Journal of The Korea Society of Computer and Information
Vol. 18, No. 12, December 2013
www.ksci.re.kr
http://dx.doi.org/10.9708/jksci.2013.18.12.113

네트워크 기상 관리 시스템의 설계 및 구현

김 현 철*

Design and Implementation of a Network Weather Map System

Hyun-Chul Kim*

요 약

본 논문에서는 네트워크의 전반적인 구조와 함께 트래픽 흐름을 한 눈에 보여줄 수 있는 거시적인 view를 제공하는 네트워크 기상도 시스템을 위한 모델을 제안하고, 이를 설계 및 구현 하여 실제 전국 규모의 연구망에 구축 및 활용된 사례를 소개한다. 개발된 기상도 시스템은 전반적인 네트워크 사용 현황 정보에 더해 네트워크 내의 주요 라우터 노드 및 백본 링크들에 대한 현 상황은 물론 과거의 주요 트래픽 플로우 상황 정보들을 모두 데이터베이스화 하고, 이렇게 축적된 데이터를 바탕으로 웹 기반의 질의 응답 기능까지 모두 제공하는 통합 관리 시스템으로, 저비용으로 효율적인 네트워크 관리 시스템을 필요로 하는 중소규모 망 사업자 및 관리자들에게 하나의 좋은 관리 도구가 될 수 있을 것이다.

▸ Keywords : 넷플로우, 플로우스캔, 네트워크 기상도

Abstract

In this paper, we design and implement a network weather map system, which provides a macroscopic view on the whole network topology as well as the network link status and utilization. The proposed system also provides distributed NetFlow-based database facility and Web-based query interface, through which network operators can check the detailed network router or link status as well as submit predefined queries to easily find out and locate heavy hitters and/or their usage. We believe that our develop system will be a useful tool for small-to-mid-scale ISPs or network operators, in managing their own networks in a cost-effective way.

▸ Keywords : NetFlow, FlowScan, Network Weather Map

•제1저자 : 김현철 •교신저자 : 김현철
•투고일 : 2013. 12. 6, 심사일 : 2013. 12. 24, 게재확정일 : 2013. 12. 29.
* 상명대학교 컴퓨터소프트웨어공학과(Dept. of Computer Software Engineering, Sangmyung University)
※ 이 논문은 2012학년도 상명대학교 교내연구비 지원에 의한 결과임 (2012-A000-0173)

I. 서 론

고속 인터넷 서비스 사용자의 증가와 함께 네트워크 트래픽의 증가는 대규모 인터넷의 확장성, 안정성, QoS 등을 보장하기 힘들게 하며, 더욱이 차세대 고성능 시험(연구)망에서는 이런 일반 상용망에서의 트래픽과 또 다른 차이점을 보이고 있어 네트웍의 상태에 대한 정당한 보고와 예측의 어려움을 겪는다. 이러한 문제점을 해결하기 위해서 네트웍 트래픽의 측정과 분석, 가시화에 대한 중요성이 커지며, 이를 연구하고 개발하려는 움직임 역시 활발하다. 이와 같이 효과적인 망 관리를 위한 네트웍 트래픽, 성능 측정 기능은 차세대 고성능 시험 연구망에서도 선도적 분석 측면에서 반드시 필요하다. 그러나 국내의 경우 one-way delay, round-trip time, connectivity, throughput 등과 같은 각각의 metric에 대한 end-to-end behavior를 측정하는 tool들은 있으나, 이런 기능과 더불어 전체적인 망의 구조와 흐름을 함께 보여줄 수 있는 거시적인 (macroscopic) 시각에서의 트래픽 측정과 분석 및 가시화를 제공하는 통합적인 시스템에 대해선 아직 초기 단계에 머무르고 있거나, (다음 섹션에서 설명되듯이) 아직 제공되는 기능들에 많은 제약이 있다.

본 논문에서는 네트워크 내의 특정 한 노드 (호스트 혹은 라우터)에 대한 성능 및 상태 측정, 분석, 가시화 뿐만 아니라 전반적인 네트워크의 구조와 흐름을 한 눈에 보여줄 수 있는 거시적인 view를 제공하는 네트워크 기상도 시스템을 디자인, 구현하여 실제 구축 및 적용된 예를 소개한다. 구축된 네트워크 기상도 시스템은 네트워크 내 각 라우터 및 라우터 간의 링크에 대해서 웹 기반의 실시간 트래픽 정보를 제공하고 과거의 데이터에 대해서 사용자 입력에 따른 질의를 통해 결과를 추출하고 이를 가시화하는 기능을 지원한다. 이러한 정보는 기존의 MRTG[1] 기반의 네트워크 기상도들이 제공하는 제한된 정보를 개선하고 또한 기존의 시스템들에서는 제공하지 않았던 질의와 그 결과의 가시화를 통해 네트워크 사용자 및 관리자들이 현재 그리고 과거의 네트워크 흐름을 이해하고 문제 발생 시 원인 규명 및 해결 방안 모색에 도움을 주는데 목적이 있다.

