플로 기반의 인터넷 트래픽 측정 기술 동향

Flow-Based Internet Traffic Measurement Technologies

박정숙(J.S. Park) IP네트워킹기술팀 선임연구원
윤승현(S.H. Yoon) IP네트워킹기술팀 선임연구원
윤상식(S.S. Yoon) IP네트워킹기술팀 선임연구원
정형석(H.S. Chung) IP네트워킹기술팀 선임연구원
이병준(B.J. Lee) IP네트워킹기술팀 연구원
최태상(T.S. Choi) IP네트워킹기술팀 선임연구원
정태수(T.S. Jeong) IP네트워킹기술팀 책임연구원, 팀장

인터넷 망 규모의 지속적인 확장, 다양한 응용 서비스의 제공, 인터넷 트래픽의 증가 등으로 인해 복잡해진 인터넷 특성의 이해와 규모 예측은 주로 측정에 의존한다. 또한 인터넷이 단순한 최선형 서비스에서 품질형 비즈니스 서비스 제공으로 진화됨으로 인해 QoS, 과금, SLA 등이 중요한 요구사항이 되면서, 측정 기술의 중요성이 더욱 부각되고 있으며 그에 대한 연구도 활발히 이루어지고 있다. 본 고에서는 그 측정 기술 중 하나로, 최근 가장 활발히 연구되고 있는 플로 기반 측정 기술의 현황 및 향후 발전 방향을 살펴보고자 한다.

I. 도 입

인터넷은 태동 이후 짧은 시간 동안 많은 발전을 이루었으며, 최근 인터넷이 차세대 통신망의 인프라로 대두되면서 이에 필요한 많은 연구와 기술 개발이 이루어지고 있다. 이에 따라, 인터넷은 단순한 최선형의 서비스에서 벗어나 품질형 비즈니스 망으로 진화하고 있고 망도 대규모화되고 있다. 그러나 다양한 응용 서비스의 지속적인 제공, 인터넷 사용자 증가 등은 망의 고속화뿐만 아니라 인터넷 트래픽의 특성을 보다 복잡하게 만들어서 측정 기술을 필수적으로 요구하고 있다[1].

지금까지 망에서 사용된 트래픽 측정 방식은 주로 장치 내의 MIB 정보를 이용해서 각 회선의 사용률을 모니터링하거나 이를 약간 보완한 수준의 방식들로, 회선별 또는 장치별 트래픽의 규모를 측정하거나 간단한 분석 결과를 제공해 주는 용도로 사용되어 왔다. 그러나 앞서 언급했던 인터넷 환경의 급속한 변화로 인해 기존 방법으로는 인터넷 망의 특성을 이해하기에는 부족하며, 특히 국부적인 성능보다는 종단간 성능에 대한 이해를 요구하므로 기존에 사용되던 방법과는 다른 진보된 측정 방법이 필요하게 되었다.

인터넷 망에서 트래픽 측정은 망 초기 단계의 설계 및 계획, 운영 단계의 트래픽 엔지니어링을 위해 수행해야 할 작업일 뿐만 아니라, 향후 고품질 인터넷 서비스, 종량제 과금(usage-based billing), SLA (Service Level Agreement), QoS 제어, 보안 등의 제공을 위해서도 중요한 역할을 한다[2],[3]. 따라서 측정 기술은 망의 고속화, 대규모화, 응용의 다양화, 품질의 고도화, 유해 트래픽, 망 이상 유무 등에 대응해야 하며, 응용에 따라서 다른 수준의 정밀성을 제공하여야 한다.

이러한 방향에서 활발히 연구되고 있는 방식이 플로(flow)에 기반한 인터넷 트래픽 측정 방식이다. 이 방식은 수집한 패킷들을 플로(공통된 특성을 가지는 패킷들의 집합)로 가공함으로써 측정량을 줄임과 동

시에 위에서 언급한 서비스들을 제공 가능하게 한다.

본 고에서는 플로 기반 측정 기술 동향을 통하여 인터넷 측정 기술의 전반적인 현황과 앞으로의 발전 방향에 대해 살펴보고자 한다.

본 고의 구성은 다음과 같다. 제 II장에서는 현재의 측정 기술을 분류하고 유용한 툴들, 표준화 현황, 측정 활동들을 소개한다. 제 III장에서는 패킷 기반 측정 방법의 한계점을 극복하기 위한 방안으로 새로이 부각되어 활발히 연구되고 있는 플로 기반 측정 기술에 대해 기술한다. 제 IV장에서는 플로 기반 측정 기술에서의 문제점과 이를 해결하기 위한 다양한 노력들을 소개하고, 제 V장에서는 측정 기술의 향후 발전 방향에 대해 기술한다.

Ⅱ. 측정 기술

1. 측정 목적

인터넷에서의 측정은 트래픽 특성 분석, 망 모니터링과 지속적인 운용, 망 제어, 망 이상 유무 탐지 등 다양한 목적을 위해 사용된다. ISP, 단말 사용자, 라우터 업체 등 인터넷 사용자 별로 관심 있는 목표와 이에 따른 측정 항목들이 약간 다른데, 그 요구사항들을 간략히 분류해 보면 <표 1>과 같다[4].

<표 1> 사용자 별 측정 요구사항

	ISP들	사용자들	업체들
목표	- 용량설계 - 부가가치 서비스 - 종량제 과금 - TE - 망 설계	- 성능 모니터링 - 업그레이드 계획 - 서비스 계약 협상 - 사용자 기대치 설정 - 콘텐츠 전송 최적화 -사용량 policing	- 설계 및 설치 장비 개선 - 실시간 디버깅 및 하드웨어 진단 구현
측정 항목	- 대역폭 이용률 - pps - RTT - RTT 편차 - 패킷 손실 - 도달 가능성 - 회선 성능 - 라우팅 진단	- 대역폭 유효성 - 응답 시간 - 패킷 손실 - 도달 가능성 - 연결률 - 서비스 품질 - 호스트 성능	- 샘플 추적 - 로그 분석

2. 측정 방식

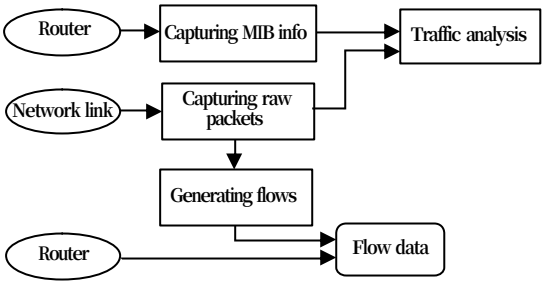
현재까지 인터넷 망에서는 다양한 측정 방법들이 연구 및 사용되고 있다[5] - [9]. 이는 각기 다른 목적을 위해서 고안된 방법들로써, 정리하면 몇 가지 기준에 따라 분류 가능하다[9],[10].

