SNMP를 이용한 웹 기반의 네트워크 트래픽 분석 모델 구현

윤홍일, 장경수, 변선일, 신동렬
성균관대학교 전기전자 및 컴퓨터 공학과
e-mail : glyun@nova.skku.ac.kr

An Implementation Of Web-Based Network Traffic Analysis Model Using SNMP

Hong-Il Yun, Kyung-Soo Jang, Sun-Il Byun, Dong-Ryul Shin
Dept. of Electrical and Computer Engineering, Sungkyunkwan University

요약

본 시스템은 로컬 시스템에 저장되어 있는 관리 정보를 원격지 시스템에서 웹 브라우저를 이용한 그래픽 환경에서 네트워크를 보다 쉽게 판단, 관리하고자 하는 목적으로 둔다. 그리고 이를 위해 네트워크 관리 정보 수집프로그램인 MRTG(Multi Router Traffic Grapher)를 이용하여 얻어 온 MIB(Management Information Base)정보를 네트워크 관리자에게 보다 유용한 분석 항목의 값으로 수정하여 이를 웹 기술과 접목하고 GUI(Graphic User Interface) 환경의 사용자 인터페이스를 제공하고자 한다.

1. 서론

오늘날에는 전체 인터넷 트래픽 가운데 웹에 기반을 둔 텍스트와 멀티미디어 데이터의 양이 많은 부분을 차지하고 있다. 이러한 추세는 네트워크 관리 측면에도 반영되고 있다. 따라서 네트워크 관리자가 실시간의 네트워크 이용 현황을 파악하는 것에 대한 필요성이 대두되고 있다.

본 논문에서는 SNMP(Simple Network Management Protocol)를 이용하여 얻어 온 관리 정보를 분석하고 이를 이용하여 네트워크 관리 목적에 부합하는 항목들을 계산하여 데이터 베이스로 저장하고 웹을 통해 네트워크 관리자의 요구가 있을 때에 요청에 맞는 분석 항목의 값들을 그래프로 보여주고 있다. 2장에서 시스템에 구현 환경 및 전체적 구성, 그리고 모델의 구조를 설명하고 3장에서는 구현된 웹 모델을 보이고, 마지막으로 시스템의 결론과 앞으로의 과제에 대하여 제안하고 논문을 맺는다.

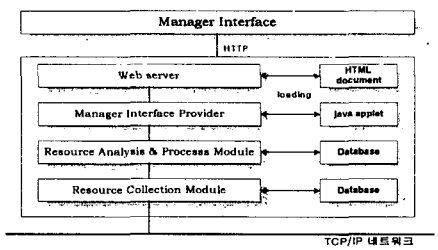
2. 구현

2.1 구현 환경

본 트래픽 분석 모델은 리눅스 6.1에서 설계되며 웹 문서의 전송을 위한 부분은 HTML(Hyper Text Markup Language) 언어로 작성한다. 그리고 관리자 인터페이스와 제공자의 통신을 위해서는 자바 소켓 응용 프로그래밍 인터페이스를 이용하고, 자료의 수집과 처리는 C 언어를 사용한다.

2.2 전체적인 구성

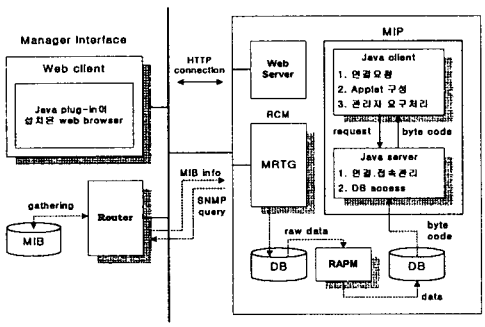
네트워크 트래픽 분석 모델의 개발 환경은 관리자 인터페이스(manager interface) 부분과 관리자 시스템(manager system) 부분으로 구성되고 관리자 인터페이스는 관리자가 트래픽 분석 항목에 대해 관리자 시스템에 자료를 요청하면 이것을 GUI(Gra phic User Interface)환경을 이용하여 관리자에게 보여준다. 관리자 시스템은 자료 수집 모듈(Resource Collection Module: RCM)과 자료 분석 처리 모듈(Resource Analysis and Process Module: RAPM), 그리고 관리자 인터페이스 제공자(Manager Interface Provider: MIP)로 구성되어 있다.