이러한 기능들을 지원하기 위해, 본 논문에서 제안하는 네트워크 기상도는 다음의 섹션에서 소개되는 바 대로 NetFlow[2]와 FlowScan[3]을 이용하여 네트워크 내의 라우터들에 대한 정보를 얻고 이 정보를 데이터베이스에 저장한다. 각 라우터의 인터페이스를 조사, 활용하여 라우터 간의 링크 트래픽에 대한 정보를 제공한다. 라우터 및 링크에 대해서 사용자가 제공되는 질의 인터페이스를 통해 질의할 수 있고 이를 데이터베이스로부터 추출하여 가시화한다.

본 논문의 구성은 다음과 같다. 먼저 섹션 2에서 관련 연구를 비교 분석하고 한계점을 논한 후, 본 논문에서 제안 및 구현될 네트워크 기상도 시스템이 목표로 한 주요 기능들을 간략히 소개한다. 섹션 3에서는 우리의 네트워크 기상도 시스템인 FlowMap의 구조 모델을 제안하고, 주요 구성 요소들 (전체 시스템 구조, 데이터베이스 모델 및 웹 기반 질의 인터페이스의 요구 조건 등) 을 소개한다. 섹션 4에서는 제안된 FlowMap 시스템을 구현한 후 국내 미래인터넷 연구망인 KOREN 상에 실제 구축, 운영한 실제 활용 사례를 소개하며, 마지막으로 섹션 5에서 본 논문에서 제안된 FlowMap의 공헌도를 요약, 정리하고 추후 개선 사항들을 논의하며 마무리 한다.

II. 관련 연구

1. 기존 관련 연구 분석 및 비교

네트워크 내의 특정 호스트 혹은 라우터나 링크를 오가는 트래픽의 종류와 양에 대한 측정, 분석, 가시화 뿐만 아니라, 이에서 한걸음 더 나아가 전반적인 네트워크의 구조와 흐름을 한눈에 알아볼 수 있는 거시적인 (Macroscopic) 시각에서 관리할 수 있도록 도움을 주는 기존 연구 결과물들이 있으며, 대표적으로 Internet2 Abiline NOC의 Weather Map[8], CANet3 ARDNOC의 Traffic Map[14]이 있다. 아래 테이블 1은 Weather Map (또는 Traffic Map) 형태의 연구 결과물들을 조사하고, 공통되는 기능 및 요구되는 주요 기능들을 나열하고, 각 해당 주요 기능에 대한 지원 여부를 분석하여 보여준다.

대부분의 시스템이 MRTG[1] 기반의 네트워크 상에서 트래픽의 총량을 중심으로 보여주고 있으나, 세부적인 주요 프로토콜 별, 응용 별 통계 정보를 보여주는 관련 연구는 CAnet3 ARDNOC 단 한군데에 불과하다. 또한, 트래픽 상황에 대한 실시간 업데이트 기능과 더불어서, 과거의 특정 시간대에 사용된 트래픽 양을 언제든지 사용자 (즉, 네트워크 관리자) 가 편리하게 사후 질의를 해서 분석할 수 있는 기능을 동시에 제공하는 연구 결과물들은 단 하나도 없는 실정이다.

표 1. 기존 네트워크 기상도 시스템 기능 분석 비교표
Table 1. Previous work on Network Weather Map (A: Internet2 Global NOC Weather Map[8], N: NORDUNET Weather Map[9], O: Opnix Internet Traffic Report[10], K: Keynote - Internet Health Report[11], W: WorldCom - Latency Statistics[12], C: CANARIE Traffic Map[13], G: GRNET[14])

기능/툴	A	N	O	K	W	C	G
지도표시 지원	O	O	O	X	X	O	O
실시간 지원	O	O	O	O	X	O	O
기간별 통계	O	O	O	X	O	O	O
프로토콜별 통계	X	X	X	X	X	O	X
응용 별 통계	X	X	X	X	X	O	X
시각화 지원	O	O	O	O	X	O	O
in/out 구분	O	O	X	O	O	O	O
링크 사용량	O	O	X	O	X	O	O
사용자 질의지원	X	X	X	X	X	X	X

이러한 문제를 해결하기 위해, 본 논문에서는 위의 모든 기능들을 통합해서 제공하는 네트워크 기상도 시스템의 모델을 제안하고, 구현 및 실제 구축하여 운영된 사례까지 포함하여 소개한다. 본 연구의 목적은 주어진 네트워크의 각 라우터들 및 라우터들 간의 링크들에 대해서 실시간으로 트래픽 정보를 제공하는 동시에, 과거에 축적해놓은 트래픽 플로우 데이터베이스를 활용해서 네트워크 관리자가 망 운영을 하는 데에 있어서의 주요 관심사들 - 즉, 누가, 어떤 종류의 트래픽을, 언제부터 언제까지, 얼마나 많이 썼는지, 가장 많이 사용하였는지 등등 - 을 효율적이고 편하게 분석, 파악할 수 있는 질의 및 가시화 기능까지 제공하는 통합 관리 시스템을 제안하고 구현 및 구축하는 데에 있다.