대표적으로, 측정 방식은 능동(active) 측정 방식과 수동(passive) 측정 방식으로 분류할 수 있다[11],[12].

능동 측정 방식은 테스트 패킷이나 응용들을 발생시키고 망의 성능을 관찰하는 방식을 의미한다. 대표적으로 망의 성능 척도와 측정 구조에 관해서는 IETF 내의 IPPM(IP Performance Metrics) WG에서 정의, 제시하고 있는데, 그 성능 척도로는 지연, 패킷 손실, 가용성 등이 있다[13]. 능동 방식은 망에 부가적인 트래픽을 발생시킴으로써 망의 성능을 저하시킬 가능성이 있으며, 인터넷 망의 동적인 라우팅 특성 때문에 측정 성능이 실제 망의 성능보다 더 우수하게 또는 더 저하되어 나타날 수 있는 단점이 있다.

또한 능동 측정 방식은 단방향성과 양방향성으로 구분할 수 있다. 그러나 인터넷 망의 비대칭적인 구조적 특성 때문에 단방향 측정을 필요로 하는 경우가 많은데[14], 이러한 경우에는 패킷을 발생시킨 시스템과 패킷을 수신하는 시스템 사이의 시각 동기화가 필요하다. 능동 방식을 더 세부적으로 분류하면 계층 4에 따라 용도가 약간 달라질 수 있다. TCP 기반은 주로 대역폭을 구하기 위해 많이 사용하고, UDP는 단방향 패킷손실, 왕복 대역폭 등을 구하는데 사용되며, ICMP 기반은 망의 가용성, 왕복지연시간, 왕복 패킷 손실 등을 구하는 데 사용된다. 능동 측정 방식의 툴은 Ping, Traceroute, Surveyor, Netperf, Skitter 등이 있다[15].

수동 측정 방식은 추가적인 패킷 발생없이 망에 흐르는 트래픽을 수집하고 그 트래픽의 특성을 분석하는 방식이다. 이의 용도는 망의 사용량 변화, 패킷 분석을 통한 망 제어, 트래픽 사용량 측정, 용량 설계, 인터넷 트래픽 특성 분석 등에 이용하기 위한 것이다. 수동 측정 방식은 (그림 1)과 같이, 라우터 등



(그림 1) 수동 측정 방식

망 장비로부터 수집하는 방식과 측정 장비를 투입하여 회선으로부터 수집하는 방식으로 나뉠 수 있다. 후자의 경우에 수집된 패킷들은 바로 분석을 수행하거나, 플로의 형태로 다시 가공한 후 분석할 수 있다. 수동 측정 방식에는 SNMP MIB를 통한 링크 트래픽량 측정, NetFlow와 같은 라우터에 탑재된 플로 생성 툴을 통한 플로 기반 트래픽 측정이 대표적이다. 그러나 이 방식은 프라이버시(privacy) 침해 가능성 등의 문제점이 있을 수 있으며, 대용량 데이터의 발생으로 인해 분석에 많은 자원을 필요로 하고 망 고속화에 대한 대응이 쉽지 않은 단점이 있다.

수동 측정의 성능 척도는 주로 처리력(throughput), 트래픽 패턴, 이용률 등이다. 이를 위한 툴은 tcpdump, MRTG, OC3MON, NetFlow, NetraMet 등이 있으며, ETRI가 개발한 NetFlow 정보를 이용하여 ISP의 실시간 트래픽 매트릭스를 구하는 TMS(Traffic Measurement System) 툴을 포함하여 다양한 분석 툴과 수집장치(probe)들이 존재한다.

보다 많은 측정 툴에 관한 정보는 CAIDA 사이트를 참고할 수 있다[15].

또 다른 측면에서, 측정 방법은 측정 시점에 따라서 상시 측정과 수시 측정으로 나눌 수 있는데, 향후 고기능 서비스를 위해서는 항상 트래픽을 모니터링하고 분석을 수행하는 상시 측정이 이루어져야 한다.

최선형 인터넷에서는 인터넷 응용 트래픽의 상세한 분석을 위한 방법으로 회선에서 패킷을 수집하고 이를 오프라인으로 분석하는 방법을 많이 사용해 왔다[8],[11]. 이는 임시로 측정 장비를 망에 장착하여 일정 기간 동안 트래픽을 수집하고 차후 분석을 통해서 트래픽 특성을 분석하는 것으로, 주로 연구나 장기적인 측면의 망 설계에 필요한 정보를 얻기 위해서 사용되었던 방법이다. 그러나 앞으로 상시 측정이 요구되면, 분석 결과도 준 실시간으로 제공되어야 하기 때문에 측정과 분석이 동시에 수행되어야 할 필요성이 대두되고 있다.

이와 같이 인터넷에서 상시 측정 및 실시간 분석이 요구되면서 샘플링 기법[16]이나 플로 기법[17] 등을 통하여 데이터 양을 줄이고 분석 시간을 짧게 하려는 노력들이 이루어지고 있다[18].

3. 측정 활동

현재 CAIDA, NLANR 등을 위주로 하여 인터넷 측정과 관련한 다양한 활동들이 진행중이다.

