# 플로우 정보를 이용한 폭주 분산 서비스 거부 공격 검출 방법

김민준*, 전재현*, 길기범*, 김승호**
*경북대학교 전자전기컴퓨터학부
**경북대학교 컴퓨터학부
e-mail:{mjkim, jhjun, gbkil}@mmlab.knu.ac.kr shkim@knu.ac.kr

# A Method for Detecting Flooding Distributed Denial-of-Service Attacks Using Flow Information

Min-jun Kim*, Jae-hyun Jun, Gi-bum Kil, Sung-ho Kim*
*Electrical Engineering and Computer Science, Kyungpook National University
**School of Computer Science and Engineering, Kyungpook National University

요 약

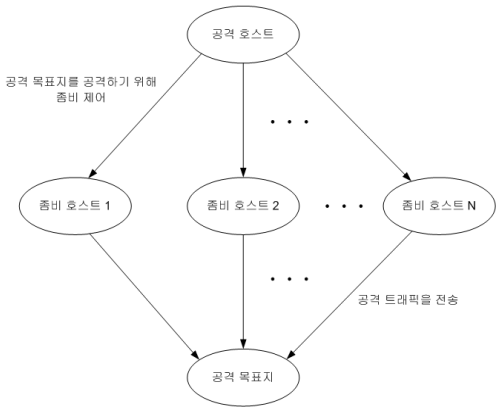
분산 서비스 거부 공격은 인터넷이 매우 발달한 현대 시대에 큰 위협으로 등장하였다. 분산 서비스 거부 공격은 단순히 정상적인 서비스 제공이 어렵다는 문제만 아니라 어디서부터 시작된 공격인지, 어떤 경로를 통해서 공격이 진행되는지 알아내기가 힘들다는 점에서 공격을 방어하기가 매우 어려운 문제에 직면하게 된다. 또한 공격의 목표가 DNS 서버 또는 백본 라우터 등이 된다면 인터넷 서비스 자체도 힘들어 질 수 있다. 이러한 이유로 분산 서비스 거부 공격 방어 시스템이 개발되어야할 필요성이 높아지게 된다. 본 논문에서는 분산 서비스 거부 공격을 방어하기 위해 필요한 공격의 검출, 특히 폭주 분산 서비스 거부 공격을 검출해 내기 위해 플로우 정보를 이용하는 방법을 제시한다. 폭주 분산 서비스 거부 공격의 성능은 일반적인 네트워크 트래픽을 이용해 평가하였다.

## 1. 서론

인터넷은 쉬운 접근성을 가진다는 장점으로 인해 큰 성공을 거두었다. 전 세계의 수많은 사람들이 인터넷을 쉽게 이용할 수 있고 또한 인터넷의 정보량 또한 크게 증가하였다. 하지만 동전의 양면처럼 인터넷의 쉬운 접근성의 특징은 유해 트래픽의 증가라는 결과를 가져왔다[1].

유해 트래픽의 유형은 크게 두 가지로 분류될 수 있다. 첫 번째는 유해 사용자가 인터넷을 통하여 원격지에 있는 컴퓨터에 접근하여, 주요한 데이터를 획득하거나 변경, 삭제하는 경우이다. 이러한 공격은 E-메일을 이용한 웜 바이러스, 각종 악성 코드, 백도어 프로그램을 통하여 이루어진다. 두 번째 유형은 공격의 목표가 되는 시스템이 정상적인 서비스를 불가능 하도록 또는 방해하는 공격의 형태이다. DoS (Denial-of-Service: 서비스 거부) 공격 또는 DDoS (Distributed Denial-of-Service: 분산 서비스 거부) 공격이 이 공격에 해당한다. DoS 공격이나 DDoS 공격은 정상적인 트래픽인척 동작하므로 피해를 받는 목표지는 검출하기가 힘들다는 특징을 가진다[4].

