인터넷 AS 레벨 토폴로지에서 분산서비스거부 공격 징후 탐지

(Detection of the Portent of Distributed DoS Attacks on the Internet AS-level Topology)

강 구 홍 † 이 희 만 †† 김 익 균 ††† 오 진 태 ††† 장 종 수 †††
(Koohong Kang) (Heeman Lee) (Ikkyun Kim) (Jintae Oh) (Jong Soo Jang)

요 약 각각의 AS 레벨에서 정확한 연결구조를 얻기 위해 들이는 노력에도 불구하고 이들 AS 레벨 인터넷 토폴로지를 이용한 응용 연구들이 매우 드물다. 본 논문에서는 UCLA IRL 연구실이 제공하는 데이터를 이용해 AS 노드의 하위 스트림 AS 분포의 power-laws 특징과 인터넷 라우팅 패스 구조에 가장 중요한 역할을 하는 AS 링크 분포를 살펴 보았다. 또한, 한국과 미국 사이트를 중심으로 (발신지-목적지) 라우팅 홉 수 분포를 조사하고 이들 분포와 BGP 밸리-프리 라우팅 정책 특징을 이용하여 분산서비스거부(DDoS) 공격 시 예상되는 인터넷 트래픽 임의성(randomness)을 근거로 DDoS 공격 징후를 인터넷 AS 레벨에서 발견하는 방법을 제시하였다.

키워드 : AS-레벨 토폴로지, 분산서비스거부 공격, 트래픽 임의성

Abstract Despite lots of efforts to obtain an accurate picture of structure at the level of individual ASes, there is a few application works using the AS-level Internet topology. In this paper, we show that the power-law fits the number of down-stream customer ASes very well and also present the distributions of AS links with the "public view" from UCLA IRL laboratory. Moreover, we obtain the distributions of source-destination pairs of routing hops for two sites in Korea and the United States, and then we propose a new method to decide the randomness of Internet traffic using the obtained distributions and the BGP valley-free routing policy. The randomness of traffic must be a portent of outbreak of the distributed denial-of-service attacks.

Key words : AS-level topology, DDoS (Distributed Denial of Service), Traffic Randomness

† 정 회 원 : 서원대학교 정보통신공학과 교수
khkang@seowon.ac.kr
†† 종신회원 : 서원대학교 멀티미디어공학과 교수
hlee@seowon.ac.kr
††† 정 회 원 : ETRI 지식정보보안연구부 책임연구원
ikkim21@etri.re.kr
showme@etri.re.kr
jsjang@etri.re.kr
논문접수 : 2009년 11월 24일
심사완료 : 2010년 6월 16일

정보과학회논문지 : 정보통신 제37권 제5호(2010.10)

1. 서 론

1.1 연구 배경

컴퓨터의 대중화와 정보화 사회의 도래와 함께 인터넷의 속도와 복잡도는 놀라운 속도로 증가하고 있다. 인터넷은 다양한 네트워크 및 인터넷 서비스 제공자(NSP, ISP: Network(or Internet) Service Provider)에 의해 관리되고 운영되는 수 천 개의 AS(Autonomous System)로 연결되어 있으며 BGP(Border Gateway Protocol) 라우팅 프로토콜에 의해 이들 AS 간 라우팅 패스가 결정된다[1]. 따라서 인터넷은 각 AS가 노드, 그리고 두 AS 사이 BGP 피어링(peering)이 링크로 표현된 하나의 AS 레벨 토폴로지 그래프로 나타낼 수 있다[2]. 지 난 수 년 간 많은 사람들은 인터넷이 어떤 형태로 상호 연결되어 있으며 어떤 토폴로지 특성을 갖고 있는지에 관한 연구를 진행해 오고 있다[1-6]. 이러한 AS 레벨 토폴로지 연구는 인터넷 운영과 인터넷 기술 연구

에 있어 매우 중요한 의미를 가진다. 즉 AS 레벨 토폴로지는 새로운 프로토콜의 효율성을 평가하고 개선하기 위한 다양한 연구활동에 사용되고 있으며, 인터넷 토폴로지 특징을 분석하고 AS 관계와 인터넷 계층구조를 추론하는데 AS 레벨 토폴로지가 활용되어 왔다.

AS 레벨 토폴로지를 생성하는 방법은 크게 두 가지가 있다. 첫 번째 방법은 일반인들에게 공개된 Route Views와 RIPE-RIS가 제공하는 데이터 셋을 이용해 직접 AS 레벨 토폴로지를 생성하는 방법과 두 번째 방법으로 AS 레벨 토폴로지를 자동으로 생성하는 발생기를 이용할 수 있다. RouteViews와 RIPE-RIS와 같은 프로젝트들은 현재 운영 중인 수 백 개의 라우터와 BGP 세션을 형성해 데이터를 수집하고 있으며, 일반인들이 접근해 이들 데이터 소스를 사용할 수 있도록 공개되고 있다[7,8]. 그러나 최근 참고문헌[5]와 [6]에서는 이들 공개 데이터 소스만을 활용해 인터넷 AS 토폴로지를 추론할 경우, 전체 AS 토폴로지의 상당 부분이 발견되지 못하는 문제점을 지적하고, 새로운 발견적 방법(heuristic method)를 이용하여 관찰된 AS 토폴로지로부터 모든 사용자-제공자(customer-provider) 링크를 정확하게 확인할 수 있는 방법을 제안하였다. 한편, AS 레벨 인터넷 토폴로지 발생기 Inet-3.0[10]과 NIT[11]는 현 인터넷 토폴로지 특징을 흉내 내어 AS 노드 수와 노드 차수(degree) 정보를 입력 받아 AS 토폴로지 연결 정보를 자동으로 생성해 낸다. 그러나 이들 발생기들이 현 인터넷 토폴로지 특징을 정확하게 반영하기에는 아직 여러 가지 문제점들이 있다[10,11].

앞에서 언급한 바와 같이 인터넷 AS 레벨 토폴로지에 관한 연구가 상당히 많이 이루어지고 있으나 실질적인 응용사례가 매우 드물다. 그 이유는 대부분의 기존 연구들이 AS 레벨 토폴로지의 물리적 연결 구조, 즉 AS 노드의 차수 정도와 두 AS 노드 사이의 물리 링크의 거리 등의 특징을 다루거나 혹은 얼마나 정확하게 실제 인터넷 토폴로지를 얻을 것인가에 초점이 맞추어져 왔다. 물론, AS 레벨에서 분산 패킷 필터링 효과를 연구한 사례[12]도 있으나, 이와 같은 실질적인 응용이 이루어진 연구 결과를 찾아보기란 쉽지 않다.

1.2 연구 동기

많은 인터넷 AS 레벨 토폴로지 연구가 물리적 연결 구조 특징을 밝히는데 머물러 있다. 그러나 BGP 라우팅 프로토콜에 의해 실질적인 AS 레벨 경로가 결정되며, 따라서 본 논문에서는 기본적인 BGP 라우팅 정책을 기반으로 한 인터넷 AS 레벨 라우팅 패스 토폴로지(이하, 본 논문에서는 간단히 'AS 레벨 토폴로지'로 약칭) 구조를 파악한다. BGP 라우팅 프로토콜의 가장 큰 특징은 각 AS가 자신의 관리정책에 의해 최적 경로를 선택하고 경로정보를 송·수신하는 것이다[16]. 그러나 수 천 개의 각 AS 별 고유한 관리정책을 모두 반영하여 AS 레벨 토폴로지 구조를 파악하는 것은 사실상 불가능한 것이며 또한 큰 의미를 가지지 못한다. 따라서 본 연구에서는 BGP'밸리 프리(valley-free)'기본 정책을 기반으로 미국 UCLA 전자계산학과 Internet Research Lab (IRL) 에서 제공하는 실제 인터넷에서 추출된 AS 레벨 토폴로지 자료를 활용하여 계층별 - tier1, largeISP, smallISP, 그리고 stub AS - AS 노드의 라우팅 패스 구조를 알아 본다. 또한 본 논문에서는 이러한 연구결과를 활용할 수 있는 응용 분야를 도출하기 위한 노력을 기울여 왔으며, 이 들 중에서 최근 가장 많은 관심을 끌고 있는 분산 서비스거부 공격(DDoS : Distributed Denial of Service) 징후를 탐지하는 방법을 제안한다.

