

공격자 네트워크 트래픽 분석을 통한 대규모 분산 서비스 거부 공격 특성 파악 (Analysis of Large-scale Distributed Denial-of-Service Traffic from an Attacker's Network)

서신석*, 원영준**, 홍원기***

* 포항공과대학교 컴퓨터공학과

** Internet Initiative Japan

*** 포항공과대학교 정보전자융합공학부

sesise@postech.ac.kr, young@ijlab.net, jwkhong@postech.ac.kr

요 약

2009년 7월 7.7 분산 서비스 거부 (Distributed Denial-of-Service - DDoS) 공격으로 불리는 일련의 대규모 DDoS 공격들이 미국과 한국의 정부 기관, 금융, 포털 사이트 등을 대상으로 발생하였다. 또한 2011년 3월에도 3.3 DDoS 공격으로 불리는 비슷한 공격이 시도되었다. 악의적인 목적으로 특정 서비스를 제공하는 서버의 자원을 고갈시켜 정상적인 서비스 제공을 어렵게 만드는 DDoS 공격은 방어하기가 매우 어렵고 심각한 피해를 주기 때문에 많은 DDoS 방어 기법들이 제안되어 왔다. 그럼에도 불구하고 DDoS 공격은 활발히 이루어지고 있으며 몇몇은 매우 성공적이어서 심각한 피해를 주고 있다. 본 논문은 기존의 방어 기법들 중에서 주류를 이루고 있는 표적 서버 측면에서의 방어 기법에 더하여 공격자 네트워크 측면에서의 방어 기법에 대한 필요성을 주장한다. 이를 위한 첫 단계로 포항공과대학교 캠퍼스 네트워크에서 7.7 DDoS 공격과 3.3 DDoS 공격 기간 동안 수집된 DDoS 공격 트래픽을 분석하여 DDoS 공격의 특성을 공격자 네트워크 측면에서 파악한다.

Keywords: DDoS, Monitoring, Traffic Analysis

1. 서론

분산 서비스 거부 (Distributed Denial of Service - DDoS) 공격은 다수의 좀비 PC를 활용하여 악의적으로 특정 서비스를 제공하는 서버의 자원을 고갈시켜 정상적인 서비스의 제공을 불가능하게 만드는 행위를 말한다. 좀비 PC란 악성코드에 감염되어 악성코드 제작자의 의도에 따라 명령을 수행하는 PC를 말한다. 수많은 좀비 PC들이 다수의 트래픽을 특정 서버에 지속적으로 보내면 표적이 되는 서버는 다운이 되거나 서비스 반응 속도가 현저히 느려지게 된다. 이러한 DDoS 공격은 그에 대한 방어 및 공격의 주체 파악이 매우 어려운 특징을 가지고 있다.

DDoS 공격의 피해는 매우 심각하기 때문에, DDoS 공격을 탐지 및 방어하기 위한 다양한 방법 [1-4]들이 제안 및 적용되고 있지만, 여전히 DDoS 공격을 완벽히 방어할 수 있는 방법은 존재하지 않는다. 현재 제안되고 있는 DDoS 공격 방어 기법들은 대부분 DDoS 공격의 표적이 되는 서버 바로 직전의 위치에서 트래픽을 점검 및 식별하여 악성 트래픽이 표적 서버로 전달되는 것을 방지하는 것에 중점을 두고 있다. 그러나 이러한 표적 서버 측면에서의 방어 기법들은 지속적으로 지능화되고 대규모화되는 DDoS 공격을

본 연구는 한국연구재단을 통해 교육과학기술부의 세계수준의 연구중심대학육성사업(WCU) (R31-10100)과 방송통신위원회의 "HiMang (Highly Manageable Network and Service Architecture for New Generation) 원천 연구" 원천기술개발사업의 연구결과로 수행되었음 (KCA-2011-10921-05003).

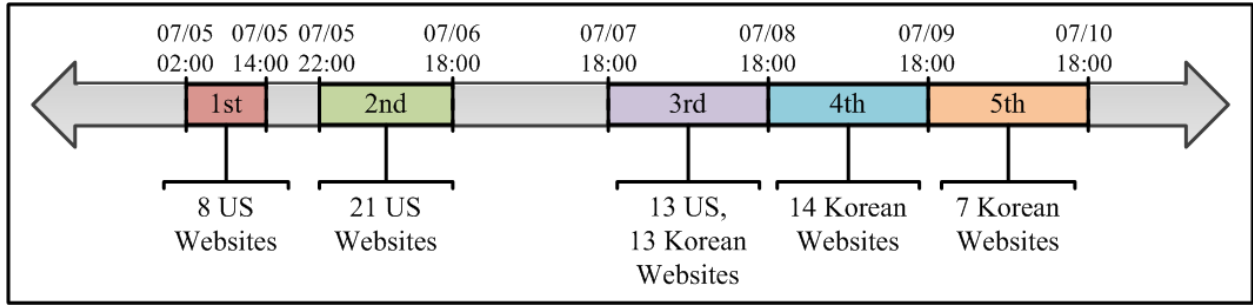


그림 1.7.7 DDoS 공격 양상

막기에는 역부족이며, 이것은 심각한 피해를 주었던 7.7 DDoS 공격이 잘 보여주고 있다 [5]. 따라서 DDoS 공격을 보다 효율적으로 방어하기 위해서는 DDoS 공격의 실질적 주체인 좀비 PC 들이 위치하고 있는 공격자 네트워크에서 DDoS 공격 트래픽을 원천적으로 차단할 수 있는 방안에 대한 연구도 동시에 진행되어야 한다 [6, 7]. 이를 위해서는 공격자 네트워크에서 측정할 수 있는 DDoS 공격 트래픽의 특성에 대한 이해가 필수적이다. 본 논문에서는 DDoS 공격 트래픽에 대한 분석을 통하여 공격자 네트워크 측면에서 DDoS 공격의 특성을 파악하고자 한다.

최근 한국에서 대규모 DDoS 공격이 2009 년 7 월과 2011 년 3 월에 발생하였다. 이들 공격의 주된 대상은 미국과 한국의 정부 기관, 금융, 포털 사이트 등 이었다. 우리는 이 두 DDoS 공격에 사용된 좀비 PC 가 포항공과대학교 캠퍼스 네트워크 내에도 다수 존재할 것이라고 가정하였다. 즉, 우리의 캠퍼스 네트워크를 DDoS 공격자 네트워크로 간주한 것이다. 이러한 가정에 기반하여, 우리는 공격자 네트워크 측면에서 DDoS 공격의 특성을 파악하기 위하여 DDoS 공격 기간 중에 트래픽을 수집하여 DDoS 공격이 없던 기간의 트래픽과 그 특성을 비교 및 분석하였다. 트래픽 분석은 패킷 개수, 플로우 개수, 트래픽 량, 프로토콜 비율, 연결 그래프, 플로우 지속 시간 분포, 평균 패킷 크기 분포를 이용하여 수행되었다.