가. CAIDA

CAIDA(the Cooperative Association for Internet Data Analysis)[15]는 인터넷 인프라에 대한 엔지니어링 및 관리를 촉진시키는 툴과 분석을 제공한다. CAIDA는 자체적으로 개발한 툴을 제공하고 있으며 다른 곳에서 개발된 유용한 툴들을 토폴로지, 트래픽 부하, 성능, 라우팅, 멀티캐스트 등으로 분류하여 정보로 제공하고 있다. 또한 다양한 인프라 관련 프로젝트들에 대한 관련 정보들도 CAIDA에서 관련 정보들을 쉽게 얻을 수 있다.

CAIDA에서는 현재 IP 연결성 분석, BGP 연결성 분석, DNS 분석, NMS(Network Modeling and Simulation) 등 측정, 분석, 시각화에 관한 프로젝트들을 수행하고 있으며, 널리 알려진 cflowd, CoralReef, skitter, Flowscan, NetGeo 등은 CAIDA에서 개발되어 많이 활용되고 있는 툴들이다.

나. NLANR

NLANR(National Laboratory for Applied Network Research)[19]는 NSF의 지원을 받아 NSF

연결 사이트들과 NSF/MCI vBNS과 같은 HPNSP에 대한 기술, 엔지니어링, 트래픽 분석을 지원하는 기관이다. 그 중 NMS(Measurement and Analysis) 기관이 고성능 연결 사이트들을 위한 성능 및 플로 측정 기능을 수행하고 있으며, PMA(Passive Measurement and Analysis) 프로젝트, AMP(Active Measurement Project) 프로젝트를 포함하여 다양한 측정 관련 접근을 시도하고 있다.

다. RIPE

RIPE(Réseaux IP Européens)[20]는 WAN IP 망에 관심가지는 유럽 내의 모든 단체들로 구성되는 포럼으로, 유럽 지역 내의 인터넷 운용에 필요한 관리 및 기술적인 협력을 도모하기 위한 목적을 가진다. RIPE NCC는 서비스 지역 내에서 기술적인 협력을 통하여 인터넷의 인프라를 지원하는 비영리 단체로, Whois DB를 운영하고 있다. 또한 TTM(Test Traffic Measurements) 프로젝트를 통하여 인터넷 상에 존재하는 두 사이트 간의 연결성과 관련한 척도들을 측정하여 지원 단체에 그 결과를 제공하고 있다.

이 외에도 유럽에서 수행하는 측정 관련 프로젝트들은 TEQUILA 프로젝트, INTERMON 프로젝트 등이 있다. 특히 INTERMON은 IPFIX의 플로 개념과 능동 성능 측정 방식을 결합하여 대규모 네트워킹을 위한 트래픽 측정 및 모델링을 수행한다.

라. CANARIE

CANARIE(Canadian's Advanced Internet Development Organization)[21]는 캐나다의 인터넷 개발을 가속화하고, 차세대 제품, 응용, 서비스들을 위한 고속 백본 네트워크를 제공, 운영하기 위해 만들어진 비영리 단체이다. 망은 현재 CA*net3를 거쳐 CA*net4 단계에 있으며, CA*net4를 통하여 지방의 연구망을 상호 연결하고 그것을 통해 정부연구소, 대학교 등을 상호 연결해 주거나 국제 피어망과 연결해 준다. 현재 거의 대부분이 OC-192(10Gbps)의 속도로 연결되어 있다.

측정 툴은 CA*net3 Traffic Map이 대표적이며, 이는 MRTG, cflowd에 기반한 트래픽 레벨의 상황을 보여주는 것 외에도 Flowscan, CoralReef 및 AMP 툴에 기반한 트래픽 데이터를 제공하고 있다.

마. Internet2

Internet2[22]는 미국 내의 200개 이상의 대학에 의해 주도되는 협회로서, 망 응용들과 기술들을 개발하고 적용하기 위한 목적을 가진다. Abilene, the Quilt, ARENA 등의 연구교육망을 보유하고 있으며, 이들 상에서 IPv6, 멀티캐스트, 보안, 토폴로지 등과 관련된 다양한 연구를 수행하고 있다. 현재 측정과 관련해서 인터넷 망의 종단간 성능을 측정하기 위한 E2Epi 프로젝트 등이 진행되고 있으며, OWAMP, BWCTL 등의 측정 관련 툴을 개발하여 사용하고 있다.

바. 기타

Sprint에서도 IPMON(IP Monitoring) 프로젝트를 통하여 측정활동을 수행하고 있으며[23], 일본에서는 GENESIS 프로젝트를 통하여 차세대 장비, 프로토콜, 응용 등의 개발을 위한 트래픽 측정 연구를 수행하고 있다[24].

4. 표준화

인터넷 트래픽 측정과 관련한 표준은 현재 IETF를 중심으로 활발히 이루어지고 있다.

가. IPPM WG

IPPM(IP Performance Metrics)[25]은 인터넷 데이터 전달의 품질, 성능, 신뢰성에 적용할 수 있는 표준 척도 및 측정 구조를 개발하는 WG이다. 이 척도들은 망 운용자, 단말 사용자나 독립적인 테스팅 그룹에 의해 수행될 수 있도록 설계되고 있다. 그룹에서 설계하고 있는 성능 척도로는 연결성(connectivity), 단방향 지연 및 손실(one-way delay

and loss), 왕복 지연 및 손실(round-trip delay and loss), 지연변이(delay variation), 손실 패턴(loss patterns), 패킷 재정렬(packet reordering), 큰 전달 용량(bulk transport capacity), 링크 대역폭 용량(link bandwidth capacity) 등이 있다. 이 그룹의 작업 중 일부는 BMWG(Benchmarking WG)와도 관련성이 있다.