2003년 발생된 1.25 인터넷 대난과 최근 발생된 2009년 7.7 인터넷 대난을 겪으면서 인터넷 보안 분야가 오늘날 정보화 사회에서 차지하는 비중이 얼마나 막중한지 간접적으로 가늠해 볼 수 있었다. 뿐만 아니라, 물질적인 피해를 떠나 사회적 혼란에 따른 정신적 피해 규모는 실로 엄청나다고 볼 수 있다. 따라서 DoS 공격으로부터 네트워크와 시스템을 안전하게 보호하는 문제는 현재 우리에게 당면한 가장 중요한 이슈 중 하나이다. DDoS 공격을 탐지하는 방법은 크게 시그너처(signature) 기반과 비정상행위(anomaly) 기반으로 구분된다[13]. 시그너처 기반은 Snort 혹은 Bro와 같은 보안 전문가들에 의해 DDoS 공격 행위와 특징들을 분석한 결과를 이용해 이를 패턴화하고 이 패턴을 검출하고 방어할 수 있는 방법들을 동원하는 것이다[13,17]. 예를 들어, 최근 유행하는 DDoS 공격을 담당하는 봇넷(Bot-Net)을 검출하기 위해 감염된 봇들이 시도하는 숙주 DNS 질의를 시그너처로 만들어 모니터링하는 방법을 사용하게 된다[14]. 그러나 새로운 DDoS 공격 형태가 출현하게 되면 일정시간 이들 공격 유형과 방법들을 분석하고 이를 반영하기 까지는 상당한 시간이 소요된다. 따라서 새로운 변종 DDoS 공격이 출현할 때마다 엄청난 사회적 혼란과 비용을 지불하게 된다. 이에 반해 비정상행위 기반 DDoS 공격 탐지는 정상 트래픽을 모델링하고 이 모델을 벗어나게 되면 공격을 탐지하게 된다[13,18,19]. 따라서 비정상행위 기반은 시그너처가 만들어질 필요가 없기 때문에 새로운 공격을 탐지할 수 있다. 그러나 공격의 가능성만 알려줄 뿐 공격의 성격을 정확하게 밝혀내지는 못하며 정상 트래픽이 경우에 따라 모델을 벗어날 수 있어 오탐(false alarms)을 발생시킬 수 있다. 예를 들어, TCP SYN 플러딩을 이용한 DDoS 공격에 대한 검출은 일정시간 불완전하게 이루어지는 TCP 연결회수를 카운트 함으로서 탐지가 가능하

다. 그러나 카운트 값에 대한 임계값(threshold) 설정은 DDoS 공격에 대한 탐지율과 오탐율에 영향을 미치게 된다.

인터넷 상에서 DDoS 공격은 수 천에서 수 만의 감염된 좀비 호스트들이 하나의 표적 시스템을 공격하여 이 표적 시스템이 정상적인 사용자의 접근에 따른 서비스를 더 이상 지원하지 못하는 상태에 이르게 한다. 따라서 DDoS 공격이 발생하게 되면, 공격 대상 시스템을 중심으로 AS 레벨 토폴로지 상에서 해당 이벤트가 전역적으로 고르게 분포하게 될 것이며, 본 논문에서는 이와 같은 DDoS 공격의 본질적인 성질인 트래픽 임의성(randomness)[15,18,19]을 인터넷 AS 레벨 토폴로지 상에서 검출하는 방법을 제안하였다. 제안된 방법은 몇 개의 모니터링 AS에서 검출된 이벤트 수를 상호 비교함으로써 현재 발생되고 있는 이벤트가 얼마나 광범위하게 이루어지고 있는지 예측할 수 있게 된다.

서론에 이어, 제2장에서는 인터넷 AS 레벨 토폴로지의 다양한 분포 및 특징들을 기술하고 BGP'밸리-프리' 정책에 기반한 AS-레벨 라우팅 패스 토폴로지 특징을 기술한다. 제3장에서는 이들 분포를 이용해 인터넷 트래픽 임의성을 검출하는 방법을 제시하고, 모의실험을 통해 제안된 방법의 타당성을 검증하였다. 마지막으로 제4장에서 결론 및 향후 연구 방향에 대해 기술하였다.

2. 인터넷 AS 레벨 토폴로지

2.1 AS 레벨 토폴로지

본 논문에서는 최근의 AS 레벨 토폴로지 구조를 분석하기 위해 미국 UCLA IRL 연구실에서 제공하는 2009년 8월 9일자 실제 인터넷 AS 토폴로지 데이터 소스를 사용한다. AS 레벨 토폴로지는 계층구조를 가진다. 즉 상위계층에 위치하는 AS 노드는 사용자 링크를 통해 하위 AS 노드들의 트래픽을 전달하는 서비스를 제공하게 된다. 과거에는 각 AS 노드의 차수 혹은 AS에서 기인하는 prefix 수를 기준으로 AS 계층을 분류하기도 하였으나, 최근에는 제공자-사용자의 관계를 추론하여 계층화하는 방법을 사용하고 있다[5,6]. 본 논문에서도 Oliveira et al.[5,6]가 제안한 방법을 사용하여, 각 AS의 하위 스트림 사용자 AS의 수를 기준으로 다음 표 1과 같이 4계층으로 각 AS를 분류하였다. 표 1에서 전체 AS 노드들의 집합 S 의 크기는 33,495이며, 세 번째 열의 $C(j)$ 는 AS 번호 $j \in S$ 의 하위 스트림 사용자 AS 개수를 나타낸다. 참고문헌[5]에서 제시한 2008년 기준 AS 분류와 비교하여, 전체 AS에 대한 stub AS의 비율이 95.5%로 3.5% 증가하였으며 사용자 AS를 전혀 가지지 않는 AS 비율도 80%에서 89.2% 증가한 것으로 조사되었다. 이와 같은 stub AS 비율의 증가는 급증하는 인터넷 사용자 추세와 더불어 쉽게 예측되는 결과라고 볼 수 있다.

표 1 2009년 8월 9일자 AS 레벨 토폴로지 데이터 소스

AS 타입	AS 수 (전체 AS에 대한 퍼센트)	기준
Tier1	8 (0.02)	제공자가 없는 AS
Large ISP	235 (0.7)	$C(j) \geq 50$
Small ISP	1263 (3.77)	$5 \leq C(j) < 50$
Stub	31,989 (95.5)	$C(j) < 50$

Faloutsos et al.[3]는 AS 토폴로지 그래프 상에서 노드 차수 분포의 power-law 특징 연구 결과를 발표했다. 이러한 연구결과는 당시 네트워크 관련 분야에서 전혀 예상하지 못한 사실이었으며, 이러한 현상을 만들어 내는 원인 파악에 많은 노력을 기울여 왔다[4]. 본 논문에서 사용하는 AS 레벨 토폴로지 역시 그림 1에서 보는 바와 같이 AS 노드 차수의 power-law 특성이 여전히 유지되고 있음을 확인할 수 있다. 그림에서 빈도수 f_d 는 차수 d 를 가진 AS 노드 수이다. 그림 1에서 f_d 는 로그 좌표에서 선형적으로 근사됨을 확인할 수 있고 상관계수(correlation coefficient)가 0.9617로서 1997년 기준 0.968-0.99[3]와 비슷한 수준으로 유지되고 있음을 확인할 수 있다. 한편, 본 논문에서는 AS 노드들의 하위 스트림 AS 노드 개수 (사용자 트리 크기 c) 분포에 대한 power-law 성질을 그림 2에서와 같이 확인하였다. 그림 2(b)에서 사용자 트리 크기가 큰 214개 AS (전체 AS의 0.63%)를 제외한 빈도수 f_c 는 power-law 성질을 따르고 있다.