2. 관련 연구

다양한 DDoS 공격 기법들 및 그에 대한 방어 기법들은 [8-10]에 잘 정리되어 있다. [8]은 DDoS 공격을 자동화 정도, 공격에 이용된 취약점, 공격 빈도, 공격의 영향력에 따라 분류하였다. 또한, DDoS 공격에 대한 방어 기법을 공격에 대응하는 시점에 따라 예방, 탐지, 경감, 응답의 네 가지로 구분하였고, 공격에 대응하는 위치에 따라 피해자 네트워크, 중간 네트워크, 공격자 네트워크로 구분하였다. [9]도 [8]과 비슷하게 DDoS 공격을 분류하였지만 보다 체계적이고 자세한 분류 방식을 제안했다. DDoS 공격의 방어 기법도 [8]에 제안된 것에 더하여 다른 네트워크와의 협력 정도를 새로운 분류 기준으로 제안했다. [10]은 DDoS 공격을 방어하는 기법들을 평가하기 위한 주요 지표로 방어 기법 적용 위치, 탐지 방식, 대응 방식, 보안성, 견고성을 제안했고 이들 기준에 따라 기준에 제안된 12 가지 DDoS 방지 기법들을 평가 및 비교하였다.

[11]은 DDoS 공격 트래픽을 웹 서비스의 이용자 측면에서 Quality of Service (QoS)를 고려하여 분석하였다. [12]는 직접적으로 수집된 DDoS 공격 트래픽과 Backscatter 분석을 통해 간접적으로 획득한 DDoS 공격 트래픽 등 다양한 DDoS 공격 트래픽에 대해서 심도 있는 분석을 보여준다. [13]은 인기 있는 웹 사이트들에 대한 응용 수준의 DDoS 공격에 대한 측정을 실시하고 주성분 분석을 통하여 DDoS 공격을 탐지하는 방법을 제안했다. 이러한 논문들은 공격의 표적이 되는 서버 측면에서의 트래픽 분석에 중점을 두고 있다. 그러나 본 논문은 좀비 PC 가 존재하는 공격자 네트워크의 트래픽에 대해 분석한다는 것이 기존 연구와의 큰 차이점이다.

3. 분석 대상 DDoS 공격 양상 및 특징

최근 두 번의 대규모 DDoS 공격이 한국에서 발생하였다. 하나는 2009 년 7 월에 발생한 7.7 DDoS 공격으로 7 월 5 일 02:00 부터 발생하여 7 월 10 일 18:00 까지 지속되었다 (그림 1). 다른 하나는 2011 년 3 월에 발생한 3.3 DDoS 공격으로 3 월 3 일 17:00 에 공격이 시작되었으며, 공격 종료 시점은 정해져 있지 않았다 (그림 2). 즉, 감염된 좀비 PC 들이 치료되기 전까지는 공격이 계속되었다. 이번 장에서는 이 두 대규모 DDoS 공격의 양상 변화 및 다른 DDoS 공격들과 차별화되는 여러 특징에 대해 소개한다.

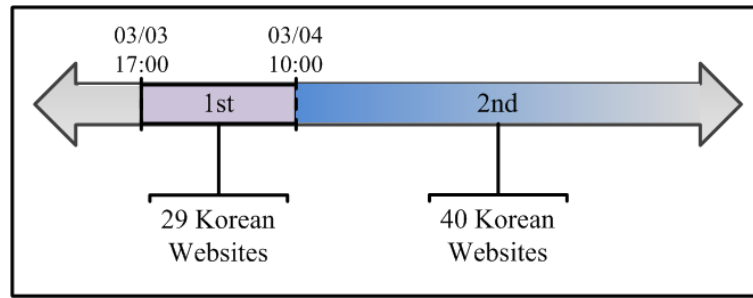


그림 2.3.3 DDoS 공격 양상

3.1.7.7 DDoS 공격

7.7 DDoS 공격은 2009년 7월 5일 02:00부터 7월 10일 18:00까지 총 5차례에 걸쳐 감행되었다(그림 1). 1차 DDoS 공격은 2009년 7월 5일 02:00부터 14:00까지 총 12시간에 걸쳐 미국의 8개 주요 웹사이트를 공격하는 것으로 시작되었다. 이 공격은 같은 날 22:00부터 다음 날인 7월 6일 18:00까지 21개의 미국 웹사이트를 공격하는 것으로 확대되었다(2차 공격). 이 두 차례의 공격들은 미국의 백악관을 비롯한 주요 정부기관과 야후, 아마존과 같은 상업적 용도의 웹사이트들을 대상으로 하고 있었다. 그러나 미국의 웹사이트들은 해당 기간 동안 DDoS 공격 트래픽의 대부분이 한국에서 흘러나오는 것을 파악하고 IP 주소가 한국에 속해있는 호스트로부터 전송되는 의심스러운 트래픽을 원천 차단함으로써 큰 피해는 입지 않았다.

제 3차 공격은 7월 7일 18:00을 기점으로 미국 13개 및 한국 13개의 웹 사이트들을 동시에 공격하는 양상으로 변화한다. 이 공격은 다음 날인 7월 8일 18:00까지 24시간 동안 지속되었으며 한국의 주요 정부기관, 금융, 인터넷 포털 사이트 등에 심각한 피해를 주어 일반적인 웹 서비스 제공이 불가능해졌다. 7월 8일 18:00부터는 그 공격 대상이 한국의 14개 웹 사이트로 변경되었으며, 7월 9일 18:00까지 24시간 동안 지속적으로 공격을 시도했다(4차 공격). 이 기간 동안의 주된 공격 대상은 국내 주요 금융 업체와 보안 업체의 웹 사이트들 이었다. 마지막으로 7월 9일 18:00부터 7월 10일 18:00까지 24시간 동안 5차 DDoS 공격이 국내 7개 웹 사이트에 대해 일어났다. 하지만 5차 DDoS 공격은 국내 정부 기관 및 보안 업체를 통해 사전에 파악되었고 그에 대한 대응 조치가 이루어졌기 때문에 심각한 피해를 주지는 못했다.

7.7 DDoS 공격에 동원된 좀비 PC 들은 해킹된 웹하드 사이트를 통해 감염된 것으로 추정되고 있다. 또한, 7.7 DDoS 공격은 다음에 기술하는 것과 같이 기존 DDoS 공격과는 다른 여러 특징을 가지고 있었다.

