 계산하여 목적지 IP 주소의 엔트로피 임계치(T_2)를 초과하는지 검사한다. 만약 라우터로 들어오는 트래픽이 몇몇 특정 목적지 IP 주소(피해자)로 향하고 있으면 엔트로피는 감소할 것이고, 여러 목적지 IP 주소로 향하고 있으면 엔트로피는 증가할 것이다. 그러므로 목적지 IP 주소의 엔트로피가 목적지 IP 주소의 엔트로피 임계치(T_2)보다 적으면 특정 목적지 IP로 향하고 있다고 판단한다.

다음으로 앞의 특정 목적지 IP 주소를 송신지 포트 넘버에 대한 엔트로피가 송신지 포트 넘버의 엔트로피 임계치(T_3)를 넘는지 검사한다. 만약 특정 목적지 IP로 향하는 트래픽에 대한 엔트로피 값은 패킷이 다양한 송신지 번호를 가지고 있으면 엔트로피 값은 높아 질 것이고 패킷이 적은 송신지 포트 번호를 가지고 있다면 엔트로피 값은 낮아지므로 특정 포트만 이용한다고 볼 수 있다. 송신지 포트 넘버의 엔트로피 임계치(T_3)를 넘으면 다음 단계로 간다.

마지막 단계는 위험 대상이 되는 플로우에 대한 초당 패킷 생성량을 비교한다. 위험 플로우에 시간당 패킷 생성량이 초당 패킷 생성량 임계치(T_4)를 넘어서면 DDoS 공격 플로우라 판단하고 넘지 못한다면 일반 플로우라 판단한다.

Ⅳ. 실험 및 결과

4장에서는 본 논문에서 제안한 플로우 분석을 이용한 DDoS 공격 탐지 방법의 성능에 대해 알아본다. 제안한 DDoS 공격 탐지 방법은 피해자에 제일 인접한 라우터에 적용하였다. 그리고 라우터에 들어오는 트래픽의 Volume 임계치 값(T_1), 유입되는 트래픽의 목적지 IP 주소의 엔트로피의 임계치 값(T_2)과 해당 트래픽의 송신지 포트 넘버의 엔트로피 임계치 값(T_3)을 이용한다. 마지막으로 해당 플로우의 패킷 생성량의 임계치(T_4)를 이용하여 DDoS 공격인지 탐지 한다. 성능을 측정하기 위해 네트워크 시뮬레이터로 OPNET을 이용하였다.

1. 실험 환경

제안한 방법의 성능을 검증하기 위해 네트워크 시뮬레이터인 OPNET을 이용하였다. 실험에 이용한 트래픽은 DDoS 공격을 할 때 사용하는 DDoS 트래픽과 웹 서비스, 전자 메일등을 이용할 때 사용하는 Normal 트래픽이다. 이 2가지(DDoS, Normal) 트래픽으로 실험하였다.

실험 토폴로지 구성은 19개의 노드와 1개의 서버 그리고 5개의 라우터로 구성되어 있으며, 그 형태는 그림 3와 같다. 각 노드의 역할로는 DDoS 공격 트래픽을 생성하여 서버로 보내는 12개의 노드들(node_1~node_12)과 웹 서비스, 전자 메일등에 사용하는 Normal 트래픽을 생성하여 server, node_17, node_18, node_19에 각각 보내는 node_13, node_14, node_15, node_16이 있다. 그리고 각 라우터는 트래픽을 전송하는 역할을 한다. 그리고 서버에 가까이 있는 router_5는 DDoS 공격을 검출하기 위해 트래픽을 수집하는 시간인 타임 윈도우를 6초로 설정하여 DDoS 공격 탐지 방법을 적용시켰다.

2. 실험 결과 및 분석

이 절에서는 제안한 방법의 성능을 OPNET을 이용하여 구성한 토폴로지 상에서 실험한 결과를 기술한다. 실험은 그림 3와 같이 구성한 시뮬레이션 네트워크 구성에서 DDoS 공격이 발생했을 때 DDoS 공격을 탐지할 수 있는지 실험한다.