그림 3과 그림 4는 각 레벨에서 AS가 갖는 사용자 및 피어 링크의 분포를 각각 보여 준다.

그림 3에서 보듯이 stub AS의 89.2%가 사용자 링크를 가지지 않으며, smallISP와 largeISP AS 계층은 각

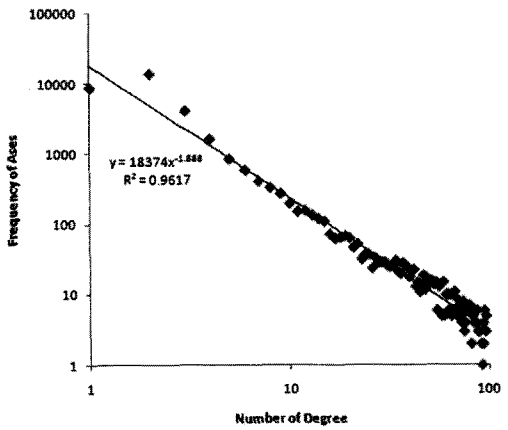
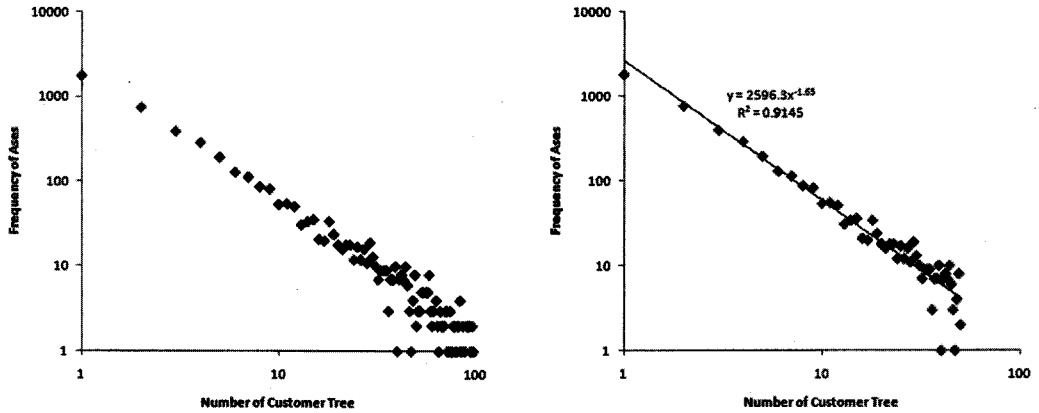
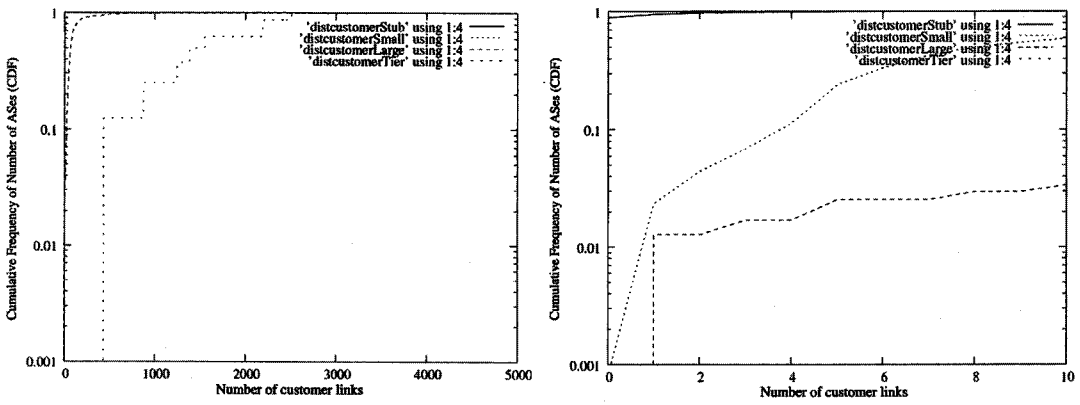


그림 1 AS 노드의 차수 분포: 차수 d 에 대한 빈도수 f_d



(a) 전체 (b) $c = 97$ 에서 제한

그림 2 AS 노드의 사용자 트리 분포: 사용자 트리 크기 c에 대한 빈도수 f_c



(a) (b)

그림 3 각 AS 레벨에서 사용자 링크 개수 분포 ((b)는 (a)의 x 축을 확대)

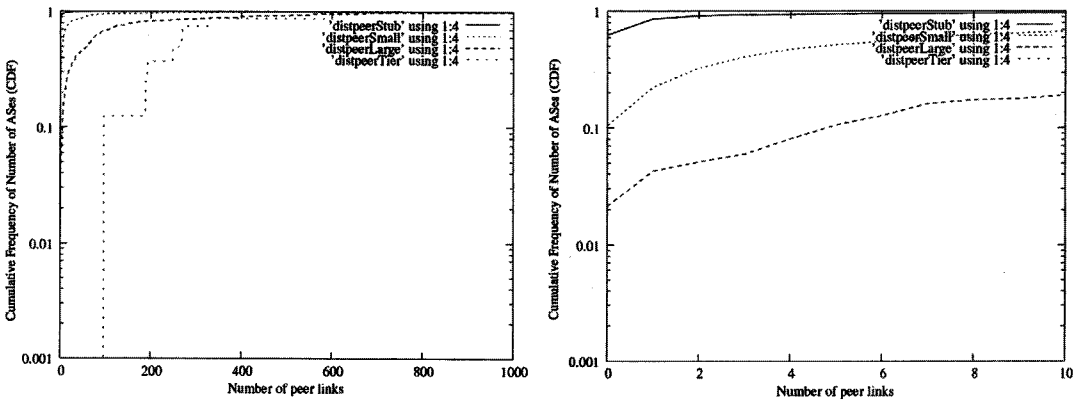


그림 4 각 AS 레벨에서 피어 링크 개수 분포 ((b)는 (a)의 x 축을 확대)

각 평균적으로 8개와 69개의 사용자 링크를 가진다. 한편 tier1 AS는 최소 436에서 최대 2511개의 사용자 링크를 갖는 것으로 조사되었다. 그림 4에서 보듯이 stub AS의 63%는 피어 링크를 가지지 않으며 smallISP AS는 90%가 1개 이상의 피어 링크를 가지며 평균 5개 피어 링크를 가진다. 또한 largeISP AS는 98%가 1개 이

표 2 Tier1 AS의 하위 스트림 AS 수

AS 번호	1760	10309	17275	18091	18187	21373	25847	26461
$C(j)$	27,899	26,748	26,855	26,648	25,274	25,713	26,722	27,500

상의 피어 링크를 가지며 평균 58개 피어 링크를 가지고, tier1 AS의 경우 최소 97에서 최대 584개의 피어 링크를 가지는 것으로 조사되었다. 이러한 조사 결과는 우리가 일반적으로 예상하는 것보다 AS 레벨 토폴로지가 훨씬 복잡하고 심하게 상호 연결되어 있음을 확인할 수 있다. 한편, tier1 AS에서 $C(j)$를 조사하여 다음 표 2에 나타내었다(본 논문에서 사용된 AS 번호는 보안상의 이유와 더불어 개인정보 보호 차원에서 무작위 번호로 변환하여 표기하였으며, 시험용 테스트 베드로 사용 중인 1개의 AS 노드와 잘못 설정된 230개의 제공자-사용자 링크가 IRL에서 제공하는 데이터 소스에서 제외되었음을 밝힌다). 표 2에서 보듯이 tier1 AS 노드들은 25,000개 이상의 하위 스트림 AS 노드들을 연결하고 있으며, 따라서 전체 AS 수를 고려하면 대부분의 stub AS 노드들은 8개의 tier1 AS의 하위 스트림 AS 노드에 포함되어 있다고 보아야 한다. 이러한 사실을 직접 확인하기 위해 미국 중부에 위치한 주립대학(AS 번호 5384) 한 곳과 국내 연구소(AS 번호 4008) 한곳을 중심으로 8개 tier1 AS와의 연결 구성을 그림 5에서 나타내었다. 그림 5에서, 두 stub AS 모두 트래픽 분산과 이중화를 위해 멀티-홈 연결을 유지하고 있으며, 각각 8개 tier1 AS의 하위 스트림 노드에 속해 있음을 확인할 수 있다. 한편 국내(AS 4008)의 경우 미국(AS 5384)에 비해 상대적으로 간단한 트리 구조에 연결되어 있음을 확인하였다.