- **불명확한 공격 목적:** 기존의 DDoS 공격들은 금전적 혹은 정치적 목적을 가지고 특정 웹사이트를 공격하였지만, 7.7 DDoS 공격은 그 목적이 명확히 드러나지 않았다. 북한이 정치 및 군사적 목적으로 DDoS 공격을 감행했다는 추측은 있었지만 아직까지 명확한 공격 목적은 밝혀지지 않고 있다.
- **여러 서버에 대한 동시 공격:** 특정 웹 사이트에만 국한되었던 기존의 DDoS 공격들과는 달리 7.7 DDoS 공격은 미국 및 한국의 주요 정부 기관, 금융 기관, 포털 사이트 등을 포함하여 매우 광범위한 대상에 대한 공격이 이루어졌다.
- **자율 공격:** 기존 DDoS 공격에 사용된 좀비 PC 들은 Command and Control (C&C) 서버의 명령을 받아 공격을 실행하였다. 따라서 C&C 서버를 찾아내어 그 기능을 정지시키면 전체 DDoS 공격을 막을 수 있었다. 하지만 7.7 DDoS 공격은 각각의 좀비 PC 에 탑재된 악성코드 자체에 공격 대상 및 시간이 정해져 있어 C&C 서버의 명령 없이 스스로 공격을 수행하였다. 이러한 특성은 7.7 DDoS 공격에 대한 방어를 보다 어렵게 만들었다.
- **좀비 PC 손상:** 7.7 DDoS 공격에 이용된 악성코드는 좀비 PC 에 존재하는 중요한 문서 파일들을 삭제하고 하드 디스크 드라이브를 소프트웨어적으로 파괴하는 명령을 탑재하고 있었다. 이것은 증거를 남기지 않으려는 의도로 추정되고 있다.
- **대규모 좀비 PC 동원:** 정부 및 보안 회사들의 보고서에 따르면 7.7 DDoS 공격에 동원된 좀비 PC 는 78,000 대에서 200,000 대에 달할 것으로 추정되고 있으며 그 중 대부분은 한국에 속한 IP 대역을 가지고 있었다. 이렇게 많은 수의 좀비 PC 는 기존 DDoS 공격들에서 그 유례를 찾아보기 힘들 정도이다.

- **저 용량 공격:** 7.7 DDoS 공격에서 하나의 좀비 PC가 발생시켰던 총 트래픽은 54.2 Kbps 이고 각 웹 사이트로 향했던 공격 트래픽은 1.0 ~ 25.3 Kbps 수준이었다. 이렇게 낮은 수준의 DDoS 공격 트래픽은 기존의 DDoS 방어 시스템이 탐지하기 매우 어려웠다.
- **복합 공격:** 다양한 DDoS 공격 방법 중 한 가지 방법만 이용하여 공격을 시도한 것이 아니라 TCP Syn Flooding, UDP 80 Flooding, ICMP Flooding, HTTP Get/POST Flooding 공격을 복합적으로 시도하여 서버의 자원뿐만 아니라 네트워크의 대역폭도 고갈 시켜 DDoS 공격에 대한 방어를 더욱 어렵게 만들었다.

3.2. 3.3 DDoS 공격

3.3 DDoS 공격은 두 단계에 걸쳐 이루어졌다 (그림 2). 첫 번째 공격은 2011년 3월 3일 17:00에 시작되었고 29개의 한국 웹사이트들을 공격하였다. 두 번째 공격은 3월 4일 10:00에 시작되었으며 40개의 한국 웹사이트들을 공격하였다. 3.3 DDoS 공격의 대상 웹사이트들은 7.7 DDoS 공격의 대상과 비슷하였다. 공격에 동원된 예상 좀비 PC의 수는 약 50,000여 대로 7.7 DDoS 공격에 동원되었을 것으로 추정되는 좀비 PC의 수보다는 적었다.

3.3 DDoS 공격은 정부 및 보안 회사들의 신속한 대응으로 7.7 DDoS 공격만큼 성공적이지는 않았지만 다음과 같은 측면에서 7.7 DDoS 공격과 매우 유사한 특징을 보였다.

- 웹하드 사이트를 통한 좀비 PC 감염
- 불명확한 공격 목적
- 여러 서버에 대한 동시 공격
- 자율 공격
- 좀비 PC 손상
- 저 용량 공격
- 복합 공격

3.3 DDoS 공격과 7.7 DDoS 공격의 차이점은 다음과 같다. 첫째, 7.7 DDoS 공격과는 달리 3.3 DDoS 공격에는 C&C 서버가 사용되었다. 그러나 3.3 DDoS 공격에서 C&C 서버의 역할은 일반적인 경우와는 달랐다. 일반적으로 C&C 서버의 역할은 DDoS 공격의 시작과 끝을 명령하는데 있지만, 3.3 DDoS 공격에 사용된 C&C 서버는 감염된 좀비 PC들에 추가적인 악성 프로그램 코드를 전송하는 역할을 하였다. 둘째, 3.3 DDoS 공격에 이용된 악성코드는 컴퓨터 바이러스 백신의 업데이트를 방지하기 위하여 윈도우 기반 운영체제의 시스템 파일인 “hosts” 파일을 변경하였다. 7.7 DDoS 공격은 동일한 목적을 위하여 컴퓨터 바이러스 백신의 업데이트 서버를 공격하였다. 셋째, 공격 대상 서버의 목록 및 감염된 좀비 PC들과 C&C 서버들 간의 통신이 암호화되어 있었다. 이것은 3.3 DDoS 공격에 대한 분석을 매우 어렵게 만들었다. 넷째, 공격의 종료 시점이 정해지지 않았다. 즉, 3.3 DDoS 공격에 사용된 좀비 PC들은 치료되기 전까지 공격 패킷을 지속적으로 목표 웹사이트에 보냈다.

4. 트래픽 분석

본 연구에서는 7.7 및 3.3 DDoS 공격에 사용된 좀비 PC가 포항공과대학교 캠퍼스 내에도 다수 존재할 것이라는 가정 하에 포항공과대학교 캠퍼스 네트워크에서 외부 인터넷과 연결되는 지점을 통과하는 트래픽을 수집하였다. 즉, 포항공과대학교 캠퍼스 네트워크를 DDoS 공격자 네트워크로 본 것이다. 포항공과대학교 네트워크는 2개의 1-Gbps 이더넷 링크를 통해 외부 인터넷과 연결되어 있으며 본 논문에서 사용된 트래픽 트레이스는 그 중 하나의 링크에 물린 엠티컬 탭을 통해 수집되었다. 트래픽은 2009년 3월 31일 (7.7 DDoS 공격 발생 전), 7월 8일 및 9일 (7.7 DDoS 공격 중), 8월 12일 (7.7 DDoS 공격 발생 후), 2011년 3월 4일 (3.3 DDoS 공격 중), 3월 14일 (3.3 DDoS 공격 발생 후)에 17:00부터 한 시간 동안 수집하였다.