[그림 1] 시스템의 개괄적인 구조

2.3 트래픽 분석 모델의 구조

구현된 응용 프로그램을 모듈별로 나누어 각 모듈별 기능에 대해 설명해보면, 자료 수집 모듈은 MIB 값을 주기적으로 얻어 오는 일련의 과정을 설명하고 있고, 자료 분석 처리 모듈에서는 MIB 값을 이용한 각각의 트래픽 분석 항목의 공식을 유도한다. 그리고 관리자 인터페이스 제공자의 구성과 기능에 대한 세부적인 것은 [그림 2]에 도식화하였다.



[그림 2] 응용 프로그램의 기능별 관계

2.3.1 자료 수집 모듈

본 시스템에서는 관리자의 요청에 따른 관리 정보를 수집하기 위해서 SNMP 문의(query)를 이용하여 트래픽을 모니터링하고 SNMP 대리자로부터 얻은 자료를 관리자에게 그래픽으로 보여주는 MRTG (Multi Router Traffic Grapher)의 MIB 값에 대한 환경파일을 분석하고 이를 통해 얻은 가공되지 않은 데이터의 정보를 사용하고 있다. [그림 3]은 구성된 환경 파일의 일부이다.

다음은 자료 수집을 위해 MRTG를 이용하는 일련의 과정을 나타낸 것이다.

- MIB 정보를 가져올 SNMP 대리자의 IP 주소와 커뮤니티를 설정하여 환경파일을 구성한다.
- 네트워크 관리를 위해 필요한 SNMP 변수의 OID 값을 적어준다.
- 컴파일 한다.
- 크론탭(crontab)에 MRTG 작업을 등록함으로서 일정 시간동안 자동 수행하게 한다.

2.3.2 자료 분석과 처리 모듈

MRTG를 이용하여 얻은 MIB 값은 가장 최근에 폴링하여 얻은 값이 앞에 나와 있다. 따라서 자료 분석에 앞서 MRTG에서 저장한 파일을 읽어들이고, 이것을 역순으로 재 정렬하는 과정이 필요하다. 본 논문에서는 MRTG의 환경파일을 구성 후, 크론탭의 주기를 5분으로 설정하였다. 따라서 5분마다 MIB에 폴링하여 얻은 MIB 값을 얻어오게 되는데, 이러한 값들의 30분 동안의 평균값을 실제 자료로 이용하고 있다. 필요한 MIB 값을 선별 후 활용율, 인터페이스 패킷 송수신율 등의 트래픽 분석 항목을 계산하여 관리자 인터페이스 제공자에서 실제적으로 사용하게 될 파일을 만들게 된다. 다음은 본 논문의 트래픽 분석 모델 구현에 사용된 공식에 대한 설명과 유도 과정이다.

◉ 활용율(utilization)

링크의 활용율을 구하는 것은 현재 링크가 이용되는 정도와 링크의 용량에 비추었을 때의 혼잡한 정도를 파악 할 수 있어 효율적인 네트워크 관리를 위한 지표가 될 수 있다. 링크에는 두 가지 종류가 있다. 전 동시송수신(full duplex: FDX) 방식과 반 송수신(half duplex: HDX) 방식이다. 따라서 링크의 유형에 따라 활용율의 계산 방식 또한 다르다. 인터페이스에서의 총 패킷의 개수는 그 인터페이스를 통해 전송된 바이트 량과 그 인터페이스로 수신된 바이트 량의 합으로 이루어지는데, 전 동시송수신 방식인 경우에는 두 값 가운데에서 최대 값으로 설정된다.

$$utilization_{FDX} = 8 * \frac{\sum_{i=0}^{T} MAX(\text{ifInOctets}, \text{ifOutOctets})}{\Delta t_p * \text{ifSpeed}}$$

$$utilization_{HDX} = 8 * \frac{\sum_{i=0}^{T} (\text{ifInOctets} + \text{ifOutOctets})}{\Delta t_p * \text{ifSpeed}}$$

Δt_p 는 폴링(polling)한 시점의 시간차를 의미하며 sysUpTime으로 표시되는 timeticks 값이다[2].