그림 6은 smallISP와 largeISP에 속한 AS 노드들의 하위 스트림 AS 노드 수 분포를 보여준다. SmallISP의 경우 평균 14.3개, largeISP의 경우 평균 299.6개, 그리고 stub AS의 경우 평균 0.07개의 하위 스트림 AS 노드를 가지고 있음을 확인하였다.

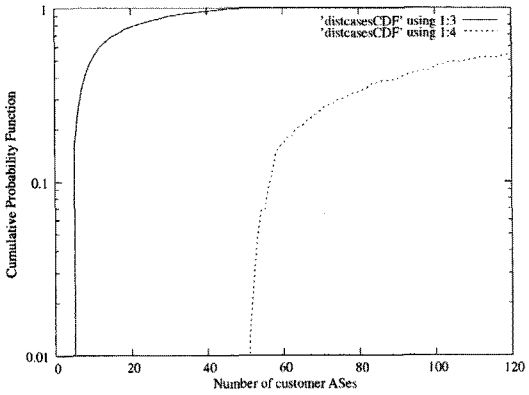


그림 6 SmallISP와 LargeISP AS들의 하위 스트림 AS 수 분포(실선: SmallISP, 점선: LargeISP)

2.2 인터넷 도메인 연결 및 피어링

BGP 라우팅 결정은 대부분 라우팅 정책에 의해 결정되며 가장 중요한 요소는 이웃 AS 사이의 사업적 관계이다. 이들 사업적 관계는 두 가지 주요 타입, 즉 사용자-제공자(customer-provider)와 피어-피어(peer-peer)가 있다[1,5]. 사용자-제공자 관계는 사용자는 인터넷 사용을 위한 트래픽을 송·수신을 위해 제공자에게 비용을 지불하고, 제공자 AS는 사용자 AS에게 모든 인터넷 경로를 알려주며 사용자 AS의 인터넷 트래픽을 전달하는 역할을 수행한다. 그러나 사용자 AS는 자신의 제공자 AS 트래픽을 전달하지는 않는다. 즉 그림 7(a)에서 보듯이 자신의 제공자 트래픽은 자신의 하위 사용자 AS로만 전달하며 또 다른 제공자 AS나 피어 AS로 전달하지 않는다. 한편, 피어-피어 관계는 두 피어 AS에 직접 연결된 하위 스트림 AS에서 시작되고 종료되

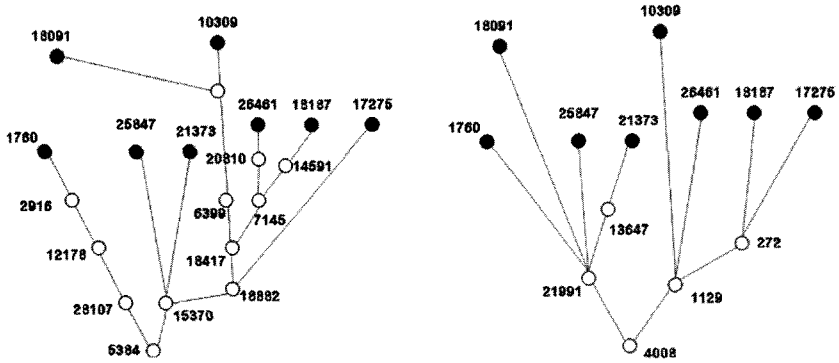


그림 5 Stub AS 5384, 4008의 tier1 AS와 연결 토폴로지(검은 점: tier1 AS 노드)

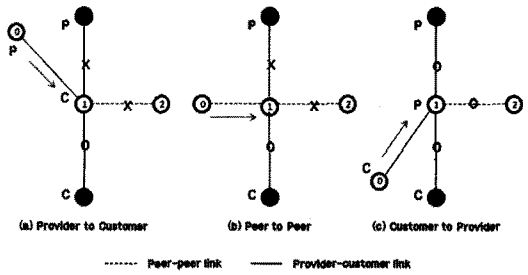


그림 7 AS 레벨 "밸리-프리" 라우팅 정책
(P: Provider, C: Customer, O: Permission, X: Deny)

는 트래픽을 상호 간에 비용을 지불하지 않고 교환한다. 따라서 그림 7(b)에서 보듯이 AS는 피어-피어 링크를 포함하는 루트를 자신의 제공자 혹은 다른 피어 AS에게 전달하지 않는다. 이러한 특징을 요약하면, 오늘날 인터넷에서 사용하는 기본 정책은 "밸리-프리" 혹은 "노-밸리(No-valley)" 라우팅 정책이다. 즉 AS는 자신의 제공자 AS의 트래픽을 자신의 하위 사용자 AS로 전달하는 것 이외의 트래픽 전달 서비스는 허용하지 않는다. 마지막으로 사용자 트래픽을 받는 제공자 AS는 그림 7(c)와 같이 모든 인터넷 경로를 사용자 트래픽을 전달할 수 있어야 한다.

2.3 AS 레벨 라우팅 패스 토폴로지

AS 레벨 라우팅 프로토콜인 BGP는 정책기반 라우팅 기법으로 각 AS에서 자신의 고유한 라우팅 정책을 운영할 수 있다. 즉 AS들은 특정 AS 패스를 우회하거나 특정 AS 패스에 대한 우선순위를 부여할 수 있다[16]. 그러나 본 연구에서는 이와 같은 개별 AS 별 고유한 정책은 고려하지 않으며, 모든 AS들은 단지 최소 거리(minimum AS-path distance)에 의한 라우팅 패스를 결정한다. 물론 "밸리-프리" 정책에 추가적으로 하나의 목적지에 대해 여러 개의 동일 metric 라우팅 패스가 존재할 경우 하나의 최적 라우팅 패스를 결정하기 위한 다음 두 가지 기본 라우팅 정책을 사용하는 것을 가정한다:

- AS-path 에트리뷰트(attributes)에 tier1 AS 번호가 없는 업데이트 메시지에 우선순위
- 피어 링크를 통해 입력되는 업데이트 메시지에 우선순위

첫 번째 가정은 AS 라우팅 패스의 지역성을 고려하기 위함이다. 즉 미국 내에 존재하는 AS 레벨의 최상위 계층까지 거치는 패스보다는 각 AS의 지역 내에서 우선적으로 라우팅 패스가 형성되도록 한다. 또한, 피어 링크를 설치하는 경우는 경제적 그리고 우선적인 패스 경로를 확보하기 위함이다. 따라서 두 번째 가정은 이러한 피어 링크 정책에 기인한다. 그림 8은 그림 5에서 설명한 AS4008과 AS5384를 각각 하나의 목적지로 설정한 다음, 모든 stub AS 로부터 시작하는 라우팅 패스의 홉 수에 따른 stub AS 개수를 보여준다. 그림에서 보듯이 전체적으로 tier1 AS 노드를 경유하지 않는 stub AS 개수가 tier1AS 노드를 경유하는 stub AS보다 많으며, 이것은 앞에서 설명한 기본 라우팅 정책에 의한다. 즉, 전체 stub AS 중, AS4008은 29.5% 그리고 AS5384는 38.4%가 tier1 AS 노드를 경유한다. 한편, 그림 9는 모든 stub AS 로부터 시작되는 표적 AS4008과 AS5384의 라우팅 패스의 홉 수 분포를 보여준다. AS4008에 비해 AS5384는 상대적으로 라우팅 홉 수가 많은 것을 확인할 수 있다. 이것은 그림 5에서 설명했듯이, AS4008의 경우 AS5384에 비해 상대적으로 간단한 트리 구조에 포함되어 있기 때문이다. AS4008(혹은 AS 5384)을 기준으로 tier1 AS를 경유할 경우 평균 3.409 홉(혹은 3.953 홉)과 tier1 AS를 경유하지 않을 경우 평균 3.676 홉(혹은 4.49 홉)을 갖는다.