수집된 트래픽은 우선 CoralReef [14]를 이용하여 플로우 형태로 변환하였다. 하나의 플로우는 마지막 패킷이 전송된 후 300초 동안 추가적인 패킷의 전송이 없으면 종료되는 것으로 간주하였다. 또한, 인터넷 트래픽의 대부분을 차지하고 있는 TCP, UDP, ICMP 프로토콜에 대해서만 플로우를 생성하였다.

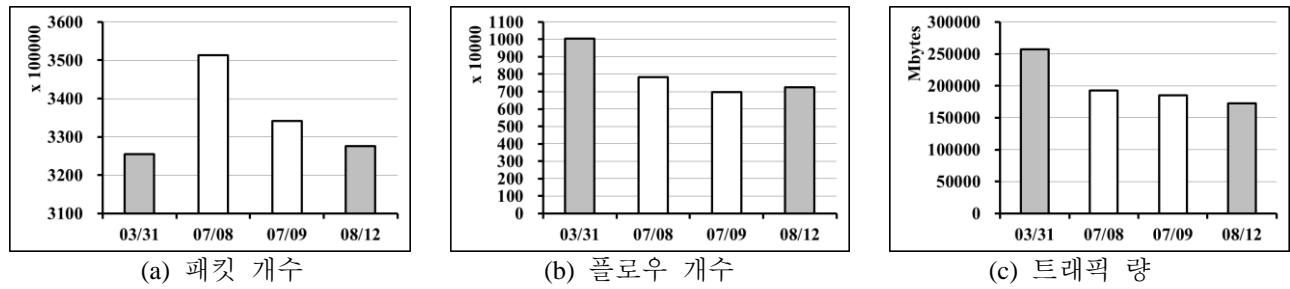


그림 3. 2009 년 전체 트래픽에 대한 패킷 개수, 플로우 개수, 트래픽 량
(채워진 막대: DDoS 공격 없는 기간, 빈 막대: DDoS 공격 기간)

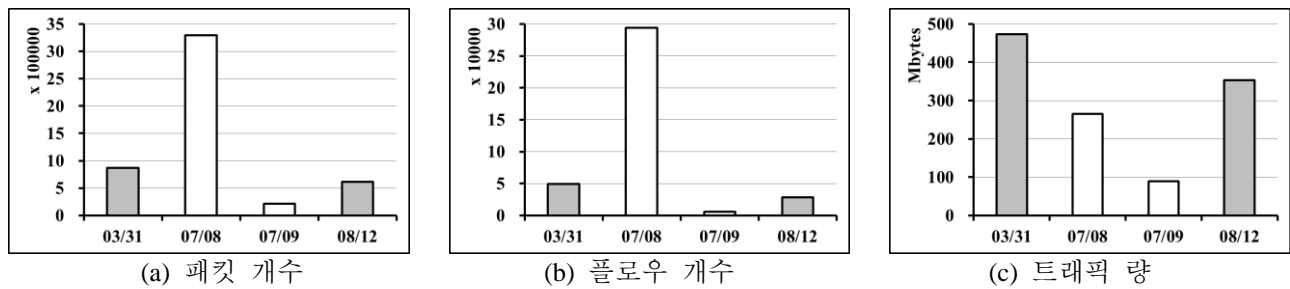


그림 4. 2009 년 의심스러운 트래픽에 대한 패킷 개수, 플로우 개수, 트래픽 량
(채워진 막대: DDoS 공격 없는 기간, 빈 막대: DDoS 공격 기간)

4.1. 패킷 개수, 플로우 개수, 트래픽 량

그림 3 은 2009 년에 17:00 부터 한 시간 동안 수집된 포항공과대학교 캠퍼스 네트워크 전체 트래픽의 패킷 개수, 플로우 개수 및 트래픽 량을 나타낸다. 그래프에서 보는 것과 같이 DDoS 공격이 있던 기간에는 DDoS 공격이 없던 기간에 비해 전송되는 패킷의 개수는 많았으나 플로우의 개수와 전체 트래픽 량은 더 적었던 것을 알 수 있다. 그러나 이러한 특징은 통계적으로 커다란 의미를 부여하기에는 무리가 있는 수준이다. 이것은 7.7 DDoS 공격에 사용된 좀비 PC 들이 저용량 공격을 시도했고 포항공과대학교 캠퍼스 네트워크의 전체적인 트래픽에 큰 영향을 미치지 않았다는 것을 의미한다.

이와는 반대로 그림 4 는 DDoS 공격이 없던 기간과 DDoS 공격이 발생했던 기간 사이에 큰 차이를 보이고 있다. 그림 4 는 포항공과대학교 캠퍼스 내에 존재했던 좀비 PC 로 의심되는 호스트의 트래픽에 대해서만 패킷 개수, 플로우 개수, 트래픽 량을 나타낸 것이다. 본 논문에서는 DDoS 공격이 발생했던 기간 동안 DDoS 공격의 표적이 되었던 웹 사이트에 접속한 포항공과대학교 내의 호스트를 좀비 PC 로 간주했다. DDoS 공격이 가장 심했던 7 월 8 일에는 패킷 및 플로우의 개수가 다른 기간에 비해 월등히 많은 것을 알 수 있다. 그에 비해 전송된 총 트래픽 량은 DDoS 공격이 없던 기간보다 낮은 수준을 보인다. 이것은 좀비로 의심되는 PC 들이 표적 웹 사이트들에 의미 있는 데이터를 포함하지 않는 DDoS 공격 패킷을 전송했기 때문이다. 한 가지 더 주목할만한 사항은 마찬가지로 DDoS 공격이 발생했던 7 월 9 일에는 패킷 개수, 플로우 개수, 트래픽 량이 나머지 경우에 비해 현저히 낮은 수준을 보였다는 것이다. 이것은 많은 수의 좀비 PC 들에 탑재된 악성 코드가 치료되어 더 이상 DDoS 공격을 시도하지 않게 되었으나 표적 웹 사이트들은 여전히 서비스가 정상화되지 않아 정상적인 트래픽이 발생하지 않은 것으로 해석할 수 있다.