이러한 시스템을 위해서는 기존의 MRTG 기반의 기상도들이 제공하는 제한된 정보들을 개선하고, 또한 기존 네트워크 기상도 시스템들에서 제공하지 않았던 질의와 그 결과의 가시화를 위한 모듈을 설계해야 한다. 표 1에 표시된, 이러한 기능들을 모두 통합적으로 제공하는 시스템은 일단 구현, 구축되고 나면, 네트워크 사용자 및 관리자에게 현재는 물론 과거의 네트워크 사용 흐름을 이해하고, 비정상적으로 과다한 트래픽을 누군가가 발생시키고 있다든지 하는 등의 문제가 발생할 시에 빠르고 정확한 원인 규명 및 해결 방안 모색에 큰 도움을 주게 될 것이며, 본 논문의 주요 공헌은 이러한 다양한 기능을 통합적으로 제공하는 기상도 시스템을 위한 FlowMap 모델을 제안하고, 이를 구현한 후 전국적인 KOREN 연구망에 실제 구축까지 한 후 활용하는 사례를 소개하는 것에 있다.

2. NetFlow와 FlowScan

본 연구에서는 기존 네트워크 기상도 시스템의 한계를 극복하고 프로토콜 별 통계 및 응용 별 통계, 시각화 지원, 라우터 in/out 총량 구분 기능 등을 모두 지원하기 위해 NetFlow와 FlowScan 시스템을 활용하여 네트워크 기상도 시스템을 구축한다. 네트워크의 플로우는 네트워크 내에서 소스와 목적 지점을 공유하는 한 방향의 연속된 패킷들의 집합으로 정의된다[2]. 구체적으로는 〈source IP, destination IP, protocol, source port, destination port〉의 5 tuple로 이루어지며, NetFlow에는 Type of Service (ToS), 그리고 input interface 식별자도 이용한다. NetFlow는 1:n 샘플링 기능 등을 통해 라우터의 성능에 최소한의 영향을 미치면서 상세한 데이터를 모을 수 있도록 설계되었다.

FlowScan은 David Plonka에 의해 개발된 수동적인 트래픽 측정 툴이다. NetFlow를 내보낼 수 있는 기능이 탑재되어 있는 라우터에서 NetFlow 데이터그램을 받아 가공하여 라우터에 흐르는 트래픽에 대해서 바이트, 패킷, 플로우와 같은 양적인 정보들 뿐 아니라 프로토콜, 응용 별 카테고리 등에 대한 정보들 또한 보여줌으로써 라우터를 지나가는 트래픽의 흐름 및 추이를 보여줄 수 있다. 그림 1은 FlowScan에서 제공하는 near-realtime 트래픽 분석 그래프의 한 예를 보여준다.

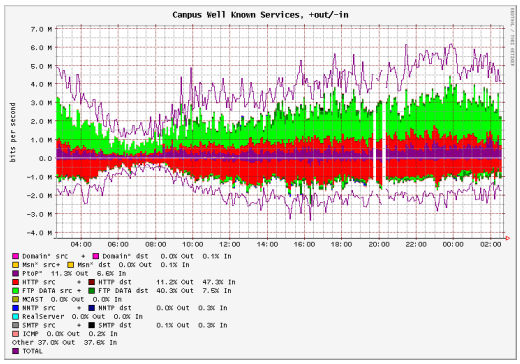

그림 1. FlowScan: 샘플 출력 화면
Fig. 1. FlowScan: a screenshot

III. FlowMap 시스템 모델

1. 시스템 구조

1.1 FlowMap 시스템 모델

본 논문에서 제안하는 네트워크 기상도 시스템 (이하 FlowMap이라 한다) 은 여러 개의 라우터로 구성된 네트워크 상에서, 각 라우터를 통해 지나가는 트래픽 플로우와 라우터 간의 링크들에 대한 정보를 나타내 주는 것을 목표로 한다. 이를 위해, FlowMap은 각 라우터에서 제공되는 NetFlow 정보를 받도록 설계하며, 따라서 모니터링 하고자 하는 네트워크의 관측 대상 라우터의 개수가 n개이면 n개의 라우터로부터 NetFlow 정보를 받아서 사용자 (즉, 네트워크 관리자)에게 네트워크 기상도를 보여주도록 설계한다.