그림 4은 각 노드별 패킷 생성량을 나타낸 것이다. 가로축은 시간을 나타내며 새로축은 패킷의 수를 나타내고 있다. DDoS 공격을 수행하는 노드들 (node_1~node_12)은 DDoS 공격하기 위해 각각 초당 약 400, 340, 280개의 패킷을 생성하고 있다. 그리고 웹 서비스, 전자메일에 해당하는 역할을 수행하는 노드들(node_13~node_16)은 초당 약 40개의 패킷을 생성하는 것을 볼 수 있다. 여기서 볼 수 있듯이 웹 서비스, 전자메일에 해당하는 패킷보다 DDoS 공격에 이용되는 DDoS 공격 패킷이 월등히 많은걸 볼 수 있다.

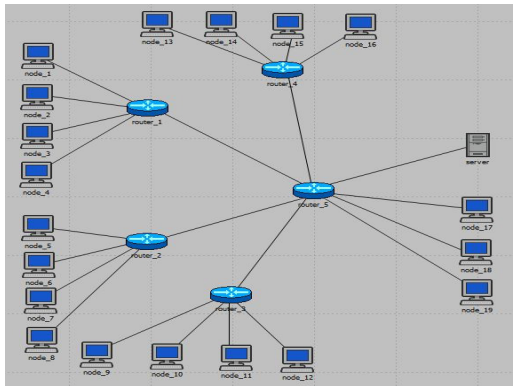

그림 3. 시뮬레이션 네트워크 구성
Fig. 3. Composition of simulation network

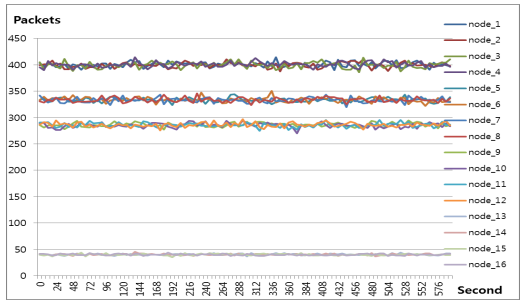

그림 4. 각 노드별 패킷 생성량
Fig. 4. Creation rate each node packet

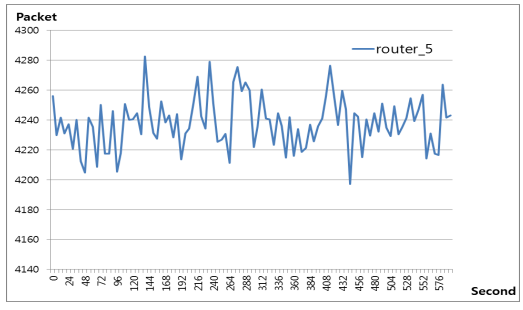

그림 5. DDoS 공격시 라우터 5로 유입되는 트래픽량
Fig. 5. Traffic amount flow in router_5 when DDoS attack

그림 5는 DDoS 공격시 라우터5로 유입되는 트래픽량을 수집한 것을 나타내었다. 가로축은 시간을 나타내고 있으며 세로축은 패킷들의 수를 나타낸다. DDoS 공격이 일어나는 동안 초당 약 4200개의 패킷이 라우터로 들어오는 것을 볼 수 있따. 1단계 위험을 판단하는 Volume 임계치 값(T_1) 1500을 훨씬 웃도는 값이다. 그러므로 1차 위험이라 판단 할 수 있다.

그림 6은 DDoS 공격이 발생했을 때 라우터5로 유입되는 트래픽의 목적지 IP 주소의 엔트로피를 나타낸다. DDoS 공격이 일어나는 동안 목적지 IP 주소의 엔트로피 값은 약 0.23인 것을 볼 수 있다. 2단계 위험을 판단하는 임계치 값(T_2) 0.4를 훨씬 밑도는 값이다. 일반적으로 유입되는 트래픽의 목적지 엔트로피 값이 낮을수록 어느 특정 방향으로 흐르는 것을 판단할 수 있기 때문에 2차 위험이라 판단 할 수 있다.