동일한 분석을 2011 년의 트래픽 트레이스들에 대해서도 수행하였지만, DDoS 공격이 있는 트래픽과 DDoS 공격이 없는 트래픽 사이에는 큰 차이가 존재하지 않았다. 다만 3 월 4 일의 트래픽은 3 월 14 일보다 약간 낮은 수준의 패킷 개수, 플로우 개수, 트래픽 량을 보였다. 이러한 경향은 주간 인터넷 사용 패턴의 변화에 따른 것으로 보인다. 즉, 금요일이었던 3 월 4 일에 월요일이었던 3 월 14 일보다 표적이 되었던 웹 사이트들에 대한 접속을 적게 했던 것이다. 이러한 결과를 보았을 때, 3.3 DDoS 공격은 포항공과대학교 캠퍼스 네트워크 트래픽에 큰 영향을 주지 않았다는 것을 알 수 있다.

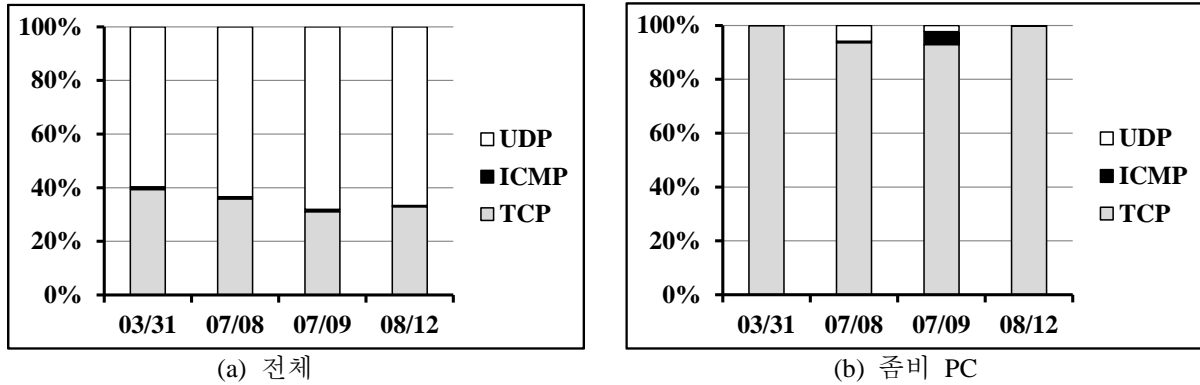


그림 5. 2009 년 트래픽에 대한 TCP, ICMP, UDP 프로토콜 비율

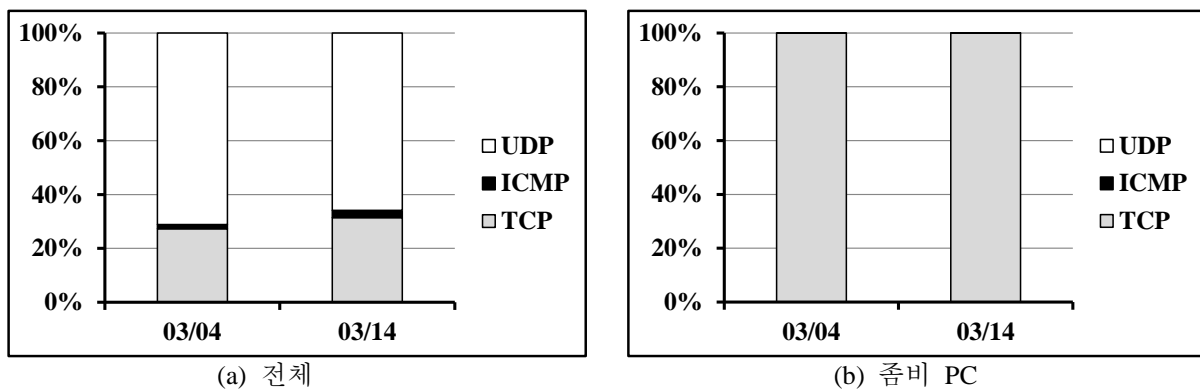


그림 6. 2011 년 트래픽에 대한 TCP, ICMP, UDP 프로토콜 비율

4.2. 프로토콜 비율

그림 5 는 2009 년 트래픽들의 TCP, ICMP, UDP 프로토콜의 비율을 나타낸다. 그림 5a 의 전체 트래픽에서의 각 프로토콜 비율은 DDoS 공격이 없을 때와 DDoS 공격이 있을 때 간에 의미 있는 차이가 보이지 않는다. UDP 가 60% 이상을 차지하고 있으며, TCP 가 30~40% 정도를 차지하고, 나머지를 ICMP 가 차지하고 있다. 그러나 그림 5b 에서 좀비 PC 로 의심되는 호스트들의 트래픽만을 보았을 때는 그 차이가 나타난다. 우선 DDoS 공격이 없던 기간에는 TCP 가 트래픽의 대부분을 차지하고 있는 것을 볼 수 있다. 이것은 7.7 DDoS 공격의 표적이 TCP 위에서 동작하는 HTTP 를 사용하는 웹 사이트들이었기 때문이다. 하지만 DDoS 공격이 있었던 7 월 8 일과 7 월 9 일에는 ICMP 와 UDP 트래픽이 존재했다. 이것은 7.7 DDoS 공격이 HTTP, ICMP, UDP 등을 복합적으로 활용했기 때문이다.

그림 6 에 나타낸 2011 년 트래픽들의 프로토콜 비율을 보면 3 월 4 일과 14 일 모두 2009 년의 DDoS 공격이 없던 때와 거의 동일한 패턴을 보이는 것을 알 수 있다. 즉, 그림 6a 의 전체 트래픽을 보면 UDP 가 60% 이상을 차지하고 있으며, TCP 가 30~40% 정도를 차지하고, 나머지를 ICMP 가 차지하고 있으며 그림 6b 의 좀비 PC 의 트래픽을 보면 거의 100%가 TCP 이었음을 알 수 있다. 이것은 3.3 DDoS 공격 동안에는 포항공과대학교 캠퍼스 네트워크 내에 좀비 PC 가 많지 않아 그 영향도가 적었던 것으로 해석할 수 있다.

그림 3-6 의 결과를 종합해 보았을 때 저 용량 공격을 시도하는 DDoS 공격을 공격자 네트워크에서 탐지하기 위해서는 네트워크 내의 전체 트래픽에 대한 분석은 큰 효과를 보이기 어렵다는 결론을 내릴 수 있다. 따라서 DDoS 공격을 공격자 네트워크에서 효율적으로 방어하기 위해서는 공격의 표적이 될만한 주요 웹 사이트별 트래픽 모니터링이 필요하다는 것을 알 수 있다. 이 결론에 따라서 이후의 분석들은 좀비로 의심되는 PC 에서 발생된 트래픽만을 이용하여 수행되었다.