나. IPFIX WG

IPFIX(IP Flow Information Export)[26]는 IP 플로 정보를 만들어 내는 시스템(예를 들면, 라우터)들에 대해 공통적인 구조 및 방법을 표준화하기 위해 활동하는 그룹이다. 이 WG은 생성된 플로 데이터를 분석 시스템으로 보내기 위한 데이터 포맷과 전달 프로토콜에 대한 작업들을 2001년부터 활발히 진행하여 많은 부분이 표준화되어 가고 있다. 표준 IP 플로를 정의하고, IPv4/IPv6 유니캐스트 및 멀티캐스트 플로의 분석을 지원하는 데이터 암호화 고안, 패킷 샘플링에 기반한 IP 플로 정보 전달의 개념 고려, 보안 프라이버시 문제, 신뢰성있는 시스템임을 보장하는 방법 등이 IPFIX 표준화 그룹의 목표이다.

다. PSAMP WG

PSAMP(Packet Sampling)[27]는 망 요소들이 통계적이거나 다른 방법들에 의해 패킷의 일부를 샘플링하기 위한 기능들에 대한 표준을 정의한다. 패킷이 샘플링되는 데 필요한 선택 동작들을 명시, 샘플링된 패킷들에 관한 보고를 위해 사용 가능한 정보 명시, 샘플링된 패킷들을 응용들에게 보고하는 데 필요한 프로토콜, 패킷 선택과 보고를 위해 필요한 프로토콜 기술을 표준화하는 것이 PSAMP에서 하는 역할이다. IPFIX의 샘플링 작업은 PSAMP와 많은 관련성을 가진다.

Ⅲ. 플로 기반 측정 기술

전술한 바와 같이, 앞으로 인터넷의 상세한 트래픽 측정 및 분석을 필요로 하는 응용들이 많다. 그러나 단순한 패킷 기반 측정 방법으로는 이에 대응하기가 어려우며, 따라서 이를 해결하기 위한 많은 방법들이 제안 도입되고 있다. 그 대표적인 방법으로는 필터링(filtering), 플로 기반(flow-based) 측정, 샘플링 등이 있다.

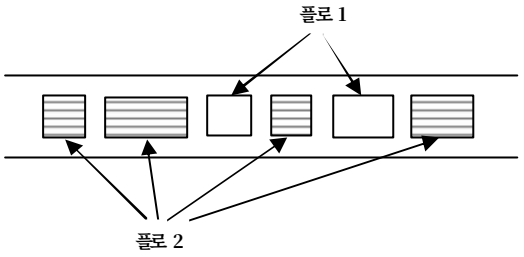
이 중 현재 가장 큰 이슈로 떠오르고 있는 것이 플로 기반 측정 방법이다. 플로 기반 측정 방법은 동일한 소스 및 목적지를 가지는 패킷들을 플로라는 개념으로 묶음으로써 패킷 자체를 수집하는 것보다는 3~4배 이상으로 측정량을 줄이면서 정보 손실을 최소화하는 방법이다.

이러한 플로 기반의 측정 방법에 기반하여 사용량 기반 과금, 트래픽 엔지니어링, 트래픽 프로파일링, QoS 모니터링, 라우팅 이상 탐지, 공격 탐지 및 분석, 침입 탐지 등의 연구 및 기술 개발이 활발히 진행되고 있다.

플로 기반 측정 기술을 탑재한 라우터들이 많이 있으며 앞으로 표준이 확정되면 모든 라우터, 스위치에는 플로 기반 측정 기술이 도입될 것이다. 현재까지 시스코의 NetFlow가 가장 많이 알려져 있으며, 주니퍼 역시 시스코의 NetFlow와 동일한 형태로 플로 포맷을 지원하고 있다. Riverstone은 LFAP(Lightweight Flow Accounting Protocol)이라는 독자적인 플로 기반 측정법을 사용하고 있다. In-Mon 등에서는 프로브 형태로 플로 측정 툴을 제공하고 있어 라우터에 플로 측정 기능이 없는 경우에 활용할 수 있다[28]-[32]. 이 중 시스코 라우터에서 제공되는 NetFlow 기능이 사실상 업계 표준으로 인식되고 있으며, 최근 IETF의 IPFIX WG에서도 사실상 시스코의 NetFlow v9을 기준으로 표준화가 마무리되어 가고 있는 상황이다[26],[28].

1. 플로 생성 및 분석 방법

IP 플로는 (그림 2)와 같이 어떤 특정한 기간동안 망 내의 한 관측점을 지나는 공통된 특성을 가지는 IP 패킷들의 집합으로 정의된다[26]. 이러한 플로의 정의는 패킷 헤더 내에 나타난 것만으로 구성될



(그림 2) 플로 개념

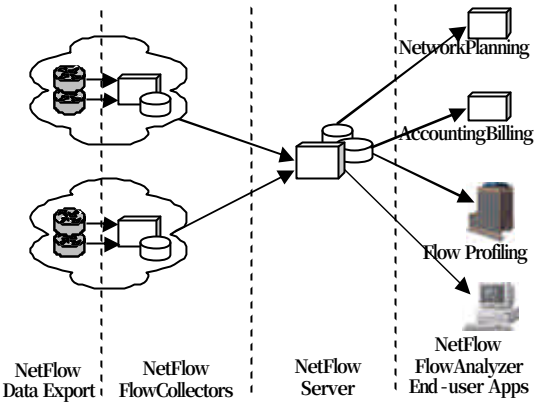
수도 있고, 그 패킷으로부터 유추 가능한 정보가 플로 속성이 될 수 있다. 이러한 속성에는 AS, 국가, 서브넷, next-hop, TOS 등이 포함되어 있다.

IP 플로 생성 방법은 일반적으로 플로 종료 방법 또는 플로 지속시간에 따라 몇 가지로 나눌 수 있다. IP 패킷은 TCP의 경우와 같이 FIN, RST 등 명백한 종료 패킷이 존재하는 경우도 있지만, UDP나 ICMP와 같이 명백한 종료 패킷이 존재하지 않는 경우도 있다. 또한 그런 종료 패킷의 존재 유무와는 상관없이 플로 지속 시간이 너무 길어서 강제적으로 플로를 종료해야 하는 경우도 있다. 이러한 특성들을 고려하여 인액티브(inactive) 타임아웃, 액티브(active) 타임아웃 등 몇 가지 타임아웃 메커니즘을 사용하고 있다.