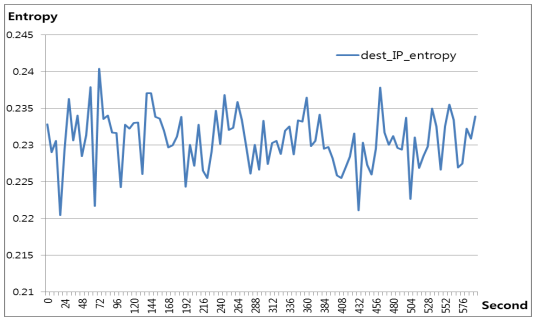

그림 6. DDoS 공격이 발생했을 때 라우터 5로 유입되는 트래픽의 목적지 IP 주소의 엔트로피

Fig. 6. The entropy of destination IP address incoming traffic in router_5 when DDoS attack happens

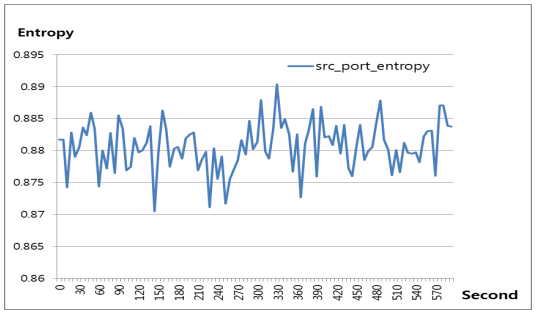

그림 7. 2차 위험이라 판단한 트래픽의 송신지 포트 번호의 엔트로피

Fig. 7. The entropy of source port number of traffic judged the second danger

그림 7은 2차 위험이라 판단된 목적지 IP 주소의 송신지 포트의 엔트로피를 나타낸다. DDoS 공격은 많은 송신지 포트를 이용하는데 그림에서 보듯이 송신지 포트의 엔트로피가 약 0.88인 것을 볼 수 있다.

이것은 3단계 위험을 판단하는 송신지 포트의 엔트로피 임계치 값(T3) 0.8을 훨씬 웃도는 값이다. 그러므로 3차 위험이라 판단할 수 있다.

4차 위험 판단은 3차 위험까지 판단한 플로우의 패킷 생성량을 가지고 판단할 수 있다. 그림 8에서 보듯이 공격노드는 초당 약 400, 340, 280개의 패킷을 생성하고 있다. 이것은 패킷 생성량 임계치(T4) 60을 넘는 것을 볼 수 있다. 따라서 플로우의 정보를 이용하여 4단계 정보를 분석하여 DDoS 공격 플로우를 탐지할 수 있다.

그림 8과 그림 9은 DDoS 공격 상황일 때 서버와 가까운 라우터에서 트래픽을 분류하는 것을 보여준다.

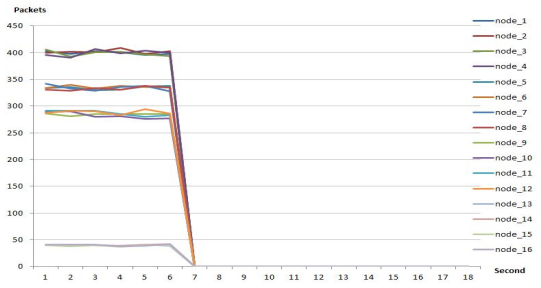

그림 8. 엔트로피의 Behavior 모델을 이용한 DDoS 공격 탐지 방법을 적용한 후 서버로 들어오는 트래픽

Fig. 8. The traffic came to server after applying DDoS attack detection method by using Behavior

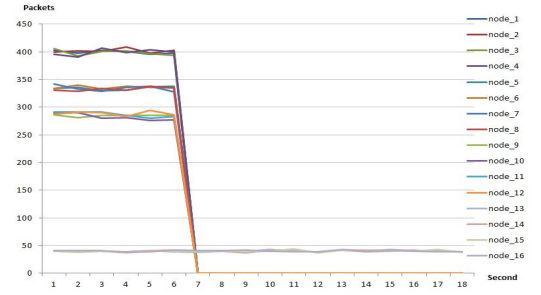

그림 9. 제안한 방법을 이용한 DDoS 공격 탐지 방법을 적용한 후 서버로 들어오는 트래픽

Fig. 9. The traffic came to server after applying DDoS attack detection method by using entropy