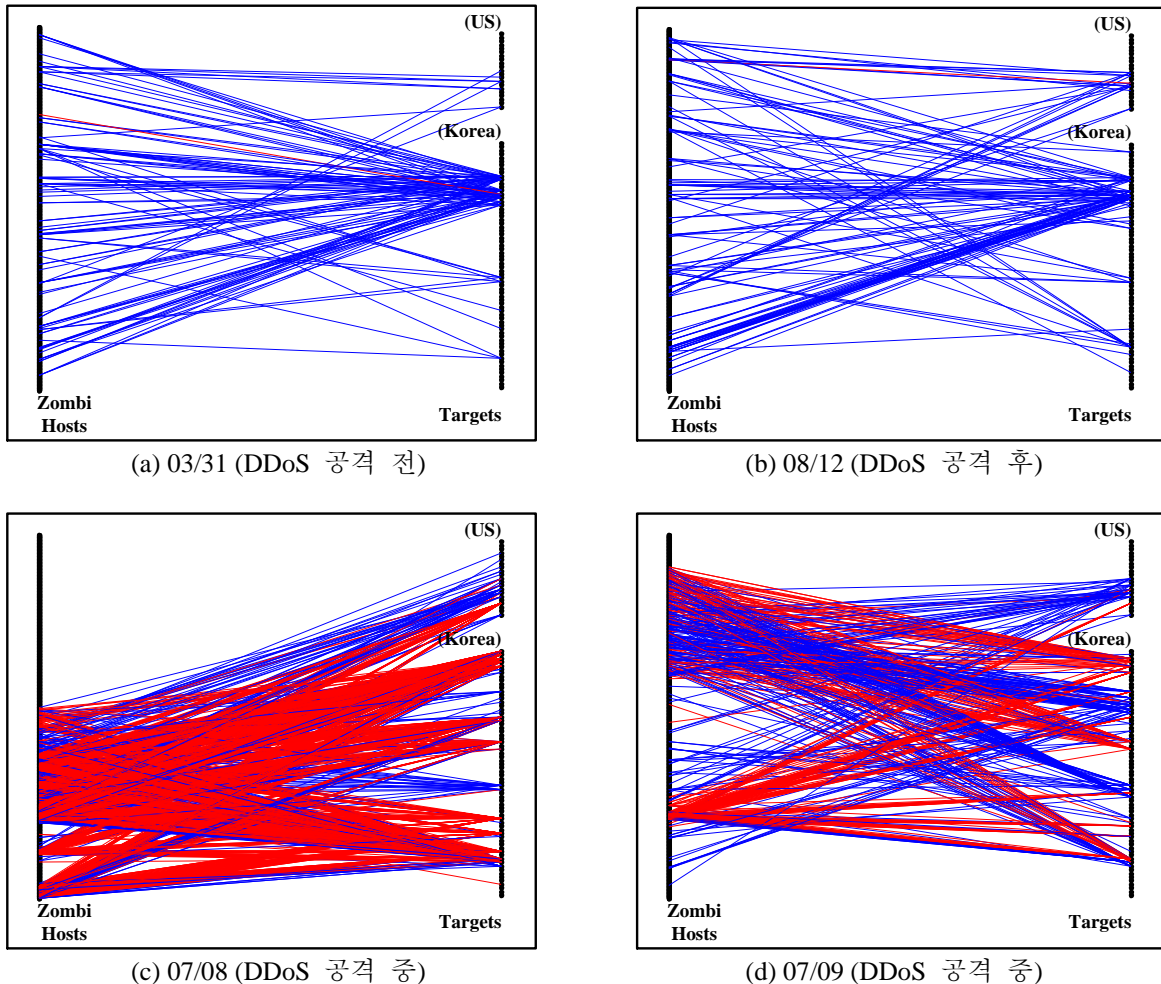


그림 7. 2009년 트래픽에 대한 연결 그래프

4.3. 연결 그래프

그림 7은 17:00부터 한 시간 동안 포항공과대학교 내의 2011년 7.7 DDoS 공격에 사용된 좀비 PC로 의심되는 호스트와 7.7 DDoS 공격의 표적이 되었던 웹 사이트들 간의 연결 그래프를 나타낸다. 표적이 되는 웹 사이트들은 미국과 국내로 구분하여 표시했다. 평균 패킷의 크기가 64 bytes 이하인 두 호스트 간의 연결은 빨간색으로 표시했고 그 이상인 연결은 파란색으로 표시했다. 64 bytes는 하나의 패킷이 가질 수 있는 최소의 데이터 크기인 46 bytes에 12 bytes의 여분을 둔 것이다.

이 연결 그래프들을 보면 DDoS 공격이 없던 기간과 DDoS 공격이 있던 기간 사이에 확실한 차이를 보이는 것을 알 수 있다. 우선 3월 31일과 8월 12일의 연결 그래프(그림 7a, b)를 보면 평균 패킷 크기가 64 bytes를 넘는 연결이 대다수를 차지하여 파란색으로 표시되고 있다. 또한, 대부분의 연결들은 몇몇의 특정 웹 사이트들에 집중되어 있는 것을 알 수 있다.

하지만 DDoS 공격이 있었던 7월 8일과 9일의 그래프(그림 7c, d)를 보면 많은 수의 연결들이 64 bytes 이하의 평균 패킷 크기를 가지고 있어 빨간색으로 표시되었다. 또한, 연결들이 몇몇의 특정 웹 사이트에 집중되어 있지 않고 분산되어 있다. 한 가지 특이한 사항은 7월 8일의 연결 그래프에서 포항공대 내의 좀비 PC로 의심되는 호스트들 중 상단에 위치한 호스트들에서 발생한 트래픽이 전혀 없다는 것이다. 이것은 DDoS 공격이 없었던 3월 31일 및 8월 12일뿐만 아니라 DDoS 공격이 있었던 7월 9일과도 현격히 다른 결과이다. 이러한 현상은 우리가 가지고 있는 한 시간 단위의 전체 트래픽 트레이스 중에서 7월 8일 17:00과 18:00의 트래픽에서만 관측되고 있다. 이것은 해당 기간 동안 트래픽이 존재하지 않던 호스트들을 담당하던 스위치에 문제가 발생했기 때문으로 추정된다.

그림 8은 2011년 트래픽에 대한 연결 그래프이다. 두 그래프는 DDoS 공격 여부에 관계없이 동일한 패턴을 보이고 있으며, 2009년의 DDoS 공격이 없던 때의 그래프(그림 7a, b)와 매우 유사함을 알 수 있다. 즉, 대부분의 연결이 특정 웹사이트들에 집중되어 있으며 평균 패킷 크기가 64 bytes보다 크다.