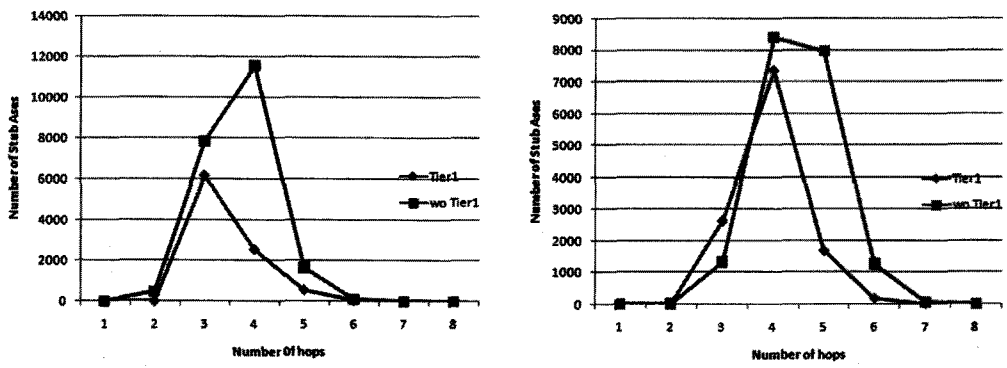


그림 8 발신지-목적지 사이 라우팅 패스의 홉 수에 따른 stub AS 수((a) AS 4008, (b) AS 5384)

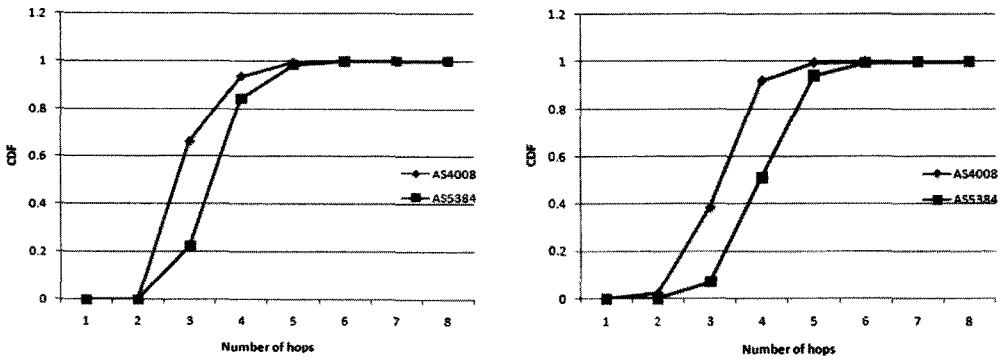


그림 9 발신지-목적지 사이 라우팅 패스의 홉 수((a) Tier1 AS 노드를 경유하는 경우, (b) Tier1 AS 노드를 경유하지 않는 경우)

3. AS 레벨 토폴로지에서 트래픽 임의성 검출

DDoS 공격은 수 천에서 수 만개 이상의 좀비 컴퓨터로부터 공격 이벤트가 발생된다. 본 절에서는 제2장을 통해 얻어진 AS-레벨 토폴로지에서 DDoS 공격 징후를 탐지하는 방법을 제시한다. 즉 AS 레벨 토폴로지 상에서 몇몇 특정 AS 노드를 모니터링 지점으로 지정하고, 이 곳에서 검출되는 이벤트의 수를 기초로 현재 발생되는 이벤트의 임의성을 판단한다. 예를 들어, AS 노드 i,j 그리고 k가 각각 모니터링 지점으로 사용되고 각 stub AS에서 균일하게 표적 AS로 이벤트가 발생되면, 이들 각 지점에서 검출된 이벤트 수 $m(i), m(j)$ 그리고 $m(k)$는 각 모니터링 지점의 하위 스트림 AS 분포를 따르게 된다.

3.1 모니터링 지점과 예상 이벤트 수

먼저, 본 절에서는 모니터링 지점으로 사용할 AS 노드를 결정한다. 이러한 결정에서 가장 중요한 요소는 최소의 모니터링 지점으로 효율적으로 이벤트 수를 추적하는 것이다. 따라서 AS 레벨 토폴로지 상에서 가능한 상위 계층, 즉 tier1 혹은 largeISP AS 노드를 모니터링 지점으로 선택함으로써 최대한 많은 이벤트 수를 검출할 수 있도록 한다. 제3장에서 설명한 바와 같이 AS 토폴로지 상에서 tier1 AS 들은 피어 링크를 통해 풀-메쉬(full mesh)로 연결되어 있으며, 이들 tier1 AS 노드의 $C(j)$는 표 2에서 보듯이 최소 25,000 이상이다. 따라서 대부분의 stub AS 노드는 이들 8개의 tier1 AS 노드들의 하위 스트림 AS 내에 존재하게 되고 임의의 표적 AS 노드로 갈 수 있는 매우 다양한 패스가 존재하게 된다. 궁극적으로 이들 stub AS가 어떤 tier1 AS 노드를 경유하게 될지는 통계적 혹은 확률적으로 예측하기가 사실상 불가능하다. 따라서 본 논문에서는 tier1 AS의 사용자 링크로 직접 연결되어 있는 198개의 largeISP AS 노드를 사용 가능한 모니터링 지점으로 활용하였다. 다음 표 3은 이들 198개 AS 중 임의로 선택한 9개 모니터링 AS의 하위 스트림 AS 분포를 보여준다. 표 3에서 $C_2(j)$, $C_1(j)$ 그리고 $C_0(j)$는 각각 AS j의 하위 스트림 상의 largeISP, smallISP, 그리고 stub AS에 속한 AS 개수이며, $D_2(j)$, $D_1(j)$ 그리고 $D_0(j)$는 각각 AS j의 가입자 링크에 의해 직접 연결된 각 계층별 AS 노드 수이다. 따라서 $C_i(j) \geq D_i(j)$, $i = 0,1,2$의 관

표 3 모니터링 지점 AS의 하위 스트림 AS 분포

No	AS	$C(j)$	LargeISP		SmallISP		Stub AS	
			$C_2(j)$	$D_2(j)$	$C_1(j)$	$D_1(j)$	$C_0(j)$	$D_0(j)$
9	13490	230	0	0	10	3	220	40
8	18	304	0	0	0	0	304	287
7	32755	300	1	1	8	6	291	17
6	25841	128	0	0	7	3	121	35
5	33330	158	0	0	4	4	154	84
4	31706	128	0	0	1	1	127	106
3	819	295	1	1	11	1	283	57
2	31015	592	0	0	3	3	589	523
1	31202	252	0	0	14	13	238	55

계식이 성립한다.

그림 10은 하나의 표적 AS 노드를 기준으로 stub AS들의 가능한 라우팅 패스를 보여준다. 그림에서 보듯이, 모니터링 AS k에서 다음 사실을 알 수 있다.