플로 정보를 분석하기 위한 방법은 단기간(short-term) 측정, 장기간(long-term) 측정으로 구분해 볼 수 있다. 단기간 측정은 트래픽 플로의 통계적인 행동에 관한 특성으로, 이는 자원 관리, 트래픽 제어, 트래픽 셰이핑 등을 위해 사용된다. 장기간 측정은 주로 망 토폴로지에 관련되는 트래픽 플로의 패턴을 연구하는 것으로써, 망 설계나 계획 등을 위해 사용된다. 또한 이들을 함께 고려하는 방법도 사용될 수 있다.

2. 시스코의 NetFlow

NetFlow를 이용한 측정 시스템의 구조는 (그림 3)과 같다. 즉, 라우터에서 NetFlow를 이용하여 플로로 가공된 트래픽 정보를 UDP 패킷에 담아 보내주면(exporter), 수집기(collector)에서는 이들 플로 데이터를 수집하여 분석 서버로 보내고, 분석 서



(그림 3) NetFlow 시스템의 구조

버는 이러한 정보를 가공하여 특정 응용에 필요한 정보를 생성해 낸다.

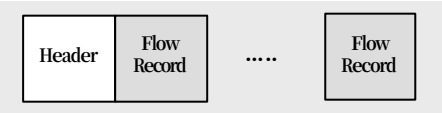
NetFlow에서 사용하는 플로는 기본적으로 {SrcIP, DstIP, SrcPort, DstPort, Protocol, TOS, InputIf} 등의 7-튜플에 의해 식별되며, 단방향성을 가진다. 개별 플로는 식별자 외에도 그 플로의 시작 시각 및 지속 시간, 패킷량과 바이트량을 가지는 구조로 되어 있다.

현재 NetFlow는 이러한 플로 정보에 대해 v1, v5, v7, v8, v9 등의 데이터 포맷을 제공하고 있다. (그림 4(a))는 NetFlow에서 제공하는 데이터 포맷 중 v1과 v5의 구조를 나타낸다. 첫번째 버전인 v1에 비해 현재 가장 보편적으로 사용하고 있는 v5는 주소 및 포트 외에 AS 번호(또는 인접 AS 번호), 네트워크 주소, 인터페이스, TOS 등의 필드들을 모두 사용하므로, 용도에 따라 유용한 정보를 제공할 수 있다[34]. V8은 v5에서 AS, 프로토콜 포트, 서브넷 매트릭스 등 사용자가 원하는 정보만을 얻을 수 있도록 라우터에서 미리 aggregation하여 보내주므로 데이터의 양을 줄일 수 있지만, 그 외의 데이터는 손실되는 단점도 있다. 현재 11개의 aggregation 기법을 제공한다.

그러나 v5, v8 등의 데이터 포맷은 레코드 내의 필드들이 고정되어 있어서 유연성과 적응성이 떨어지며, 이러한 특성은 사용자가 새로운 필드 추가를 요구할 때마다 새로운 버전을 만들어야 한다는 단점이 있다. 따라서 시스코에서는 NetFlow에서 생성하

Field	v1	v5
Source IP address	*	*
Destination IP address	*	*
Source app port	*	*
Destination app port	*	*
Next hop IP address	*	*
Input interface index	*	*
Output interface index	*	*
Packet count for this flow	*	*
Byte count for this flow	*	*
Start of flow timestamp	*	*
End of flow timestamp	*	*
IP protocol	*	*
TOS	*	*
TCP flags	*	*
Source AS number		*
Destination AS number		*
Source subnet mask		*
Destination subnet mask		*

(a) 플로 레코드 포맷



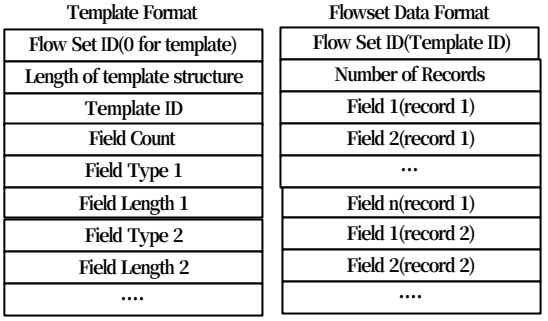
(b) 플로데이터 전송 포맷

(그림 4) NetFlow 데이터 포맷(v1, v5)

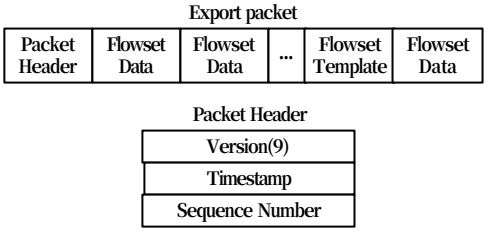
는 데이터가 좀더 넓은 범위의 응용들을 위해 사용될 수 있도록 v9 버전을 만들고 있다. V9에서는 (그림 5)와 같이 사용자가 원하는 필드들을 미리 템플릿으로 만들고 이 구성에 맞추어 실제 플로 데이터 정보를 라우터에서 보내주는 방식을 사용한다.

NetFlow에 의해서 생성된 플로 데이터는 시스코의 Flow Collector나 NetFlow를 지원하는 툴에 의해서 수집, 분석이 가능하다. 이러한 분석 패키지는 ISP나 망 엔지니어가 용량 설계, 추세 분석, 과금 및 트래픽 부하의 특성을 파악할 수 있도록 데이터 수집 및 분석 기능을 제공한다.

수집 및 분석 툴의 대표적인 한 가지 예는 CAIDA에서 개발한 cflowd이다[15]. Cflowd는 NetFlow 포맷의 데이터를 수신하여 입력 인터페이스 번호에 따른 AS 별, 프로토콜별, 포트별, 서브넷별 트래픽



(a) 템플릿 포맷과 데이터 포맷



(b) 플로 데이터 전송 포맷

(그림 5) NetFlow 데이터 포맷(v9)

량을 시간 단위별로 구하고 파일에 저장하는 기능을 한다. 또 다른 툴인 Flowscan과 Flowscan+는 cflowd의 파일 분석을 통하여 인터넷 응용의 변화량을 그래프를 사용하여 실시간으로 사용자에게 보여준다. Flow-tools 역시 NetFlow 데이터들을 수신하여 처리, 분석 보고서를 만들어 내는 유용한 툴로서, 다양한 분석 기능을 제공한다.