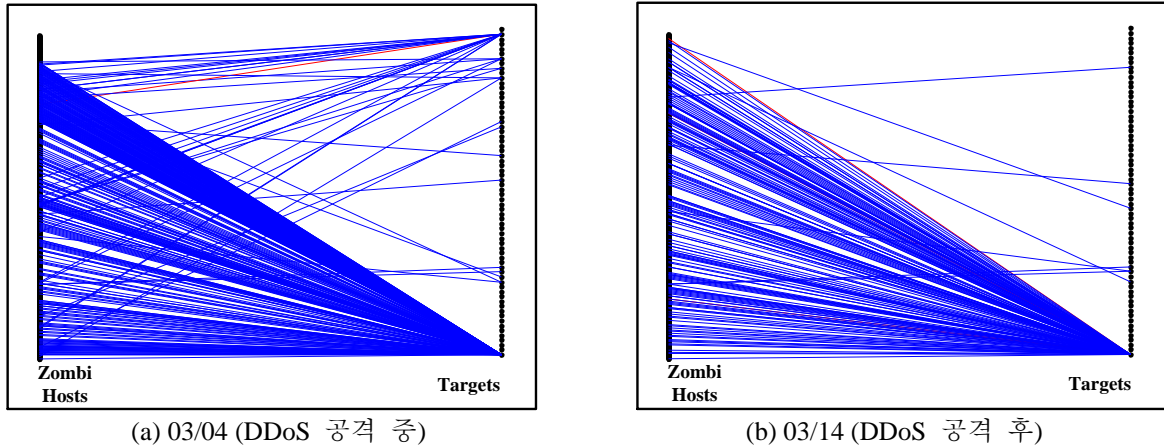


그림 8. 2011 년 트래픽에 대한 연결 그래프

4.4. 플로우 지속 시간 분포

그림 9 는 좀비 PC 로 의심되는 호스트의 17:00 부터 한 시간 동안의 플로우 지속 시간에 대한 CDF 그래프이다. 2009 년의 그래프를 보면 DDoS 공격이 없었던 3 월 31 일과 8 월 12 일의 그래프는 거의 동일한 형태를 취하는 반면 DDoS 공격이 있었던 7 월 8 일과 9 일의 그래프는 다른 분포를 보이고 있다. DDoS 공격이 없던 기간에는 플로우 지속 시간이 0.01 초 이하인 플로우가 거의 존재하지 않았으나 DDoS 공격이 있던 기간에는 이러한 플로우가 10% 정도 존재했다. 이것은 좀비 PC 로 의심되는 호스트가 표적이 되는 웹 사이트들에 대해 단발성 공격 패킷을 간헐적으로 보내는 형태의 공격을 포함하고 있음을 의미한다. DDoS 공격이 없던 기간에 비해 DDoS 공격이 있을 당시에는 지속 시간이 10 초 이상인 플로우의 비율이 더 높았다는 것도 주목할만한 사항이다. 이것은 좀비 PC 로 의심되는 호스트가 표적이 되는 웹 사이트들에 대해 10 초 이상 지속적으로 공격 패킷을 보냈음을 의미한다. 위 두 가지 분석 결과를 종합해 보면 7.7 DDoS 공격은 여러 웹 사이트들에 대해서 매우 짧은 시간 동안 공격 패킷을 전송하는 것과 한 웹 사이트에 대해 지속적으로 공격 패킷을 전송하는 것의 두 가지 형태의 공격을 복합적으로 시도했음을 알 수 있다.

2011 년의 플로우 지속 시간 CDF 들은 거의 동일한 형태를 띄고 있으며, 그 특징이 2009 년의 DDoS 가 없던 때의 플로우 지속 시간 CDF 들과 거의 비슷하다는 것을 알 수 있다.

4.5. 평균 패킷 크기 분포

그림 10 은 좀비 PC 로 의심되는 호스트의 17:00 부터 한 시간 동안의 평균 패킷 크기에 대한 CDF 그래프이다. 2009 년의 그래프들을 보면, DDoS 공격이 있었을 때 (7 월 8, 9 일) 의 평균 패킷 크기가 DDoS 공격이 없었을 때 (3 월 31 일, 8 월 12 일) 보다 작은 것을 알 수 있다. 이러한 경향은 7 월 9 일보다 8 일에

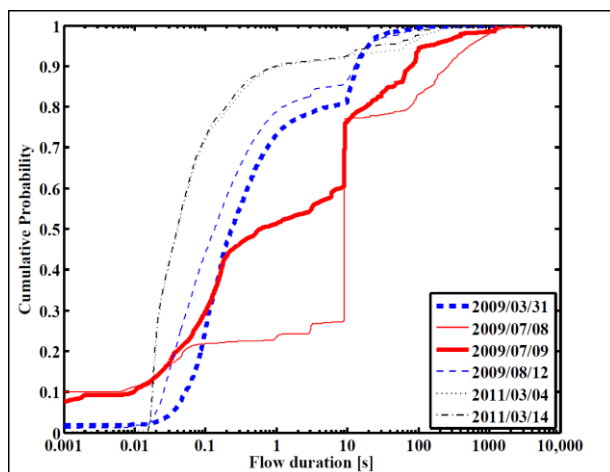


그림 9. 플로우 지속 시간 CDF

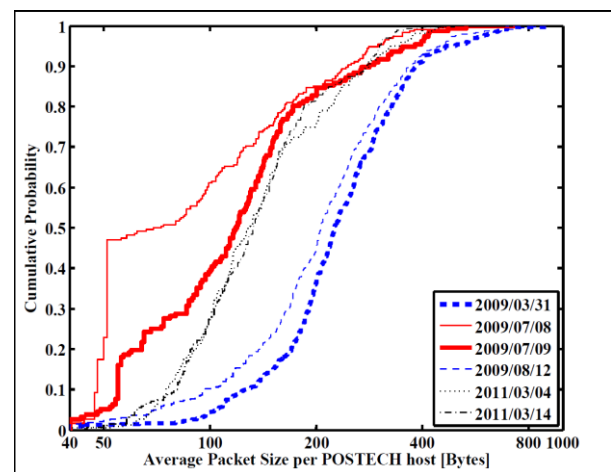


그림 10. 평균 패킷 크기 CDF

보다 뚜렷이 나타나는데, 이것은 7 월 8 일에 DDoS 공격이 더 강력했기 때문이다. 또한, 2011 년의 그래프들은 거의 유사한 것을 알 수 있다. 따라서, 이제까지의 2011 년도 트래픽에 대한 분석 결과를 종합해 보면 3.3 DDoS 공격 당시에는 포항공과대학교 캠퍼스 네트워크 내에 좀비 PC 가 거의 존재하지 않았다는 결론을 내릴 수 있다.