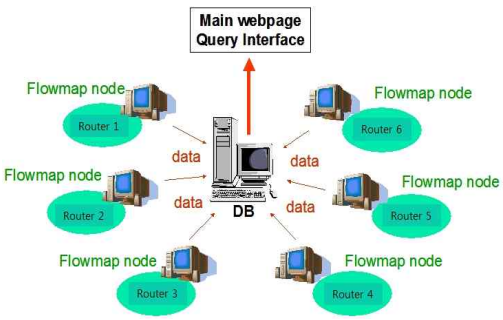

그림 2. 플로우맵 전체 시스템 모델
Fig. 2. Flowmap System Model: Overview

전체 시스템 구조는 그림 2와 같고, 실제 네트워크 관리자가 사용하게 될 예제 기상도(weather map)는 본 연구 결과 구현물의 스크린 샷인 그림 7과 같으며, 주요 라우터들을 디스플레이 하고, 주요 라우터 사이의 링크들을 흐르는 트래픽의 사용량 (활용량 %, 즉 utilization)을 그림으로 보여주게 된다. 그리고, 이 기상도 화면에서 네트워크 관리자가 관심 있는 라우터 또는 링크를 클릭하면 해당 라우터 또는 링크에 대한 세부적인 정보를 그림 1과 같이 보여주는 동시에, 여기에 추가로 세부적인 분석을 위한 다양한 질의를 지원하는 데이터베이스와 웹 기반 인터페이스까지 제공하게 된다.

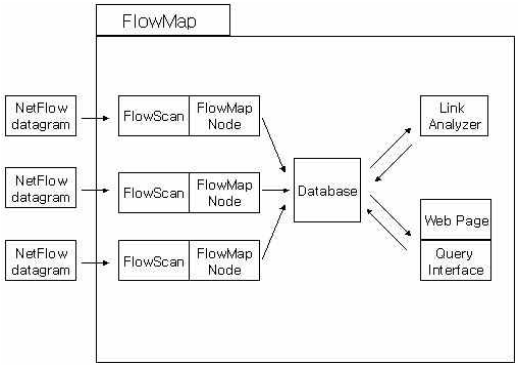

그림 3. 플로우맵 각 노드의 모델: 내부 구조
Fig. 3. FlowMap Node model: the internal structure

각 FlowMap 노드는, 담당하고 있는 해당 라우터의 flow exporter로부터 NetFlow를 제공받는다. 그리고 기존의 FlowScan은 NetFlow들을 받아서 기존의 FlowScan이 제공하는 트래픽 그래프들을 (그림 1과 같은) 만들어 낸다. 그 뒤 각 FlowMap node는 필요한 정보들을 보여주기 쉬운 형태로 정리하여 flow data를 저장한다. (저장되는 정보들은 다음 서브 섹션인 데이터베이스 모델 설계 부분에서 설명된다.) 이렇게 저장된 데이터는 링크나 질의에 대한 정보를 제공할 때 사용된다. 각 FlowMap 노드의 내부 구조는 그림 3과 같다.

Database에 저장되는 정보는 크게 (i) 각 라우터에 대한 세부적인 트래픽 정보와 (ii) 각 링크들에 대한 세부적인 트래픽 정보인데, 링크 트래픽 정보들은 NetFlow 데이터에 제공되는 인터페이스들의 정보를 이용하여, 각 링크에 대해 연결되는 라우터의 어떤 인터페이스로부터 트래픽이 제공되는지를 살펴봐서 추출한다. 라우터 인터페이스 정보로부터 라우터 간 링크별 트래픽 정보를 추출해내는 과정을 간단히 도식화하면 그림 4와 같다. 즉, 각 라우터들 별로 (per-router), Netflow 데이터로 제공되는 라우터 인터페이스 정보를 이용하여, 각 링크에 대해 연결이 되는 라우터의 어떤 인터페이스로부터 트래픽들이 유입 또는 유출되는지를 살펴본다.

1.2 데이터베이스 모델 설계

앞서 언급된 바와 같이 flow exporter로부터 얻어진 플로우들은 데이터베이스 서버에 저장된다. 데이터베이스 서버는 각 라우터들로부터 입력되는 정보를 각 라우터별로 별도로 저장, 관리하며, 입력되는 정보들은 그림 5에서와 같이, 각 라우터 당 front table이라는 임시 테이블에 1차적으로 저장해 두었다가 매 15분 간격으로 aggregation해서 해당 라우터

에 대한 테이블로 정리해서 저장된다. 즉, 최종적으로 데이터베이스에 저장되는 데이터는, 각 라우터 별로 매 15분마다 aggregation된, 또한 각 라우터별 데이터 별로 추출되는 링크 별 트래픽들에 관해, 다음과 같은 정보들을 저장한다; 각 Autonomous System 별 트래픽 현황, 각 프로토콜 별 트래픽 현황, 포트 별 트래픽 현황, 사용자 (즉, IP 주소) 별 트래픽 현황, Router의 Next hop 별 트래픽 현황, 전체 트래픽 총량 별 랭킹 정보 등. 이와 같이 aggregation을 매 15분마다 반복해서 해줌으로써 DB 저장 공간을 상당히 절약할 수 있도록 설계하였고, 따라서 결과적으로 보다 오랜 기간동안의 데이터들을 저장할 수 있게 된다.