그림 8은 Behavior[10]를 적용했을 때 트래픽을 분류하는 것을 보여준다. [10]는 목적지 IP 엔트로피를 기반으로 송신지 포트의 엔트로피와 송신지 IP의 엔트로피가 크고 목적지 포트의 엔트로피가 적으면 공격 트래픽으로 분류한다. 이것을 적용한 결과 그림 8와 같이 node_1에서 node_12가 발생한 DDoS 공격을 탐지할 수 있다. 하지만 일반노드(node_13~node_16)도 위의 조건을 만족하므로 DDoS 공격이라 판단하고 모두 차단하는 것을 볼 수 있다.

그림 9은 제안한 방법을 적용했을 때 트래픽을 분류하는 것을 보여준다. [10]에서는 엔트로피만을 이용하여 공격을 탐지 하였지만 제안한 플로우 정보를 이용하여 엔트로피와 초당 패킷 생성량 그리고 송신포트의 임계치를 이용해 DDoS 공격 노드(node_1~node_12)를 탐지할 수 있다 공격 트래픽은 정확하게 탐지하고 차단하며, 일반 플로우 분류하여 정상적인 서비스가 가능한 것을 보여준다.

V. 결 론

본 논문에서는 플로우가 가지는 정보들을 기반으로 분석하여 사회적으로 큰 문제가 되고 있는 DDoS 공격을 검출하는 방법을 제안하였다. DDoS 공격을 검출해 냄으로써, 제어 방법에 따라 공격자 또는 좀비 호스트의 공격 트래픽을 조절하는 것이 가능하다. 이를 통하여 공격의 목표지는 지속적으로 일반 사용자에게 정상적인 서비스 제공이 가능할 것이다. 제안한 방법의 탐지 성능은 실험 결과를 통해 제시하였다.

어플리케이션 DDoS 공격은 부하가 많이 걸리는 패킷을 적게 보냄으로 공격을 수행한다. 따라서 Volume 기반한 공격 탐지 방법은 어플리케이션 DDoS 공격을 탐지할 수 없다. 하지만 엔트로피 파라미터는 다른 여러 파라미터보다 high sensitive 하기 때문에 어플리케이션 DDoS 공격을 탐지하는데 더 유용할 것이라 생각한다. 따라서 어플리케이션 DDoS 공격을 탐지하기 위해서 엔트로피의 특성을 이용한 탐지 방법의 연구가 향후 필요할 것이다.

References

[1] Y. Xie and S. Z. Yu, "Monitoring the Application-Layer DDoS Attacks for Popular Websites," IEEE/ACM Trans on Networking, vol 17, No. 1, pp. 15-25, Feb. 2009.

[2] H.g Noh and N. Kang, "Efficient Buffer Management Scheme for Mitigating Possibility of DDoS Attack," The Journal of The Institute of Webcasting, Internet and Telecommunication, vol 12, no. 2, pp. 1-7, Apr. 2012.

[3] J. Mirkovic and P. Reiher, "A Taxonomy of DDoS Attack and DDoS Defense Mechanisms," in ACM SIGCOMM Computer Communications Review, vol. 34, no. 2, pp. 39-53, Apr. 2004.

[4] J. B. D. Cabrear, L. Lewis, X. Qin, W. Lee, R. K. Prasanth, B. Ravichandran, and R. K. Mehra, "Proactive Detection of Distributed Denial of Service Attacks using MIB Traffic Varables - A Feasibility Study," in Proc. of the IEEE/IFIP International Symposium on Integrated Network Management, pp. 609-622, May 2001.

[5] J. Yuan and K. Mills, "Monitoring the Macroscopic Effect of DDoS Flooding Attacks," in IEEE Transactions on Dependable and Secure Computing, vol. 2, no. 4, pp. 324-335, Oct.-Dec. 2005.