5. 결론 및 향후 과제

DDoS 공격을 방어하기 위한 많은 방법들이 제안되었고 적용되고 있지만, 성공적이었던 7.7 DDoS 공격은 기존 방법들의 한계점을 명확히 드러내었다. 본 논문에서는 표적이 되는 서버 측에서 DDoS 공격을 방어하려는 기존의 주된 DDoS 공격 방어 방법에 더하여 DDoS 공격의 주체가 되는 좀비 PC 를 가지고 있는 공격자 네트워크 측면에서의 사전 방어 기법의 필요성을 주장하였다. 이를 위해서는 공격자 네트워크에서 측정할 수 있는 DDoS 공격 트래픽의 특성에 대한 이해가 필수적이다.

본 논문에서는 포항공과대학교 캠퍼스 네트워크에서 7.7 및 3.3 DDoS 공격이 있을 당시의 트래픽을 수집하여 패킷 개수, 플로우 개수, 트래픽 량, 프로토콜 비율, 연결 그래프, 플로우 지속 시간 분포, 평균 패킷 크기 분포를 이용하여 분석했다. 그 결과 공격자 네트워크에서 DDoS 공격을 효율적으로 탐지하기 위해서는 네트워크 내의 전체 트래픽에 대한 분석은 큰 효과를 보기 어렵고 DDoS 공격의 표적이 될만한 주요 웹 사이트별 분석이 필요하다는 결론을 얻을 수 있었다. 또한, 연결 그래프와 플로우 지속 시간 CDF 그래프를 이용하여 DDoS 공격의 특성 및 변화 양상을 쉽게 파악할 수 있었다. 향후 연구로 우리는 이러한 분석 결과를 바탕으로 공격자 네트워크에서 효율적으로 DDoS 공격의 징후를 탐지할 수 있는 기법에 대한 연구를 진행할 계획이다.

6. 참고 문헌

- [1] G. Zhang and M. Parashar, "Cooperative mechanism against DDoS attacks," in *Proc. IEEE International Conference on Information and Computer Science (ICICS '04)*, Malaga, Spain, Oct. 27–29, 2004.
- [2] S. S. Kim and A. L. N. Reddy, "Statistical techniques for detecting traffic anomalies through packet header data," *IEEE/ACM Transactions on Networking*, vol. 16, no. 3, pp. 562–575, Jun. 2008.
- [3] R. K. C. Chang, "Defending against flooding-based Distributed Denial-of-Service attacks: A tutorial," *IEEE Communications Magazine*, vol. 40, no. 10, pp. 42–51, Oct. 2002.
- [4] X. Yang, D. Wetherall, and T. Anderson, "TVA: A DoS-limiting network architecture," *IEEE/ACM Transactions on Networking*, vol. 16, no. 6, pp. 1267–1280, Dec. 2008.
- [5] "Large-scale DDoS attacks in the United States and South Korea," White Paper, Internet Initiative Japan Inc., Nov. 16, 2009.
- [6] J. Mirkovic, G. Prier, and P. Reiher, "Attacking DDoS at the source," in *Proc. IEEE 10th International Conference on Network Protocols (ICNP '02)*, Paris, France, Nov. 12–15, 2002, pp. 312–321.
- [7] S. Malliga, A. Tamilarasi, and M. Janani, "Filtering spoofed traffic at source end for defending against DoS / DDoS attacks," in *Proc. IEEE 17th International Conference on Computer, Communication and Networks (ICCCN '08)*, St. Thomas, Virgin Islands, USA, Aug. 3–7, 2008, pp. 1–5.
- [8] C. Douligeris and A. Mitrokotsa, "DDoS attacks and defense mechanisms: classification and state-of-the-art," *Computer Networks*, vol. 44, no. 5, pp. 643–666, Apr. 2004.
- [9] J. Mirkovic and P. Reiher, "A taxonomy of DDoS attack and DDoS defense mechanisms," *ACM SIGCOMM Computer Communication Review*, vol. 34, no. 2, pp. 39–53, Apr. 2004.
- [10] M. Sachdeva, G. Singh, K. Kumar, and K. Singh, "A comprehensive survey of distributed defense techniques against DDoS attacks," *International Journal of Computer Science and Network Security*, vol. 9, no. 12, pp. 7–15, Dec. 2009.
- [11] J. Mirkovic, P. Reiher, S. Fahmy, R. Thomas, A. Hussain, S. Schwab, and C. Ko, "Measuring denial of service," in *Proc. ACM 2nd Workshop on Quality of Protection (QoP '06)*, Alexandria, VA, USA, Oct. 30, 2006, pp. 53–58.
- [12] Z. M. Mao, V. Sekar, O. Spatscheck, J. van der Merwe, and R. Vasudevan, "Analyzing large DDoS attacks using multiple data sources," in *Proc. ACM SIGCOMM Workshop on Large-scale Attack Defense (LSAD '06)*, Pisa, Italy, Sep. 11, 2006, pp. 161–168.
- [13] Y. Xie and S.-Z. Yu, "Monitoring the application-layer DDoS attacks for popular websites," *IEEE/ACM Transactions on Networking*, vol. 17, no. 1, pp. 15–25, Feb. 2009.
- [14] CoralReef. [Online]. Available: <http://www.caida.org/tools/measurement/coralreef/>



서 신 석

2008 인하대학교, 컴퓨터공학과 학사
2008~현재 포항공과대학교, 컴퓨터공학과 통합 과정
<관심분야> 자율 컴퓨팅, 상황정보 관리



원 영 준

2003 Univ. of Waterloo, B. Math in Computer Science
2004~2006 포항공과대학교, 컴퓨터공학과 석사
2006~2010 포항공과대학교, 컴퓨터공학과 박사
2010~2011 INRIA, France, Postdoctoral Researcher
2011~2012 IJ Research, Japan, Researcher

2012~현재 한양대학교 정보시스템학과 조교수
<관심분야> 인터넷 트래픽 모니터링 및 분석, 네트워크 운용 및 시스템 관리



홍 원 기

1983 Univ. of Western Ontario, BSc in Computer Science
1985 Univ. of Western Ontario, MS in Computer Science
1985~1986 Univ. of Western Ontario, Lecturer
1986~1991 Univ. of Waterloo, PhD in Computer Science
1991~1992 Univ. of Waterloo, Post-Doc Fellow

1992~1995 Univ. of Western Ontario, 연구교수
1995~현재 포항공과대학교 컴퓨터공학과 교수
2007~2011 포항공과대학교 정보통신대학원장
2007~2010 포항공과대학교 정보통신연구소 연구소장
2008~2010 포항공과대학교 컴퓨터공학과 주임교수
2008~현재 포항공과대학교 정보전자융합공학부장
<관심분야> 네트워크 트래픽 모니터링, 네트워크 및 시스템 관리