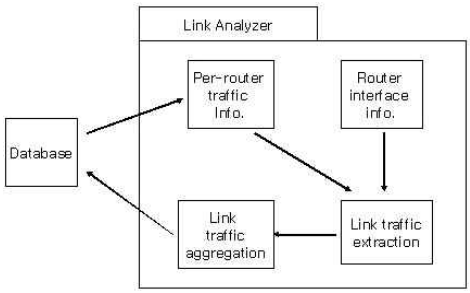

그림 4. (라우터 인터페이스 정보로부터의) 링크 트래픽 정보 추출
Fig. 4. Link traffic extraction (from router interface info.)

1.3 웹 기반 데이터베이스 질의 인터페이스 설계

FlowMap 시스템은 사용자 (네트워크 관리자)의 편의를 위해, 네트워크 기상도에서 관심 있는 노드나 링크를 선택하면 하이퍼링크를 통해 해당 노드 또는 링크의 트래픽 상태 및 히스토리에 대해 자세한 질의를 할 수 있도록 웹을 기반으로 한 질의 인터페이스를 제공하도록 설계하였으며, 네트워크 관리자인 사용자 입장에서 가장 중요한 기능들을 편리하게 제공하기 위해, 다음과 같은 기능적인 요구조건들을 만족할 수 있도록 설계하였다.

1. 각 라우터에 대하여 FlowScan이 분석한 정보를 데이터베이스에 저장하고 있으므로, 이것을 웹 인터페이스를 통해 질의할 수 있어야 한다.
2. 네트워크 기상도 시스템의 첫 메인 화면에서 각 라우터 또는 링크에 대하여 알아보기 위하여, 해당 라우터 또는 링크를 선택하면 새로운 창을 띄워준다. 해당 창은 현재 선택된 라우터 또는 링크의 상황 분석을 그래프를 이용하여 보여주게 되며, 또한 동시에 궁금한 상황들을 모니터하기 위한 질의를 할 수 있는 인터페이스를 제공해야 한다.

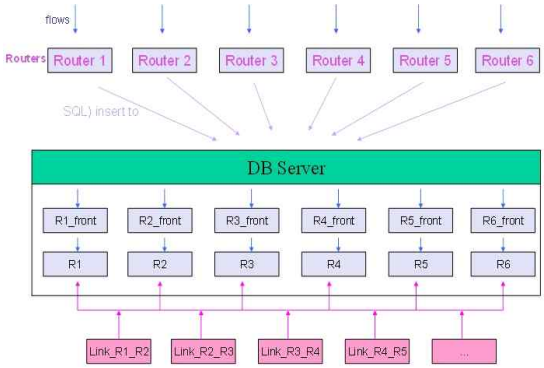

그림 5. 플로우맵 데이터 베이스 수집 및 저장 모델
Fig. 5. FlowMap Database: Collection and Storage

3. 네트워크 관리자 입장에서 가장 중요한 상황 모니터링 대상 항목들인 Top AS, User, Protocol, Port, Interface (next hop) 등의 정보들을, 선택된 라우터 또는 링크에 대해, 관리자가 입력한 기간 동안 (언제부터 언제까지, 일/시/분/초 단위로) 저장된 데이터들을 분석해서 보여 줄 수 있는 편리한 질의 기능을 제공해야 한다.

이러한 요구 사항들을 고려하여 설계 및 구현된 웹 기반 질의 인터페이스 및 질의 결과 등은 다음 섹션에서 논한다.

IV. 구현, 실제 구축 및 활용 사례

1. 개발 환경

기본적인 개발 환경으로 커널 버전 2.4.2의 리눅스를 사용했다. C로 개발하기 위해 gcc-2.96 컴파일러를 사용하고, 이미지 출력을 위해 Thomas Boutell의 GD 라이브러리인 gd-1.9.3을 사용하였다. GD 라이브러리는 기본적인 이미지 조작을 위해 사용하는 그래픽 라이브러리로, 필요한 이미지를 임의로 생성시키거나 이미지에 도형을 그리기 위한 다양한 함수들이 포함되어 있다. 프로그래머는 이 라이브러리를 자신의 소스 코드 안에 포함시키는 것으로 다양한 작업이 가능해진다. 유명한 트래픽 분석 시스템인 MRTG[1] 도 이 GD 라이브러리를 사용한다.

리눅스에서는 이 GD 라이브러리를 기본 패키지 안에 포함하고 있어, 사실상 최근 버전의 리눅스라면 따로 설치할 필요가 없다. 구현 가능한 언어도 C 뿐만 아니라 perl, Tcl, Pascal, PHP 등에서 사용이 가능하다. 생성되는 이미지의

포맷으로는 예전에는 GIF를 사용하였는데, 1.6 버전부터 GIF 포맷의 사용 제한 때문에 지원을 하지 않는 대신 libpng, zlib를 사용하여 PNG 파일 포맷을 지원할 수 있으며, jpeg-6b를 사용하여 JPEG 포맷을 지원한다. 그 외에 WBMP 포맷도 지원한다.