DoS 공격은 공격자 혼자 공격 목표지의 서비스 제공을 방해하거나 막는 공격이다[3]. DoS 공격은 침투 공격처럼 중요한 데이터를 획득하여 이용하거나, 변경, 삭제하는 행위를 취하지 않으므로 위협적이지 않다고 여길 수 있다. 하지만 DoS 공격은 목표지의 목적에 따라 충분히 위협적으로 동작할 수 있다. 실례로 2002년에 DNS (Domain Name System)의 루트 서버가 DoS 공격을 멈추게 됨으로써 수많은 도메인 네임 서비스 요청이 폐기된 사태가 발생되었다. 이처럼, DNS의 주요 서버 또는 기본 라우터 (default router) 등이 공격당하는 경우에는 엄청난 사태가 발생될 수 있음을 의미한다.




(그림 1) 분산 서비스 거부 공격의 개념

DDoS 공격은 DoS 공격이 가지는 공격자 입장에서의 단점을 보완하기 위해 등장한 공격 방법이다. DoS 공격이 공격자 혼자 공격을 시도함으로써 목표지에서는 하나의 송신지에서 수 또는 양 측면에서 어느 수준 이상의 트래픽을 생성하는 경우 검출되어 차단될 확률이 높아질 수 있다. 따라서 공격 호스트는 악성코드 경유지에 악성코드를 숨겨두고, 경우지에 접속하는 사용자 컴퓨터를 감염시킨다. 이렇게 감염된 컴퓨터를 좀비 호스트라 지칭하고, 그림 1과 같이 추후 공격 호스트의 공격 명령을 받아 동시에 목표를 공격하는 공격을 감행하게 된다. 이런 DDoS 공격은 많은 좀비 호스트들이 동시에 DoS 공격을 수행하기 때문에 실제 공격자의 위치는 더욱 파악하기 힘들어지

고, 또한 공격 자체를 검출해 내기도 매우 어렵게 된다[5].

본 논문에서는 공격 플로우의 경우 공격이 수행되는 동안 검출되는 것을 피하기 위해 짧은 길이를 갖는 많은 수의 플로우를 좀비 호스트가 만들어 내는 특징을 이용하여 DDoS 공격을 수행하는 좀비 호스트를 검출하는 방법을 제안한다. 제안하는 검출 방법을 설명하기 위하여 본 논문은 2장부터 다음과 같이 구성된다. 2장에서는 DDoS 공격을 방어하기 위한 기존 연구들에 대하여 제시한다. 본 논문에서 제안하는 플로우 정보를 이용하여 폭주 (Flooding) DDoS 공격 검출 방법에 대하여 3장에서 설명한다. 4장에서 정상 트래픽과의 비교를 통하여 제안한 방법의 성능을 측정하고, 5장에서 결론을 맺도록 한다.

## 2. DDoS 검출/방어를 위한 기존 연구

DDoS 공격을 검출/방어하기 위한 방법의 분류는 여러 가지 기준으로 이루어질 수 있다[2]. 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[6], 상호 상관 관계를 이용하여 어디서부터 언제 공격이 시작됐는지 결정하는 방법[7], 양방향 패킷 전송률의 비대칭성을 이용하는 방법[8] 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[6], 폭주 공격을 방어하기 위해 TCP SYN/FIN 패킷을 이용하는 방법[9], 수신하는 SYN, FIN, RST, PSH, ACK, URG 등의 TCP 플래그 (flag)의 비율을 계산하는 방법[10] 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[11], 특징 벡터와 기계학습을 이용하여 DDoS 공격과 혼잡 상황을 구분하여 처리하는 방법[5] 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.

## 3. 플로우 정보를 이용한 폭주 DDoS 공격 검출

DDoS 공격 트래픽을 검출하기 위하여 본 논문에서는 플로우 정보 [12]를 이용한다. 플로우는 동일 시간대에 5-쌍 (tuple)정보가 같은 3 계층의 패킷의 흐름으로 정의된다. 즉, 일정 한도 이하의 공백 시간을 가지고 전송되는 송신지/수신지 주소, 송신/수신 포트, 프로토콜 (protocol) 필드의 값이 동일한 패킷들의 모임을 말한다. 플로우는 다음의 수식 (1)을 통해서 정의될 수 있다.