3. 제품 동향

플로 기반 측정과 관련한 시장은 NetFlow를 지원하는 형태로 나아가고 있다. 전술했듯이, IPFIX WG에서도 NetFlow v9을 기본 모델로 채택함에 따라 이러한 수용 경향은 라우터나 측정 및 분석 툴 개발에서 점점 일반화되고 있는 추세이다. 라우터 업계 중에서는 기존의 시스코, 주니퍼 외에 Extremet 사에서도 NetFlow 기능을 지원한다[33]. 향후에는 대부분의 라우터에서 IPFIX 표준을 따르는 플로 export 기능 또는 NetFlow 기능을 지원할 것으로 예측된다.

NetFlow 기반 측정 툴 개발 현황을 이해하기 위해 <표 2>~<표 4>를 통하여 공개용 NetFlow 수집

기 및 분석기, NetFlow 수집장치, NetFlow 기반 상용 분석 도구들을 조사하였다. <표 2>는 공개용 NetFlow 수집기 및 분석기를 나타낸다. 이는 라우터로부터 플로 데이터를 수집해서 분석하는 도구들이다. 전술한 바와 같이 cflowd, flow-tools, flow-scan, flowscan+ 등이 대표적이다.

<표 3>은 플로 레코드를 생성하는 수집장치들을 나열하였다. 이들의 도구 역시 대부분 플로 export 형태는 NetFlow와 동일한 형태를 지원하고 있다. Nprobe, flowprobe 등이 대표적이며, 특히 Nprobe는 IPFIX 표준 포맷 및 NetFlow 포맷을 모두 지원한다[34].

<표 4>는 상용으로 개발되고 있는 NetFlow 분석 도구들이다. 시스코 사의 Flow Collector, Flow Analyzer 외에 다양한 분석 도구들이 존재한다. 우리나라에서도 삼성의 UNINMS, 네비스텍의 Isee-Flow, IfeelNet의 I-flow 등 NetFlow와 관련한 제품들이 있다.

Ⅳ. 플로 기반 측정 기술의 발전 방향

본 장에서는 플로 기반 측정 방식에 있어서 해결해야 할 기술적인 문제들에 대해 조사하고, 그 중 플로 기반 측정 기술에 있어서의 응용 식별 문제와 그 해결 방안에 관한 연구 결과를 소개한다.

1. 연구 방향

현재 플로 기반 측정 방식의 주요 연구 방향은 크

<표 2> 공개용 NetFlow 수집기 및 분석기

Name	Information	Source
Cflowd	Collection, storage, basic analysis	http://www.caida.org
EHNT(the Extremely Happy NetFlow tool)	Collection, storage, simple report	http://ehnt.sourceforge.net
FLAVIO(Flow Loader and Virtual Information Output)	Graph generation, Using NetFlow collector	http://flavio.sourceforge.net
Flow-tools	Collection, storage, scanning, convert, export, basic report analysis	http://www.splintered.net/sw/floo-tools
Flowscan	Collection using cflowd, storage, graph with RRDtool	http://net.doit.wisc.edu/~plonka/FlowScan
Flowscan+	Collection using modified cflowd, storage(mysql), graph	http://203.230.7.89
MHTG	Collection, storage(mysql), traffic graph per host	http://mhtg.the.net/mhtg.html
Flowc	Collection, storage, analysis, report generation, accounting per host	http://netacad.kiev.ua/flowc
NetFlowNet	Build RTFM flow data from NetFlow data	http://www.caida.org

<표 3> NetFlow 수집장치(probe)

Name	Information	Source
NetFlow Probe(using PCAP library)		
Softlowd	Support NetFlow v1	http://www.mindrot.org/softflowd.html
Flowprobe	Support NetFlow v1, v5, v7	http://fprobe.sourceforge.net
Fprobe	Support NetFlow v5	http://psi.home.ro/flow
Nprobe	Support NetFlow v5	http://www.ntop.org.nProbe.html
Others		
Panoptis	Detect DOS/DDOS attacks	http://panoptis.sourceforge.net
Coralreef	Off-line flow generator, analysis(using libpcap)	http://www.caida.org

<표 4> NetFlow 기반 분석 도구

Name	Information	Source
Netflow FlowCollector	NetFlow services data export feature on Cisco routers	http://www.cisco.com
Netflow FlowAnalyzer	Network analysis tool	http://www.cisco.com
ReporterAnalyzer	Application/link/host analysis, report. Supprt NetFlow, netscout probe, netIQ agent	http://www.netqos.com
NetFlow monitor	Collection, analysis	http://www.crannog-software.com/netflow.html
lsarFlow	Protocol/QoS/location/trend analysis, accounting, report	http://www.isarflow.de
Traffic server	Thresholds and alarms, congestion, SLA monitoring, traffic profiling trending	http://www.inmon.com
Netcool/USB	Collection, filtering, aggregation	http://www.micromuse.com
Ngenius Probe Performance manager	Collection, monitoring, planning, troubleshooting	http://www.netscout.com
Bandwidth manager	Billing	http://www.rodopi.com
UNINMS	Traffic analysis	http://www.uninms.co.kr/UniWeb/feature
lseeFlow	NetFlow data collection, real-time protocol analysis, application monitoring, report	http://www.nevistec.co.kr/product/pronsol 01 02 04.htm
i-flow	Collection, analysis, traffic analysis, report	http://www.ifeelnet.com/solution/iflow.htm
netflowMonitor	Collection, per-IP traffic analysis, real-time protocol analysis, TOP user, AS analysis, report	http://www.netmax.co.kr/products/main/productsmain4.asp
Bora MSP Service	NetFlow data collection, analysis	http://www.bora.net/boramsp

게 다음과 같이 5가지로 요약할 수 있다[35].