- 표적 AS 까지 홉 수, $H(k)$
- 다음-홉(next-hop) AS 가 tier1 AS 노드 여부
- 자신과 다음-홉 사이의 링크, $L(k)$,의 종류 (제공자 링크, 사용자 링크, 혹은 피어 링크)
- 자신의 하위 스트림 AS 개수, $C(k)$
- 사용자-제공자 링크로 직접 연결된 하위 스트림 AS 분포, $D(k)=\sum_{i=0}^{2} D_i(k)$

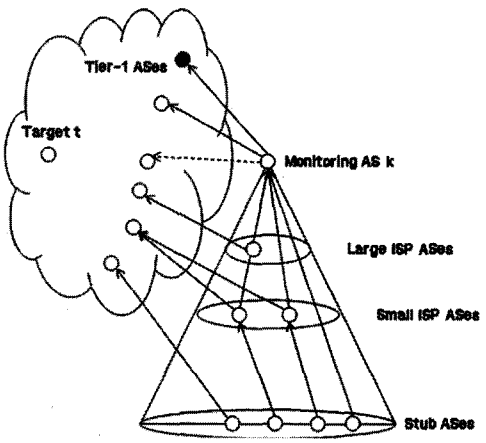


그림 10 표적 AS t와 모니터링 AS를 기준으로 stub AS들의 가능한 라우팅 패스(실선: 제공자-가입자(provider-customer) 링크, 점선: 피어(peer-peer) 링크)

한편, 모니터링 AS k의 다음-홉 링크는 다음 네 가지 경우가 존재한다: (i) tier1 AS가 아닌 제공자 링크, (ii) tier1 AS에 연결된 제공자 링크, (iii) 피어 링크, 그리고 (iv) 사용자 링크.

레마 1. 모니터링 AS k가 표적 AS t로 가는 라우팅 패스의 다음-홉 링크가 제공자 혹은 피어 링크로 연결되면 단지 사용자 링크를 통해 자신의 하위 스트림 $C(k)$에 속한 stub AS로부터 발생된 표적 AS t로 향하는 이벤트를 검출하게 된다.

증명. 모니터링 AS k에서 자신의 하위 스트림 $C(k)$에 속하지 않는 stub AS로부터 발생된 표적 AS t로 향하는 이벤트가 검출되었다고 가정하자. 이러한 이벤트는 모니터링 AS k의 제공자 혹은 피어 노드를 통해서만 입력 가능하다. 그러나 BGP'밸리-프리'기본 정책에 의해, AS k는 제공자 혹은 피어 노드를 통해 입력된 트래픽을 자신의 제공자 혹은 피어 링크를 통해 전달하는 서비스를 지원하지 않는다. 결론적으로 가정에 모순이 발생한다. ■

레마 2. 모니터링 AS k가 표적 AS t로 가는 라우팅 패스의 다음-홉 링크가 자신의 사용자 링크로 연결되면 모니터링 AS k의 제공자, 사용자, 그리고 피어 링크 등 다양한 경로를 통해 표적 AS t로 발생되는 이벤트를 모두 검출하게 된다.

증명. 모니터링 AS k가 표적 AS t로 가는 라우팅 패스의 다음-홉이 사용자 링크인 경우, 표적 AS t는 $C(k)$에 속하게 된다. 따라서, 표적 AS t는 AS k의 하위 사용자 AS 임으로 AS t로 향하는 모든 트래픽을 전달해 주어야 한다. ■

모니터링 AS에서 표적 AS로 가는 라우팅 패스의 다음-홉이 사용자 링크로 연결되는 경우, (레마 2)로부터 다양한 경로의 이벤트를 모니터링 AS가 검출함으로 이벤트 발생 임의성을 따지기에는 어려움이 따른다. 따라서 본 논문에서는 (레마 1)로부터 표적 AS로 가는 라우팅 패스의 다음-홉이 제공자 혹은 피어 링크로 연결되는 모니터링 AS에서 만 이벤트 수를 고려한다.

그림 10에서 살펴 보았듯이, 모니터링 AS k의 하위 스트림 내 stub AS 개수, $C_0(k)$, 중 표적 AS로 다음과 같이 크게 세가지 물리적 연결 구조, 즉 (i) (stub AS-smallISP-largeISP-AS k), (ii)(stub AS-small-ISP-AS k), 그리고 (iii) (stub AS-AS k) 가 가능하다. 이들 세 가지 경우에 속하는 stub AS 개수를 각각 $C_0^2(k)$, $C_0^1(k)$, 그리고 $C_0^0(k)$ 이라고 정의하면 ($C_0(k)=\sum_{i=0}^{2} C_0^i(k)$), $C_0(k)$ 중 AS k를 경유하여 표적 AS t로 라우팅 패스를 가지는 stub AS 개수 $m(k)$는 다음과 같이 계산할 수 있다.

$$m(k)=\sum_{i=0}^{2} P_{pass}(i)\cdot C_0^i(k). \quad (1)$$

여기서, $P_{pass}(i)$ 다음과 같이 계산된다.

$$P_{pass}(i)=Prob\{C_0^i(k)\text{에 속한 stub AS가 모니터링 AS } k\text{를 경유}\}$$
$$=Prob\{\text{라우팅 홉 수}=H(k)+\propto(i)\} \quad (2)$$

여기서, $H(k)$는 모니터링 AS k에서 표적 AS t까지 홉 수이며, $\propto(i)$는 $C_0^i(k)$가 모니터링 AS k까지 도달하는데 소요되는 홉 수이다. $C_0^i(k)$는 식 (1)에서 설명한 바와 같이 세가지 물리적 연결구조를 가정하고 있으나, 모니터링 AS k가 자신의 하위 스트림 AS 들이 어떠한 연결구조를 가지고 있는지 확인하기가 쉽지 않으며, 따라서 $\propto(i)$를 정확하게 결정할 수 없다. 즉 $C_0^0(k)$의 경우, (stub AS - AS k)의 물리적 연결구조이긴 하나, stub AS 역시 또 다른 stub AS를 제공자 혹은 사용자 AS로 연결될 수 있기 때문이다. 이러한 이

유는 $C_0^1(k)$와 $C_0^2(k)$에도 적용된다(그림 5 참조). 따라서 이제 상기 식 (2)를 다음과 같이 CCDF(Complementary Cumulative Distribution Function)를 이용해 계산한다.

$$P_{pass}(i)=1-Prob\{\text{라우팅 홉수}=H(k)+\hat{\alpha}(i)-1\} \quad (3)$$

여기서, $\hat{\alpha}(i)$은 $C_0^i(k)$가 모니터링 AS k까지 도달하는데 소요되는 최소 홉 수이다. 즉 $\hat{\alpha}(i)=i+1,\ i=0,1,2$가 된다. 예를 들어, $C_0^2(k)$의 경우, (stub AS-smallISP-largeISP-AS k) 임으로 $\hat{\alpha}(2)=3$이 된다. 제2.3절에서 하나의 표적 AS를 대상으로 모든 stub AS로부터 도달하는데 소요되는 라우팅 홉 수의 분포를 알아 보았다. 이제 이 분포를 확률변수 X로 나타내고 이 확률변수는 유한한 이미지 $\{1,2,\cdots,m\}$를 갖는 것으로 가정한다. 이제 확률변수 X를 세분화하여, 표적 AS의 번호가 as이고 tier1 AS를 경유하는 경우, X_{as}^{w}, 그리고 tier1 AS를 경유하지 않는 경우, X_{as}^{wo}로 각각 정의한다. 따라서 상기 식 (3)에서 $P_{pass}(i)$는 다음 식을 이용해 구할 수 있다.

$$P_{pass}(i)=1-F_{X_t}(H(k)+i) \quad (4)$$

여기서, $F_X(\cdot)$는 확률변수 X의 CDF(Cumulative Density Function)을 나타낸다. 또한, 다음-홉이 tier1 AS 여부에 따라 $F_{X_t^w}(\cdot)$ 혹은 $F_{X_t^{wo}}(\cdot)$가 각각 사용된다. 한편, 앞에서 설명한 바와 같이 모니터링 AS k가 하위 스트림 AS 들의 연결구조를 알고 있지 않는 한 $C_0^i(k), i=0,1,2$를 알 수는 없으며, 또한 하위 ISP가 스스로 관리하는 하위 구조를 모니터링 AS k가 알기에는 현실적으로 불가능하다. 따라서, 관찰된 AS 레벨 토폴로지 상에서 stub AS, smallISP, 그리고 largeISP가 갖는 평균 하위 스트림 AS 노드 수를 이용하여 다음과 같이 평균값에 근사한다.

$$C_0^i(k)\cong\hat{C}_0^i(k)=\begin{cases}D_i(k)\cdot E_i, & \text{if } i=1,2\\ D_0(k)+D_0(k)\cdot E_0, & \text{if } i=0\end{cases} \quad (5)$$

여기서, E_0, E_1과 E_2는 각각 stub AS, smallISP, 그리고 largeISP에서 관찰된 평균 하위 스트림 AS 노드 수이다.