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

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

이렇게 정의된 플로우들은 각각의 매개 변수와 전달 특성을 갖는다. 이러한 플로우 매개 변수 (flow parameter)와 전달 특성은 DDoS 트래픽을 검출하기 위한 입력 데이터로 활용된다. 이러한 값들은 네트워크에서 검출되는 트래픽을 분석하고 분류하는데 사용되며, 응용 프로그램별로 각각 다른 매개 변수 값과 전달 특성을 가지고 있다. 플로우 매개 변수와 전달 특성은 세 가지로 정의한다.

첫째, 플로우 매개 변수로 하나의 플로우가 생성되고 종료되기까지의 특성을 나타낸다. 플로우 매개 변수의 종류는 플로우의 5-튜플 정보, 플로우를 구성하는 패킷 수를 나타내는 Packet Count, 패킷 사이즈의 총합을 나타내는 Flow Size, 플로우의 지속 시간을 나타내는 Flow Duration이다. 플로우 매개 변수의 종류는 연구를 통해 지속적으로 도출되어야 하며, 이러한 플로우 매개 변수만을 이용하여 특정 응용 프로그램에서 발생시키는 트래픽 특성을 표현할 수도 있다. 즉, 플로우 매개 변수는 단일 플로우를 나타낼 수 있는 특성 값으로 정의한다.

둘째, 파생된 (derived) 플로우 매개 변수로 플로우 매개 변수들의 조합된 결과로 나온 값이다. 파생된 플로우 매개 변수의 종류로는 플로우 내의 평균 패킷 크기를 나타내는 Average Packet Size, 플로우가 지속되는 동안의 평균 전송률인 Average Rate 등이 여기에 해당한다.

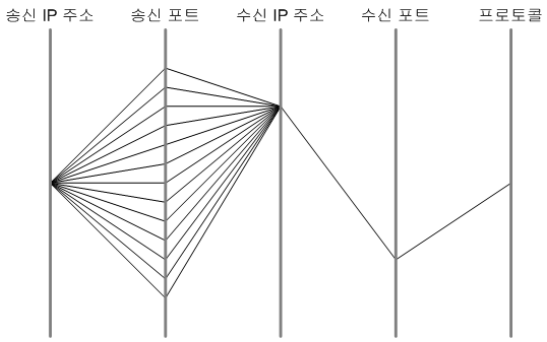
셋째, 플로우 패턴 (flow pattern)으로 하나의 호스트에서 발생한 플로우들의 상관관계로 정의된다. 예를 들어, 동일한 송신 호스트에서 여러 개의 송신 포트를 이용하여 한 대의 수신 호스트의 특정 포트를 향해 전송되는 경우, DoS 또는 DDoS 공격을 수행하는 좀비 호스트로 고려될 수 있는 것이다. 이러한 플로우들의 상관관계를 플로우 패턴으로 정의하고, 각 응용 프로그램의 동작 특성에 따라 다르게 정의될 것이다.

폭주 DDoS의 플로우는 다른 플로우와 구분되는 특징을 가진다. 즉, 하나의 송신 호스트 주소와 하나의 수신 호스트 주소를 가지며, 사용되는 플로우 수가 매우 많다. 또한 각각 플로우의 길이는 매우 짧다. 이는 검출을 피하기 위해서, 또한, 검출이 되더라도 공격자 입장에서의 피해가 최소가 되기 위해서이다.