2. 시스템 구축 및 운영 환경: KOREN (미래 네트워크 연구 시험망)

구현된 FlowMap 시스템은 미래 네트워크 연구 시험망인 KOREN (구 초고속 선도망)에 실제로 구축, 테스트 및 사용되었다. 미래 네트워크 연구 시험망[4]은 국내연구기반을 확대하고 초고속정보통신 장비 및 응용서비스 개발에 필요한 연구환경을 제공하기 위해, 정부의 지원을 받아 대학/연구소/산업체 등에 6T 관련 기술 및 응용서비스 개발에 필요한 네트워크 환경을 제공하는 비영리 연구망이다. 1995년 초고속선도망이 개통된 이후 1997년까지 네트워크 기술 및 관련 장비 개발에 관한 연구가 주를 이루었으며, 과학기술 전반의 점점 다양해지는 연구수요를 충족시키고자 1998년부터 QoS/Multicast/IPv6 /MPLS를 적용한 차세대 첨단 연구환경으로 재구성하고 서울/대전/광주/대구/부산/수원 등 6개 대도시 지역을 10Gbps~ 20Gbps로 연결하는 백본망을 구축, 운영하고 있다.

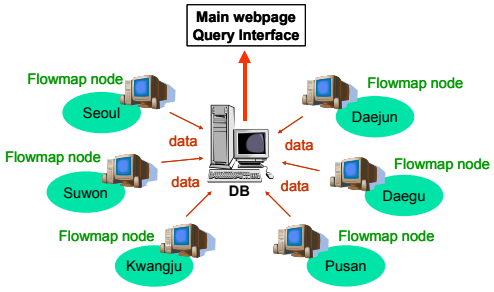

그림 6. KOREN에 구현, 구축된 플로우맵 시스템
Fig. 6. FlowMap System on KOREN

KOREN의 주 목적은 연구, 시험, 시험서비스 등 다양한 이용자 환경의 특화된 서비스를 제공하기 위해 R&D 네트워크, 테스트베드 네트워크, 서비스 네트워크 등 효율적인 구조로 운영하고 있으며, 국제연구망 (APAN [5], TEIN [6]) 등과 연동되어 있다. 실제로 KOREN 상에서 구현 및 구축, 운영된 FlowMap 시스템의 구조는 그림 6과 같다.

본 연구에서 설계 및 구현된 네트워크 기상도가 구축된 KOREN 상에서 포함하는 코어 라우터는 서울 XP, 서울 GSR, 수원 GSR, 대전 GST, 광주 GST, 대구 GSR, 부산 GSR로써 총 7개이며, 따라서 flow exporter (NetFlow를 export하는 라우터나 스위치)는 7개가 뜨고, flow collector (NetFlow를 받는 장비) 역시 7개가 필요하다. 현재 개발된 시스템의 구조상 하나의 collector에서 여러 개에서 오는 flow를 받는 것은 가능하지 않은데, 이는 우리가 기본으로 사용하는 FlowScan이 하나의 exporter를 위해 만들어져 있어서 그렇다. 이점은 추후에 수정 및 보완될 가치가 있다. 수집된 플로우들은 FlowScan이 1차적으로 처리를 하고 그 뒤에 환경에 따라 필요한 정보만을 추출해서 데이터베이스에 저장한다. 데이터베이스에 저장된 데이터는 질의 등 다른 정보들을 표현하기 위해서 사용된다.

3. FlowMap 기상도 구현

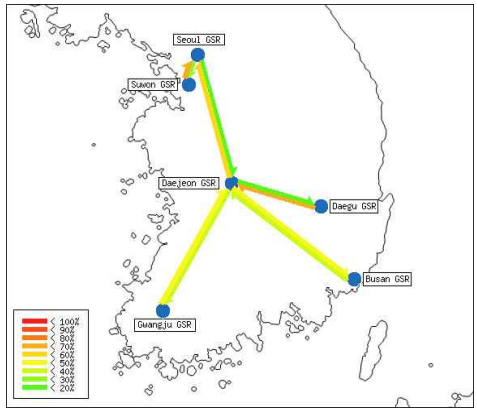

그림 7. KOREN 네트워크 사용상황 기상도
Fig. 7. KOREN Network Weathermap: link utilization

KOREN에서의 네트워크 기상도 개발을 위해, 출력될 기상도의 이미지 포맷은 PNG를 사용하였다. KOREN 네트워크에 구현, 구축한 기상도 그림은 그림 7과 같다. 배경 이미지인 대한민국 지도 그림을 PNG 포맷으로 변환시켜 CGI 프로그램이 위치하는 곳에 두고, 해당 파일을 로딩하여 배경으로 사용하였다. 이후 저장된 플로우 데이터들은 getenv() system call을 사용하여 CGI의 인자로서 받고, 받은 인자들을 각각 parsing하여 사용한 후 배경 그림 위에 분석된 정보를 덧입혀서 기상도로 출력한다. 또한, 출력된 기상도에서 각 노드나 링크를 선택하면 해당되는 노드 및 링크에 해당하는 웹페이지 또는 질의 화면으로 하이퍼 링크될 수 있도록 구현하였다.