[6] J. Mirkovic, G. Prier, and P. L. Reiher, "Attacking DDoS at the Source," in Proc. of the 10th IEEE International Conference on Network Protocols, pp. 312-321, nov. 2002.

[7] H. Wang, D. Zhang, K. G. Shin, "Detecting SYN Flooding Attacks", in Proc. of IEEE INFOCOM, vol. 3, pp. 1530-1539, Jun. 2002.

[8] S. Noh, C. Lee, K. Choi, and G. Jung, "Detecting Distributed Denial of Service (DDoS) Attacks through Inductive Learning," in Lecture Notes in Computer Science, vol. 2690, pp. 286-295, 2003.

[9] S. Ranjan, R. Swaminathan, M. Uysal, and E. Knightly, "DDoS-Resilient Scheduling to Counter Application Layer Attacks under Imperfect Detection," in Proc. of IEEE INFOCOM, pp. 1-13, Apr. 2006.

[10] X. Kuai, Z. Zhi, and B. Supratik, "Profiling Internet Backbone Traffic Behavior Models and

Applications," ACM SIGCOMM, vol.35, no.4, pp.169-180, Oct. 2005.

[11] H, K. Kim and Y. Ky Chung, "Framework for Anomaly Traffic Detection and Queue Management Component," Journal of Advanced Information Technology and Convergence, vol.7, no.3, pp.156-170, Jun. 2009.

[12] K, K. Shin, U. C. Park, and M. S. Jun, "A Design of SMS DDoS Detection and Defense Method using Counting Bloom Filter," Proceedings of the KAIS Fall Conference, vol.1, pp.53-56, May. 2011.

[13] H. Noh and N. Kang, "Efficient Buffer Management Scheme for Mitigating Possibility of DDoS Attack," The International Journal of Internet, Broadcasting and Communication, vol.12, no.2, pp.1-7, Apr. 2012.

저자 소개

전 재 현(준회원)

- 2009년 : 대구가톨릭대학교 전자공학과 (공학사)
- 2011년 : 경북대학교 전자전기컴퓨터학부 (석사)
- 2011년 ~ 현재 : 경북대학교 컴퓨터학부 박사과정

<주관심분야: 트래픽 분류, 디도스 공격 탐지, H.264/AVC, H.265, 멀티미디어>

김 민 준(정회원)

- 2005년 : 경북대학교 컴퓨터공학과 (공학사)
- 2007년 : 경북대학교 컴퓨터공학과 (공학석사)
- 2012년 : 경북대학교 전자전기컴퓨터학부 (공학박사)
- 2012년~현재 : ㈜에이투텍 책임연구원

<주관심분야: 트래픽 분류, 침해 트래픽 특성 연구, 멀티미디어, 기계학습>

조 정 현(정회원)

- 1988년 : 경북대학교 전자공학과 (공학사)
- 1990년 : 경북대학교 컴퓨터공학과 (공학석사)
- 2005년 : 경북대학교 컴퓨터공학과 (공학박사)
- ~ 현재 : 영남이공대학 컴퓨터계열 교수

<주관심분야: 영상처리, 네트워크>

안 철 웅(정회원)

- 1993년 : 경북대학교 컴퓨터공학과 (공학사)
- 1995년 : 경북대학교 컴퓨터공학과 (공학석사)
- 2009년 : 경북대학교 컴퓨터공학과 (공학박사)
- 2001년 ~ 현재: 계명문화대학교 디지털콘텐츠학부 교수

<주관심분야: 멀티미디어, 멀티미디어통신, 이미지 처리, 이미지 검색, 빅데이터 처리>

김 승 호(정회원)

- 1981년 : 경북대학교 전산학과 (공학사)
- 1983년 : 한국과학기술원 전산학과 (공학석사)
- 1994년 : 한국과학기술원 전산학과 (공학박사)
- 1986년 ~ 현재 : 경북대학교 컴퓨터학부 교수

<주관심분야: 멀티미디어, 다시점영상, 트래픽 분류, 동기식 네트워크>