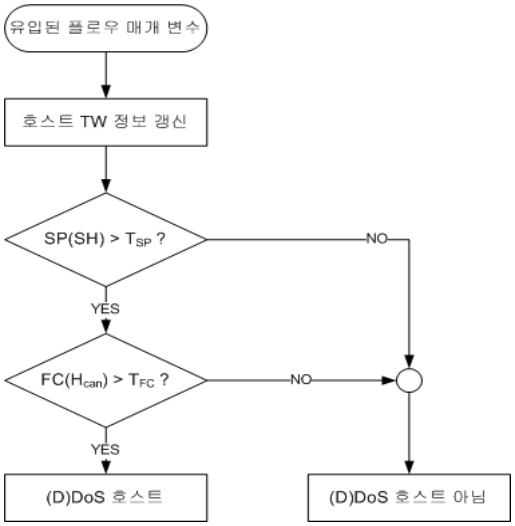
하나의 송신 호스트에서 하나의 수신 호스트로의 연결에서 플로우 수를 다수 개 만들어 내는 방법은 송/수신 포트를 변경하거나, 프로토콜 타입을 변경하여 가능해진다. 하지만 웹 서버를 주로 공격하는 폭주 DDoS 공격의 경우, 수신 포트는 HTTP (HyperText Transfer Protocol) 포트 번호인 80 포트를, 프로토콜 타입은 주로 공격 형태에 따라 고정된다. 따라서 송신 포트 수를 늘림으로써 플로우 수를 대량으로 취할 수 있다.

또한, 폭주 DDoS 공격 트래픽은 단위시간당 생성되는 플로우 수가 매우 많으며 지속적으로 이러한 형태가 유지되는 특징을 가진다. 앞에서 언급한 플로우 수가 많은 경우는 P2P (Peer-to-Peer) 트래픽의 경우에도 해당될 수가

있다. 하지만, 단위시간당 플로우 생성량이 많은 수가, 지속되는 경우는 폭주 DDoS 플로우로 판별할 수가 있는 것이다. 두 가지 폭주 DDoS 트래픽이 가지는 특징에 대해서는 그림 2에 설명한다.




(그림 2) 폭주 DDoS 트래픽이 가지는 특징




(그림 3) 폭주 DDoS 공격 호스트 검출 방법

앞에서 언급한 폭주 DDoS 플로우가 가지는 특징을 이용하여 본 논문에서는 그림 3과 같이 폭주 DDoS 공격을 수행하는 좀비 호스트를 검출한다. 송신 호스트가 전송하는 패킷을 조사하여 송신 호스트와 수신 호스트의 연결을 생성한다. 일정한 간격의 시간 윈도우 ($TW$: Time Window) 내에서 송신 호스트 ($SH$) 대 수신 호스트 간의 연결에서 사용되는 송신 포트 수 ($SP$)를 조사한다. 정상 트래픽과 비교하여 폭주 DDoS 공격의 경우 시간 윈도우 내에 많은 포트 수가 사용되므로, 송신 포트 임계치 ($T_{SP}$)를 넘는지 조사한다. 만약 임계치 이상의 송신 포트를 사용하는 경우 1차 위험군 ($H_{can}$)으로 분류가 되고, 1차 위험군에 속하는 호스트는 추가적으로 시간 윈도우 내의 시간당 평균 플로우 생성량을 조사한다. 만약 평균 플로우 생성량 ($FC$)이 플로우 생성량 임계치 ($T_{FC}$)를 넘는 경우 해당 플로우를 생성한 호스트는 폭주 DDoS 좀비 호스트로 검출된다. 폭주 DDoS 플로우 패턴 ($FP_{DDoS}$)은 수식 (2), (3), (4)와 같이 표현될 수 있다.

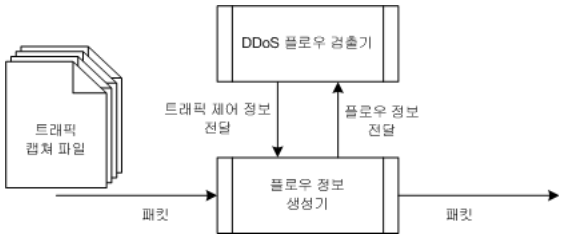
$$FP_{DDoS} = H_{can} \text{ and } FC_{many} \quad (2)$$

$$H_{can} = Host, \quad \text{if} \quad SP(SH) > T_{SP} \quad (3)$$

$$FC_{many} = FC(H_{can}) > T_{FC} \quad (4)$$

## 4. 실험 결과

본 논문에서는 플로우 정보를 이용한 폭주 DDos 공격 호스트 검출 알고리즘의 성능을 평가하기 위하여 그림 4와 같은 실험 환경을 구성하였다. 실제 네트워크에서의 성능 평가는 DDoS 트래픽이 유입되는 시점과 존재 유무가 불확실하여 공격 트래픽이 존재하는 실 트래픽을 하나의 중간 노드 (Intermediate node) 또는 하나의 호스트에서 캡쳐한 파일을 이용하였다.