• 유연한 플로 모니터링

플로 측정을 요구하는 망 보안성, TE, 실시간 QoS 및 SLA 모니터링, 트래픽 예측 등의 응용들은 각각 다른 수준의 정밀성을 요구하는데, 이를 수용하기 위한 유연한 플로 측정 기술이 필요하다. 사용량에 민감한 응용 등에 적용하기 위해 플로들의 임계치를 정하고 그 임계치를 초과하는 응용들만 샘플링하기 위한 최적의 샘플링(optimal sampling) 방법에 대한 연구나, TE를 위해 플로의 "elephants and mice" 현상에 대한 연구 등이 유연한 플로 모니터링에 대한 예이다.

• 확장 가능한 플로 모니터링

고속 링크에서도 플로 측정 기술이 사용 가능하기 위해서 플로 기반 측정 기술은 확장성을 가져야 하는데, 이러한 문제점을 해결하기 위해서 샘플링 기법, 플로 처리를 위한 효율적인 저장 및 알고리듬적인 접근법, 처리되는 플로 수를 줄이는 개념에 기반을 둔 기법들, 트래픽 측정 모듈의 구현 최적화 등이 연구되고 있다.

• 실시간 분석, 진단 및 예측

인터넷에서 실시간 분석, 진단 등을 요구하는 응용들이 많아지면서 이에 관한 연구도 활발히 이루어지고 있는데, 자동화된 보고서 생성 기능을 가지는 알고리듬들, 예측 기능(모델링)을 사용한 측정 데이터에 대한 자동화된 추론 기능, 부가적인 모델링 정보에 기반을 둔 자동화된 트래픽 분석 및 진단 등에 관한 연구가 진행되고 있다.

• 시공간적인 플로 관측

트래픽 측정은 통신망의 제어 및 엔지니어링을 위해 중요한 요소이고, 라우팅 모델이나 망 상태에 대한 지식이 없이도 수행될 수 있어야 한다. 이러한 관점에서 현재 연구되고 있는 기술 중에는 경로 샘플링(trajectory sampling) 등이 있다.

• 자동화된 이벤트 탐지 및 패턴 분석

트래픽 측정의 목적 중 하나는 망의 이상(anomaly) 현상을 분석하기 위해 라우터와 스위치 등 망 장비를 지속적으로 모니터링하는 작업을 지원하는 것이다. 이벤트 탐지나 패턴 분석은 망의 이상 현상을 탐지하기 위한 목적으로 연구되고 있으며, 이상 그룹의 식별, 이상 그룹들의 공통된 특성들 도출, 단순한 통계치를 포함하여 다양한 기술들에 기반한 자동화된 이벤트 탐지 방법, 이상 현상을 특성화하기 위한 시계열 분석과 웨이브렛(wavelet) 분석 등이 해당된다.

2. 진보된 플로 기반 트래픽 측정 기술

플로 기반 측정 기술을 요구하는 응용들 중에서는 트래픽 특성 분석이나 사용량 기반 과금 등 정확한 응용별 분석을 요구하는 것들도 있다. NetFlow를 포함하여 현재 쓰이고 있는 플로 기반 측정 방식은 포트 번호에 기반하여 응용을 식별하는 방식으로 IANA에서 제공하는 단순한 포트 번호 매핑 정보가 활용된다. 그러나 IANA에서 제공하는 정보는 실제 상황을 반영하지 못하는 경향이 있으며, 이러한 괴리는 시간이 갈수록 늘어나는 경향이 있다.

또한 p2p와 같은 응용들은 동적 포트 번호를 할당하기 때문에 포트 번호만으로는 응용을 식별하기 힘들다. 또한 ephemeral 포트 번호에 의한 식별 오류를 야기할 가능성도 있으며, 고의적 또는 기타 이유로 잘 알려진(well-known) 포트 번호를 사용하는 경우도 있다. 이는 포트 번호와 기타 IP 패킷 헤드 정보를 기반으로 하여 플로를 구분하는 방식이 더 이상 안전하거나 정확하지 않음을 의미한다.

이러한 현상은 현재의 트래픽 분석을 통해서도 극명히 드러난다(<표 5> 참조). 포트 80번은 HTTP로 일반적으로 알려져 있지만, 그 중의 12% 정도는 다른 응용이 같은 포트 번호를 사용하는 경우이다. 또한 passive FTP인 경우는 동적인 포트 번호를 사용하므로 단순한 포트 번호에 의해서는 응용 식별이 안된다. 또한 포트 번호 5003번과 같이 여러 응용이 같은 포트 번호를 사용하는 경우도 많이 존재한다.

<표 5> 단순한 포트 기반에 의한 응용 식별의 문제점

Port/Application	Port-based Accounting	Contents-aware Accounting
80/HTTP	67GB	59.1GB (11.8% reduced)
21/FTP_CTRL	0.29GB	0.28GB
20/FTP_DATA	43GB	42GB
?FTP_DATA_ PASSIVE	n/a	6GB (14.3% of FTP_DATA, 2% of the total volume)
5003/?	692MB	HTTP: 13.2MB
		BUGS_MUSIC: 402.8MB
		EDONKEY: 172.3MB
		Etc.: 85.7MB

따라서 이러한 문제를 해결할 수 있는 새로운 접근법이 필요하다[36]. 그에 대한 해결 방법들 중 [36],[37], ETRI에서는 IP 패킷의 헤더뿐만 아니라 응용 헤더까지도 식별하는 방법을 연구하고 개발하였다[1],[36].

이 접근법의 핵심적인 내용은 다음과 같다. 개별적인 응용들은 응용 헤더들에서 다른 응용들과 차별적인 독특한 패턴을 가질 가능성이 크다. 그러므로, 이들의 패턴을 미리 분석하여 측정에 적용하면 포트 번호에 기반한 방법에 비해 응용 식별 오류를 상당히 줄일 수 있다는 것이다. Passive FTP와 같이 동적인 포트 번호를 사용하는 경우도 이러한 방법에 의해 정확한 응용 식별이 가능하다.