3.2 모의실험 결과 분석

본 논문에서는 제2장에서 설명한 BGP 기본 정책에 기반한 AS-레벨 라우팅 패스 토폴로지 생성을 위해 마이크로소프트 사의 ODBC(Open Data Base Connectivity)를 이용한 MS-SQL C++ 시뮬레이션 프로그램을 자체 제작하여 모의실험을 실시하였다. 그림 11은 표 3에 기술한 모니터링 AS에서 측정된 이벤트 수와 식 (1)에 의해 예상되는 각 모니터링 AS에서 자신의 하위 스트림 내 stub AS로부터 모니터링 AS를 경유하는 라우팅 패스 수의 차이를 보여준다. 모의실험은 모의실험 단위시간 마다 하나의 stub AS가 표적 AS로 이벤트를 발생시켜 마지막 stub AS가 이벤트를 발생시킬 때까지 진행되었으며, 모니터링 AS 노드들은 이들 이벤트 수를 기록하였다. 그림 11에서 보듯이, 각 모니터링 AS에서 자신의 노드를 경유하여 특정 표적 AS 노드로 향하는 stub AS 수를 식 (1)을 이용하여 비교적 정확하게 예측할 수 있다. 따라서 각 모니터링 AS에서 상기 식 (1)과 같은 비율로 이벤트가 검출된다면 이것은 이벤트 발신지의 임의성을 보이는 것으로 판단할 수 있다. DDoS 공격은 앞에서 설명한 바와 같이 광범위하게 분포된 수천~수만의 좀비 컴퓨터로부터 표적 시스템으로 이벤트가 발생하게 되며 따라서 각 모니터링 AS에서 검출된 이벤트 수를 비교하면 상기 식 (1)과 같은 비율을 따르게 될 것이다.

그림 12는 미국 내 6,870개 stub AS를 서비스하는 하나의 대형 ISP를 출발점으로 국내 AS 4008을 표적 AS로 설정한 후, 모의실험을 통해 모니터링 AS에서 검

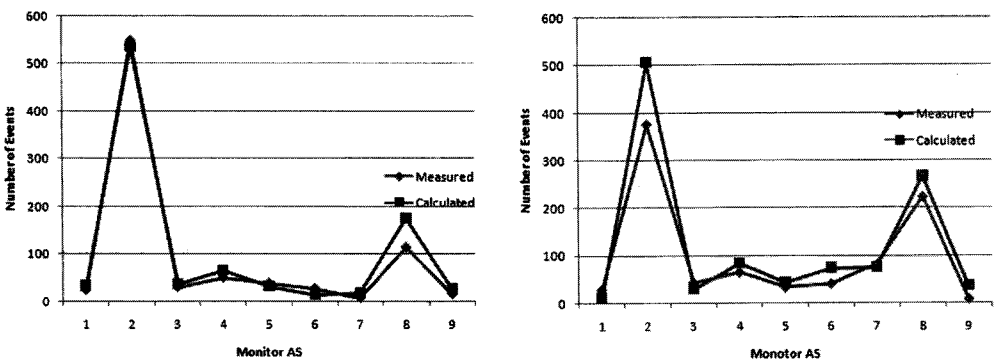


그림 11 모의실험을 통해 표 3의 모니터링 AS에서 검출된 이벤트 수와 식 (1)에 의한 예상 이벤트 수 비교 ((a) AS 4008 (b) AS 5384)

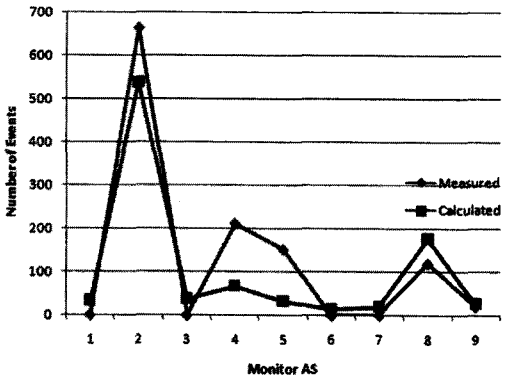


그림 12 표적 AS 4008을 목적지로 특정 협의 지역에서 발생되는 이벤트에 대한 모의실험 결과

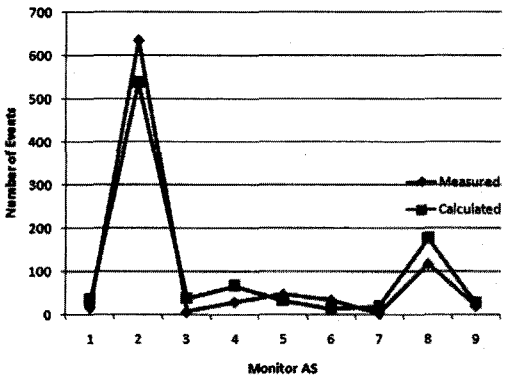


그림 13 표적 AS 4008을 목적지로 전체 stub AS 중 10%에서 발생되는 이벤트에 대한 모의실험 결과

출된 이벤트 수를 나타내었다. 모의실험 시간은 그림 11과 비교하기 위해 전체 이벤트 발생 수가 그림 11의 모의실험 이벤트 수와 동일할 때까지 지속되었으며, 이들 6,870개 stub AS를 순차적으로 발신지로 지정하였다. 그림 12에서 보듯이, 모니터링 노드 1, 3, 6, 그리고 7에서는 전혀 이벤트가 검출되지 않았으며, 모니터링 노드 4와 5에서는 지나치게 많은 이벤트 수가 검출됨을 확인할 수 있다. 따라서, 현재 표적 AS로 발생되는 이벤트의 임의성은 결여되어 있다고 판단할 수 있다. 그림 13은 전체 stub AS 중 10%를 무작위로 선택해 국내 AS 4008을 표적 AS로 설정한 후, 발생되는 이벤트를 조사하였다. 모의실험 시간은 앞에서 설명한 바와 같이 그림 11의 모의실험 이벤트 수와 동일하게 하였다. 그림에서 확인할 수 있는 바와 같이 식 (1)을 통해 우리가 예상할 수 있는 이벤트 수의 분포를 모니터링 AS 노드가 검출하였으며, 따라서 현재 발생되고 있는 이벤트가 전체 stub AS를 대상으로 지리적으로 광범위하게 발생되고 있음을 판단할 수 있다.

4. 결 론

본 논문은 AS-레벨 라우팅 패스 토폴로지의 특성과 AS 노드의 하위 스트림 AS 분포를 비롯한 AS-레벨 링크 분포를 조사하였다. 기존 AS-레벨 토폴로지에 관한 연구들은 대부분 정확한 토폴로지 생성 방법과 노드 차수 등과 같은 물리적 토폴로지 특성 분석에 초점이 맞추어져 왔다. 또한, 인터넷 power-law 특성 연구 결과들은 매우 흥미로운 사실이긴 하나 실제 그 응용 사례가 극히 부족하다. 따라서, 본 논문에서는 기본적인 BGP 라우팅 정책이라고 할 수 있는 '밸리-프리' 정책을 적용한 AS-레벨 라우팅 패스 토폴로지에 근거해 라우팅 홉-수 분포 등을 알아 보았다. 이를 간략히 요약하면 다음과 같다.