(그림 4) 실험 진행 방법

그림 4의 트래픽 캡쳐 파일은 실제 트래픽에 해당하고, 플로우 정보 생성기는 이 파일을 분석하여 생성한 플로우 정보를 DDoS 플로우 검출기에 전달한다. DDoS 플로우 검출기에서는 본 논문에서 제안한 알고리즘을 통해 DDoS 공격 호스트를 검출하고 해당하는 제어 정보를 플로우 정보 생성기에 전달하여 유입되는 트래픽의 제어를 수행한다.

<표 2> 트래픽 캡쳐 파일의 특성

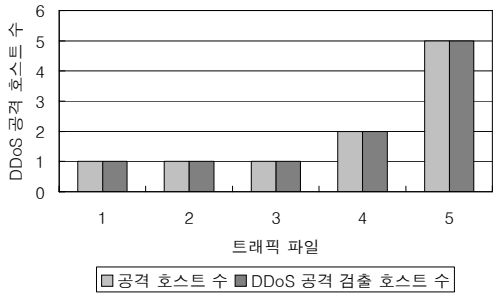
| No. | 공격 호스트 | 공격 유형 |
|---|---|---|
| 1 | 1대 | TCP SYNACK 폭주 |
| 2 | 1대 | TCP SYNACK 폭주 |
| 3 | 1대 | TCP SYN 폭주,<br>TCP ACK 폭주,<br>UDP 폭주, ICMP 폭주,<br>HTTP Get 폭주 |
| 4 | 2대 | TCP SYN 폭주,<br>TCP ACK 폭주,<br>UDP 폭주, ICMP 폭주,<br>HTTP Get 폭주 |
| 5 | 5대 | TCP SYN 폭주 |

실험을 위하여 시간 윈도우 크기는 1초 단위로 설정하여 슬라이딩 (sliding) 한다. 각각의 플로우는 종료된 시점에 따라 시간 윈도우 내의 정보를 갱신한다. 또한, 송신 포트 임계치는 30으로 설정하였고, 시간 윈도우 내 플로우 생성량 임계치는 20으로 설정하였다. 이는 일반적인 트래픽과의 비교를 통해 실험적으로 결정된 값으로 추후 알고리즘의 효율을 위해 수정될 수 있다.

공격 트래픽이 존재하는 트래픽 캡쳐 파일은 실험에서 총 5가지를 이용하였으며, 그 특징은 표 1과 같다. 공격 호스트의 수는 1대, 2대, 5대를 이용하여 공격이 진행되며, 공격은 TCP SYNACK 폭주 공격, TCP SYN 폭주 공격,

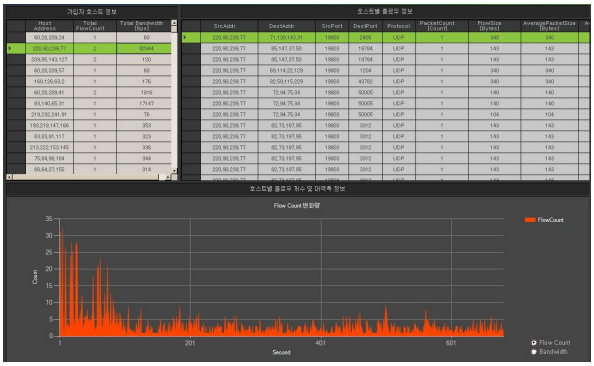
혼합 공격으로 구성된다.

표 1의 5가지 공격 트래픽 캡쳐 파일을 통해 DDoS 공격 호스트 검출 성능은 그림 5를 통하여 제시한다. 각각의 트래픽 파일에 존재하는 공격 호스트의 수와 동일한 수의 공격 호스트를 정확하게 검출한 것을 확인할 수 있었다.