네트워크 링크의 사용 현황 (utilization)을 다양한 색을 사용하였고, 20-30% 이하인 경우 초록, 50%이하인 경우 노랑, 70-80%이하인 경우 주황, 90-100%일 경우 붉은 색으

로 표기된다. 각 링크를 표현하는 화살표를 그리는 부분은 GD 라이브러리의 gdImageFilledPolygon (gdImage Ptr im, gdPointPtr points, int pointsTotal, int color) 함수와 gdImageColor Allocate (gdImagePtr im, int r, int g, int b) 함수를 사용해서 구현하였다. 그리고 각 GSR 노드 지점의 x, y 좌표를 지정하여 static 값으로 사용하였고, 각 노드를 표현하기 위해 원을 그리는 gdImageArc()함수를 사용하고, 각 라우터의 이름 태그를 위해 gdImageString() 함수들을 사용하였다. 이 함수는 각 지점의 정보를 가지고 있는 points 배열을 사용하여 색을 지정할 수 있는 다각형인 화살표를 지정한 위치에 그려주는 함수이다.

초기 화면에서 각 GSR 라우터 간의 링크의 정보들을 보여주기 위해 SNMP [7]을 사용하여 정보를 가져와 표현을 하도록 하였다. 링크 정보는 5분 주기로 새로 받아와 결과를 업데이트 하게 된다.

4. 웹 기반 질의 인터페이스 구현 및 활용 사례

FlowMap 기상도 시스템에서는 각 라우터에 대하여 FlowScan이 분석한 정보를 데이터베이스에 저장하고 있으므로, 이 정보들을 웹 인터페이스를 이용하여 질의할 수 있다. 먼저 기상도의 (그림 7과 같은) 첫 화면에서, 각 라우터 또는 링크에 대해 알아보기 위하여, 라우터를 선택하면 그림 8과 같은 새로운 창이 뜨게 된다. 이 창은 선택된 (대전) 라우터에 대한 분석을 그래프를 이용하여 보여주고 있으며, 이 창에서 웹 질의를 하기 위해서는 페이지 상단 메뉴의 Flowmap Query Page라는 링크를 선택한다. 이후 그림 9과 같은 질의 인터페이스 윈도우가 나타나면, Top User, Protocol, Port, AS, interface, General SQL query들 중 하나를 선택할 수 있다.

기본적으로 라우터 또는 어떤 링크에 대하여 질의를 할 것인지를 사용자가 직접 선택할 수 있고, 또한 원하는 시간 간격도 선택할 수 있다. 사용자가 원하는 적당한 조건을 선택한 후에 질의 submit 버튼을 눌러서 질의를 전송하면, 그림 10과 같이 질의 결과가 나타난다 (질의 인터페이스 및 분석 결과 화면에 나타나는 모든 IP 주소와 자세한 연도/날짜 정보는 개인정보 침해의 소지가 있으므로 모두 삭제 처리한다).

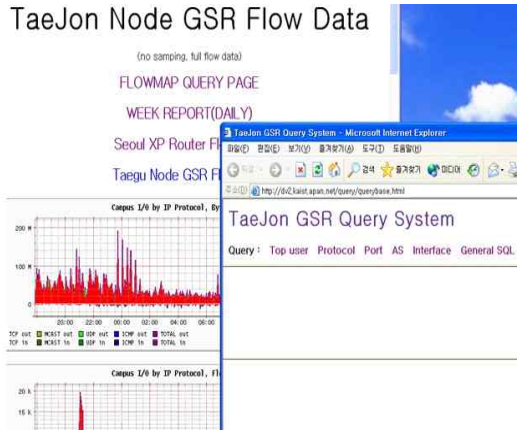

그림 8. 선택된 라우터의 상황정보 요약화면
Fig. 8. Main status page for a selected router

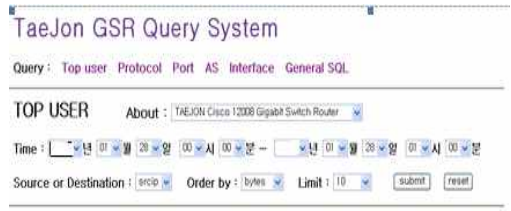

그림 9. 선택된 라우터를 위한 질의 입력 인터페이스
Fig. 9. FlowMap query interface for a selected router

그림 10. 질의 결과: Top 10 사용자들 출력 화면
Fig. 10. FlowMap query results: Top 10 users

그림 10의 결과는 전체 트래픽 중에서 가장 많은 양의 트래픽을 발생시키고 있는 Top 10 사용자들 (IP 주소들)을 질

의 결과로 나타내 주고 있으며, 이러한 기능을 활용해서 DDoS attack이나 malicious scanning을 하고 있는 IP들을 찾아내거나, 또는 비정상적으로 많은 트래픽을 많이 사용하고 있는 사용자들을 쉽게 찾아낼 수 있다. 그림 10의 경우를 보면 Top 세 명의 사용자들이 전체 트래픽 볼륨 양의 약 30% 정도를 생산하고 있는 것을 확인 할 수 있다. 또한, 라우터 뿐만 아니라 링크에 대해서도 같은 식의 질의를 할 수 있는 드롭 다운 메뉴를 별도로 제공하며, 그 이후에의 질의 진행 및 결과 출력은 위 그림 8-10의 경우와 동일하므로 생략한다.