- 2009년 8월 9일자 실제 AS-레벨 인터넷 토폴로지 데이터를 활용하여 기본적으로 우리가 알고 있는 power-law특징 및 AS 노드 분포가 여전히 유지되고 있음을 재 확인하였다.
- AS 노드의 하위 스트림 AS 분포도 power-law 특성을 가짐을 확인하였다.
- 한국과 미국에 위치한 사이트를 표적 AS로 설정하고 8개의 tier1 AS와의 연결 구성을 조사하였다. 이를 통해 우리가 쉽게 예상하지 못했던 연결의 다양성을 확인할 수 있었다. 더불어, 국내 AS-레벨 계층구조가 미국에 비해 상대적으로 단순한 구조를 가졌음을 확인하였다.
- 구해진 AS-레벨 라우팅 패스 토폴로지를 기반으로 라우팅 패스 홉 수 분포를 구했다. 이미 예상한 바와 같이, 국내와 미국의 이들 분포가 약간의 차이를 보임을 확인하였다.

한편, 본 논문에서는 사회적으로 가장 큰 관심의 대상이 되고 있는 DDoS 공격에 관한 연구에 AS-레벨 토폴로지를 이용할 수 있는 방법을 모색하였다. DDoS 공격 방법은 비교적 간단하다고 할 수 있으나, 그 방법이 계속 변화하고 있어 검출을 위한 세부적인 기술은 계속 변화할 수 밖에 없다. 그러나, 본 논문에서는 DDoS 공격의 본질이라고 판단되는 특정 표적 시스템에 대한 광범위한 공격 이벤트를 검출하는 방법을 활용하였다. 즉 몇몇 모니터링 AS에서 검출되는 이벤트 수의 상대적인 비교에 의해 현재 발생되고 있는 이벤트의 임의성을 판단할 수 있는 근거를 제시하였다.

본 논문은 인터넷 토폴로지 특성을 이용해 DDoS 공격을 검출할 수 있는 가능성을 보였다. IP 주소 스푸핑(spoofing)과 같은 IP-레벨 해킹 기술과 비교해 AS-레벨 토폴로지 자체는 상대적으로 쉽게 해킹될 여지가 줄

어드는 것은 분명한 사실이다. 따라서 본 연구 결과는 DDoS 방어를 위한 새로운 접근 방법의 출발점이 될 것으로 믿는다. 본 연구팀은 AS 번호에 따른 지리적 위치를 데이터베이스화하고 웜 전파 특성[15]을 고려해 얼마나 정확하고 빠른 시간에 DDoS를 검출할 수 있으며, 얼마나 많은 모니터링 AS가 어느 곳에서 설정되어야 하는지에 관한 연구를 현재 진행하고 있다.

참 고 문 헌

[1] L. Gao, "On Inferring Autonomous System Relationships in the Internet," *IEEE/ACM Transactions on Networking*, vol.9, Issue 6, pp.733-745, 2001.

[2] B. Zhang, R. Liu, D. Massey, and L. Zhang, "Collecting the internet AS-level topology," *SIGCOMM Computer Communication Review*, vol.35, Issue 1, pp.53-61, 2005.

[3] M. Faloutsos, P. Faloutsos, and C. Faloutsos, "On Power-Law Relationships of the Internet Topology," In *Proc. of ACM SIGCOMM*, pp.251-262, 1999.

[4] Q. Chen, H. Chang, R. Govindan, and S. Jamin, "The origin power laws in Internet topologies revisited," In *Proc. of INFOCOM 2002*, 2002.

[5] R. Oliveira, D. Pei, W. Willinger, B. Zhang and L. Zhang, "In Search of the Elusive Ground Truth: The Internet's AS-level Connectivity Structure," In *Proc. of SIGMETRICS'08*, 2008.

[6] R. Oliveira, D. Pei, W. Willinger, B. Zhang and L. Zhang, "Quantifying the Completeness of the Observed Internet AS-level Structure," *Technical Report TR-080026, Computer Science Department UCLA*, 2008.

[7] RIPE routing information service project, available at http://www.ripe.net

[8] Route Views routing table archive, available at http://routeviews.org

[9] UCLA IRL Internet Topology Collection, available at http://irl.cs.ucla.edu/topology

[10] J. Winick, S. Jamin, "Inet-3.0: Internet Topology Generator. Technical Report, Department of EECS, University of Michigan, 2002.

[11] C.D. Murta, J.N. Maciel, NIT: The New Internet Topology Generator. Technical Report, Department of Informatics, University Federal of Parana, 2008.

[12] K. Park and H. Lee, "On the effectiveness of route-based packet filtering for distributed DoS attack prevention in power-law Internets," In *Proc. of ACM SIGCOMM*, pp.15-26, 2001.

[13] 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.

[14] W. Lu, M. Tavallaee, and A.A. Ghorbani, "Automatic Discovery of Botnet Communities on Large-Scale Communications Networks," In *Proc. of ASIACCS'09*, 2009.

[15] C. Zou, W. Gong, and D. Towsley, "Code Red Worm Propagation Modeling and Analysis," In *Proc. of CCS'02*, 2002.

[16] I.V. Beijnum, *Building Reliable Networks with the Border Gateway Protocol*, O'Reilly, 2002.

[17] M. Roesch, "Snort Lightweight Intrusion Detection for Networks," In *Proc. of USENIX LISA'99*, pp.101-109, 1999.

[18] M.V. Mahoney, "Network Traffic Anomaly Detection Based on Packet Byte," In *Proc. of SAC 2003*, pp.346-350, 2003.

[19] L. Feinstein, D. Schnackenberg, R. Balupari, and D. Kindred, "Statistical Approaches to DDoS Attack Detection and Response," In *Proc. of DISCEX'03*, 2003.

강 구 홍

1985년 경북대학교 전자공학과 졸업(공학사). 1990년 충남대학교 전자공학과 졸업(공학석사). 1998년 포항공과대학교 전자계산학과 졸업(공학박사). 1985년~1993년 한국전자통신연구원 선임연구원. 1998년~1999년 한국전자통신연구원 선임연구원. 2008년~2009년 Purdue University Visiting Scholar. 2000년~현재 서원대학교 정보통신공학과 부교수. 관심분야는 성능평가, 컴퓨터 네트워크, 네트워크 보안

이 희 만

1984년 고려대학교 전자공학과 졸업(공학사). 1986년 한국과학기술원 전기 및 전자공학과 졸업(공학석사). 1994년 Texas A&M Electrical Eng. 졸업(공학박사). 1996년 3월~현재 서원대학교 멀티미디어공학과 교수. 관심분야는 가상현실, 멀티미디어, 컴퓨터그래픽스

김 익 균

1994년 경북대학교 컴퓨터공학과 졸업(공학사). 1996년 경북대학교 컴퓨터공학과 졸업(공학석사). 2009년 경북대학교 컴퓨터공학과 졸업(공학박사). 2000년~2001년 ㈜팍스콤 선임연구원, 2004년~2005 Purdue University 객원연구원. 2001년~현재 한국전자통신연구원 책임연구원. 관심분야는 네트워크 보안, 컴퓨터네트워크

오 진 태

1990년 경북대학교 전자공학과 졸업(공학사). 1992년 경북대학교 전자공학과 졸업(공학석사). 1992년~1998년 한국전자통신연구원 선임연구원. 1998년~2002년 Winnow Tech. in USA Cofounder, CTO, and VP. 2003년~현재 한국전자통신연구원 책임연구원. 관심분야는 네트워크 보안, DDoS 탐지기술

장 종 수

1984년 경북대학교 전자공학과 졸업(공학사). 1986년 경북대학교 전자공학과 졸업(공학석사). 2000년 충북대학교 컴퓨터공학과 졸업(공학박사). 2000년~2003년 한국전자통신연구원 네트워크보안구조팀 팀장. 2004년~2008년 한국전자통신연구원 그룹장. 1989년~현재 한국전자통신연구원 책임연구원. 2006년~현재 대검찰청 디지털수사자문위원회 위원. 2007년~현재 OSIA 이사. 2008년~현재 방송통신위원회 인터넷정보보호협의회 안전인터넷분과 위원. 관심분야는 네트워크 보안, 정책기반 보안관리기술