(그림 5) 공격 호스트 검출 결과

정상적인 트래픽과의 비교를 위해 웹 트래픽, P2P 트래픽, 스트리밍 트래픽에 대해서도 실험을 진행하였다. 각각의 정상적인 트래픽에 대해서도 DDoS 공격 호스트로 오판하는 상황 없이 정확히 수행되는 것을 확인할 수 있었다. 그림 6은 P2P 응용 프로그램의 하나인 BitTorrent를 대상으로 실험을 진행한 결과를 나타낸다. 트래픽을 생성하는 호스트는 매우 많지만 DDoS 공격 호스트로 검출되지 않았다.



(그림 6) P2P 트래픽 실험 진행 결과

## 5. 결론

본 논문에서는 플로우가 가지는 정보들을 이용하여 사회적으로 큰 문제가 되고 있는 DDoS 공격, 특히, 폭주 DDoS 공격을 수행하는 좀비 호스트를 검출하는 방법을 제안하였다. DoS 공격의 경우 공격자를, DDoS 공격의 경우 좀비 호스트를 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 검출 성능은 실험 결과를 통해 제시하였다.

하지만 7계층 응용 프로그램에 대한 DDoS 공격의 경우는 플로우 정보만을 이용하여 검출할 수 없는 단점을 가진다. 또한 정상적인 송신 주소를 사용하지 않고 거짓(spoofed) 송신 주소를 사용하는 경우에도 검출이 난해하다. 이러한 단점을 보완하여 폭주 DDoS 공격 뿐만 아니라 더 많은 공격에 대비한 검출 방법이 제시되어야 한다.

## 참고문헌

[1] Stephen D. Crocker, "Protecting the Internet From Distributed Denial-of-Service Attacks: A Proposal," in Proc. of the IEEE, Vol. 92, No. 9, pp. 1375-1381, Sep. 2004.

[2] Jelena Mirkovic and Peter 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.

[3] Shigang Chen and Qingguo Song, "Perimeter-Based Defense against High Bandwidth DDoS Attacks," in IEEE Trans. on Parallel and Distributed System, Vol. 16, No. 6, pp. 526-537, Jun. 2005.

[4] Ashley Chonka, Jaipal Singh, and Wanlei Zhou, "Chaos Theory Based Detection against Network Mimicking DDoS Attacks," in IEEE Communication Letters, Vol. 13, No. 9, pp. 717-719, Sep. 2009.

[5] Yi Xie and Shun-Zheng Yu, "Monitoring the Application-Layer DDoS Attacks for Popular Websites," in IEEE/ACM Trans. on Networking, Vol. 17, No. 1, pp. 15-25, Feb. 2009.

[6] João B. D. Cabrear, Lundy Lewis, Xinzhou Qin, Wenke Lee, Ravi K. Prasanth, B. Ravichandran, and Raman 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.

[7] Jian Yuan and Kevin 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.

[8] Jelena Mirkovic, Gregory Prier, and Peter L. Reiher, "Attacking DDoS at the Source," in Proc. of the 10th IEEE International Conference on Network Protocols, pp. 312-321, Nov. 2002.

[9] Haining Wang, Danlu Zhang, Kang G. Shin, "Detecting SYN Flooding Attacks", in Proc. of IEEE INFOCOM, vol. 3, pp. 1530-1539, Jun. 2002.

[10] Sanguk Noh, Cheolho Lee, Kyunghee Choi, and Gihyun Jung, "Detecting Distributed Denial of Service (DDoS) Attacks through Inductive Learning," in Lecture Notes in Computer Science, Vol. 2690, pp. 286-295, 2003.

[11] Supranamaya Ranjan, Ram Swaminathan, Mustafa Uysal, and Edward Knightly, "DDoS-Resilient Scheduling to Counter Application Layer Attacks under Imperfect Detection," in Proc. of IEEE INFOCOM, pp. 1-13, Apr. 2006.

[12] Thomas Karagiannis, Konstantina Papagiannaki, Michalis Faloutsos, "BLINC: Multilevel traffic classification in the dark," in ACM SIGCOMM, Vol. 35, pp. 229-240, Oct. 2005.