상기의 접근법은 과금을 포함한 다양한 응용에 효율적으로 적용 가능하다.

V. 맺음말

본 고에서 소개한 플로 기반의 측정 기술은 차세대 네트워킹을 위한 기술과 맞물려 고속화 수용, 고품질 인터넷 서비스를 지원하기 위해 활발히 연구 및 개발되고 있는 분야이다. 특히 이러한 플로 기반 측정 기능은 라우터에는 필수적으로 갖추어야 할 기능이 되어갈 것이다. 그러나 앞서 지적한 바와 같이 응용 식별의 문제, 측정의 고속화 문제, 이에 대한 표준화 문제 등 아직까지는 해결해야 할 난제들이

많이 있다.

인터넷 망에서의 트래픽 측정 기술은 망이 고도화될수록 그 중요성이 더욱 증가될 것이다. 또한 앞으로의 측정 기술은 본 고에서 언급한 여러 응용들 외에도 망 서비스 및 기술, 망 장비 최적화 등 차세대 네트워킹의 기술적인 개발과 요구 사항들을 고려하여야 한다. 이를 위해서는 측정 기술에 대한 연구를 보다 조직적으로 수행할 필요가 있으며, 연구망의 확충과 다양한 기관에서의 적극적인 참여가 필요할 것으로 판단된다.

참 고 문 헌

[1] M. Crovella and A. Beswtavros, "Self-similarity in World-Wide Web Traffic: Evidence and Possible Causes," *Proc. Of ACM Sigmetrics Conference on Measurement and Modeling of Computer Systems*, May 1996.

[2] TS Choi et al., "Rate-based Internet Accounting System Using Application-aware Traffic Measurement," *Proc. Of Asia-Pacific Network Operations and Mangement Symposium(APNOMS2003)*, Fukuoka, Japan, Oct. 2003, pp.404-415.

[3] TM Forum, "Service Level Agreement Management Handbook," GB917, v1.5, June 2001.

[4] K. Claffy and T. Monk, "What's Next for Internet Data Analysis? Status and Challenges Facing the Community," *Proc. Of IEEE*, Vol.85, No.10, Oct. 1997, pp.1563-1571.

[5] "Network Traffic Measurement and Experiments," *IEEE Communications Magazine*, 2000, pp.120-185.

[6] 윤승현, 양지호, 정태수, "인터넷 트래픽 측정 시스템 개발," COMSW 2001, 2001.

[7] M. Crovella, C. Lindemann, and M. Reiser, "Internet Performance Modeling: the State of the Art at the Turn of the Century," *Performance Evaluation*, Vol.42, Issues 2-3, 2000, pp.91-108.

[8] S. Banerjee, D. Tipper, and B.H. Martin Weiss, "Traffic Experiments on the vBNS Wide Area ATM Network," *IEEE Communications Magazine*, Vol.35, No.8, 1997.

[9] S. Kalidindi and M.J. Zekauskas, "Surveyor: An Infrastructure for Internet Performance Measurements," INET'99, 1999.

[10] K. Mase, "Service Quality and Traffic Management for the Internet[1]: Network Modeling and An Overview," 전자정보통신학회지(일본), Vol.82, No.10, 1999, pp.1054-1061.

[11] C. Fraleigh, C. Diot, B. Lyles, S. Moon, P. Owezarski, D. Papagiannaki, and F. Tobagi, "Design and Deployment of a Passive Monitoring Infrastructure," PAM, 2001.

[12] W. Matthews, L. Cottrell, and D. Salomoni, "Passive and Active Monitoring on a High Performance Research Network," PAM, 2001.

[13] V. Paxson, "Framework for IP Performance Metrics," RFC 2330, May 1998.

[14] V. Paxson, "End-to-end Internet Packet Dynamics," *IEEE/ACM Transactions on Networking*, Vol.7, No.3, June 1999, pp.277-292.

[15] CAIDA, http://www.caida.org.

[16] N. Duffield, C. Lund, and M. Thorup, "Charging from Sampled Network Usage," IMW, 2001.

[17] L. Zhichun, Z. Hui, Y. Yue, and H. Tao, "Linuxflow: A High Speed Backbone Measurement Facility," PAM 2003.

[18] N. Duffield, C. Lund, and M. Thorup, "Properties and Prediction Flow Statistics from Sampled Packet Streams," IMW, 2002.

[19] NLANR, http://www.nlanr.net.

[20] RIPE-NCC, http://www.ripencc.net.

[21] CA*net4, http://www.canarie.ca/canet4.

[22] Internet2, http://www.internet2.org.

[23] Sprint ATL IPMON, http://www.sprintlabs.com/Department/IPInterworking/Monitor.

[24] GENESIS, http://www.genesis.tao.go.jp.

[25] IPPM, http://www.ietf.org/html.charters/ippm-charter.html.

[26] IPFIX, http://www.ietf.org/html.charters/ipfix-charter.html.

[27] PSAMP, http://www.ietf.org/html.charters/psamp-charter.html.

[28] CISCO, http://www.cisco.com.

[29] Juniper, http://www.juniper.net.

[30] LFAP, http://www.networksorcery.com/enp/protocol/lfap.htm.

[31] sFlow, http://www.inmon.com.

[32] NetFlow, http://www.cisco.com/warp/public/cc/pd/iosw/ioft/neflct/tech/napps_wp.htm.

[33] Extreme, http://www.extremenetworks.com.

[34] NTOP, http://www.ntop.org.
[35] Traffic Measurement and Monitoring Roadmap, http://www.ist-mome.org/documents/traffic_ngni.pdf.
[36] 최태상 외 7인, "정밀 과금을 위한 컨텐츠 기반 인터넷 응용 트래픽 측정 및 분석," 전자공학회논문지, 제40권, TC편 제10호, 2003. 10.
[37] Subhabrata Sen et al., "Accurate, Scalable In-Network Identification of P2P Traffic Using Application Signatures," *Proc. of WWW2004*.