V. 결 론

본 논문에서는 기존의 트래픽 측정 시스템들을 통합하여, 전반적인 네트워크의 구조와 트래픽의 흐름을 한눈에 알아볼 수 있는 거시적인 시각을 제공하면서, 또한 네트워크 내의 특정 주요 요소 (라우터 혹은 링크)를 지나는 트래픽의 측정, 분석 및 결과 가시화를 위한 웹 기반 질의 인터페이스 및 데이터 베이스 기능까지 제공하는 네트워크 기상도 시스템을 제안하였고, 제안된 시스템을 구현한 후 실제 전국적인 규모의 네트워크인 KOREN에 구축 및 테스팅 결과 까지 소개하였다. FlowMap 시스템은 섹션 2의 관련 연구 비교표 표 1 에서 언급된 모든 기능들 - 맵 지원, 실시간 업데이트, 기간 별 통계, 프로토콜 별 또는 응용 별 분석, 시각화 지원, 라우터 in/out 총량 구분 분석, 링크 사용량 분석, 사용자 질의 기능 - 을 통합하여 지원하고 있으며, 이는 기존의 네트워크 기상도 시스템들에 비해 월등하게 편리하고 효율적인 네트워크 관리 기능을 통합하여 제공한다.

현재까지 네트워크 트래픽 및 망 상태를 모니터링하는 많은 시스템들이 나와 있으나, 실시간 네트워크 사용 현황 정보에 대한 기상도 그래프에 더해, 이를 시작점으로 네트워크 내의 주요 노드 및 링크들에 대해 지나간 과거의 주요 트래픽 상황 정보들을 모두 데이터베이스화 하고, 이렇게 축적된 데이터를 바탕으로 웹 기반의 질의 응답 기능까지 모두 제공하고 있는 오픈 소스 시스템은 거의 찾아볼 수 없는 실정이다. 본 FlowMap 시스템은 저비용으로 효율적인 네트워크 관리 시스템을 필요로 하는 중소규모 망 사업자 및 관리자들에게 하나의 대안이 될 수 있을 것이다.

참고로, 추후 개선 또는 추가되어야 할 주요 기능들에는 다음과 같은 것들이 있다: (1) 데이터베이스 최적화: 비록 aggregation을 통해 저장되는 정보의 양을 줄였다고 해도, aggregation을 할 때 어떤 비율 또는 시간 간격으로 데이터를 저장하는 것이 가장 좋을지에 대한 문제는 여전히 존재한다. 이에 대한 추가적인 성능 평가 및 실험이 필요하다. (2) 다중 플랫폼 지원: 현재는 Linux와 MySQL 상에서 작동하나 FreeBSD와 같은 다른 플랫폼이나 데이터베이스 상에서도 작동하게 하면 더 좋을 것이다. (3) 패키징: 사용자가 손쉽게 설치하고 사용할 수 있도록 전체 소프트웨어가 패키징되어 제공될 수 있도록 해야 할 것이다.

참고문헌

[1] MRTG, http://oss.oetiker.ch/mrtg/

[2] CISCO NetFlow, http://www.cisco.com/go/netflow

[3] D. Plonka, "FlowScan: A network traffic flow repoorting and visualization tool", Proc. of USENIX LISA, Dec. 2000.

[4] KOREN, http://www.koren.kr

[5] APAN, http://www.apan.net

[6] TEIN, http://www.teincc.org

[7] SNMP, http://www.net-snmo.org

[8] Internet2 Global NOC Weather map, http://atlas.grnoc.iu.edu/atlas.cgi?map_name=Internet2%20IP%20Layer

[9] NORDUnet Weather map, http://indico.cern.ch/getFile.py/access?subContId=5&contribId=6&resId=0&materialId=slides&confId=80755

[10] Opnix Internet Traffic Report, http://www.internet trafficreport.com

[11] Keynote Internet Health Report, http://www.internet pulse.net

[12] WorldCom Latency Statistics, http://www.inforede.net/Technical/Upper_Layers/Network_ SLM/Paper%20Latency%20UUNET.pdf

[13] CANARIE Traffic Map, http://weathermap.canarie.ca/index.html

[14] GRNET, http://netmon.grnet.gr

저 자 소 개

김 현 철

1995: KAIST
전산학과 공학사.
1997: KAIST
전산학과 공학석사.
2005: KAIST
전자전산학과 공학박사
현 재: 상명대학교
컴퓨터소프트웨어공학과 교수
관심분야: Internet Measurement
Email : hkim@smu.ac.kr