◉ 인터페이스 패킷 송수신율

인터페이스로 유입되고, 전송되는 패킷을 전체 패킷의 개수로 나누어 구한다.

$$receiving\ rate = \frac{\sum(\text{ifInNUcastPkts} + \text{ifInUcastPkts})}{total\ packets}$$

$$sending\ rate = \frac{\sum(\text{ifOutNUcastPkts} + \text{ifOutUcastPkts})}{total\ packets}$$

$$\begin{aligned} total\ packets = {} & \text{ifInErrors} + \text{ifInUnknownProtos} + \\ & \text{ifInDiscards} + \text{ifInUcastPkts} + \text{ifInNUcastPkts} + \\ & \text{ifOutUcastPkts} + \text{ifOutNUcastPkts} + \\ & \text{ifOutDiscards} + \text{ifOutErrors} \end{aligned}$$

◉ 입출력 트래픽 비율

인터페이스를 통해 시간 당 입출력되는 실제 입출력 바이트 양의 비율을 나타낸다.

$$input\ rate = \frac{\sum_{i=0}^{T} \text{ifInOctets}}{\Delta t_p}$$

$$output\ rate = \frac{\sum_{i=0}^{T} \text{ifOutOctets}}{\Delta t_p}$$

◉ 방송(broadcast) 트래픽 비율

전체 패킷 중에서 방송 트래픽의 비율을 얻는다. 방송 트래픽이란 여러 다수의 시스템으로 패킷이 전송되어, 각 시스템에서는 패킷을 받아 자신이 목적지로 되어 있을 경우는 수신하고, 그렇지 않을 경우는 버리게 된다. 수신 쪽과 송신 쪽이 일대일로 존재하여 전송되는 유니 캐스트 트래픽은 이와 반대되는 경우에 해당한다.

$$traffic_{broadcast} = \frac{\sum_{i=0}^{T} (\text{ifInNUcastPkts} + \text{ifOutNUcastPkts})}{unicast + nonunicast}$$

$$unicast = \sum_{i=0}^{T} (\text{ifInUcastPkts} + \text{ifOutUcastPkts})$$

$$nonunicast = \sum_{i=0}^{T} (\text{ifInNUcastPKts} + \text{ifOutNUcastPkts})$$

◉ 시스템 패킷 입 출력율

단위 시간당 시스템에 입출력되는 IP 패킷의 비율이다.

$$traffic_{in} = \frac{\sum_{i=0}^{T} \text{ipInReceives}}{\Delta t_p}$$

$$traffic_{out} = \frac{\sum_{i=0}^{T} \text{ipOutRequests}}{\Delta t_p}$$

◉ 시스템 패킷 손실율

IP 계층을 통해 전달되는 송수신 패킷의 에러가 발생하는 비율을 나타낸다. 전체 시스템에서 손실이 일어난 입력 패킷의 비율과 출력 패킷의 비율을 나타낸다[6].

$\alpha_{ir} = ipInReceives$, $\alpha_{or} = ipOutRequests$,

$\alpha_{fo} = ipFragOks$, $\alpha_{fc} = ipFragCreates$

$\beta_{od} = ipOutDiscards$, $\beta_{onr} = ipOutNoRoutes$, $\beta_{ff} = ipFragFails$

$\gamma_{id} = ipInDelivers$, $\gamma_{ro} = ipReasmOks$,

$\gamma_{rr} = ipReasmReqds$, $\gamma_{fd} = ipForwDatagrams$

$$loss_{send} = \frac{\sum_{i=0}^{T} (\beta_{od} + \beta_{onr} + \beta_{ff})}{\sum_{i=0}^{T} (\alpha_{ir} + \alpha_{or} + \alpha_{fo} + \alpha_{fc})}$$

$$loss_{recv} = \frac{\sum_{i=0}^{T} (\alpha_{ir} - \gamma_{od} + \gamma_{onr} - \gamma_{ff} - \gamma_{fd})}{\sum_{i=0}^{T} (\alpha_{ir} + \alpha_{or} + \alpha_{fo} + \alpha_{fc})}$$

◉ 패킷 전달율

ip-forwarding-rate을 ip-input-rate으로 나누어주는 것에 의해 해당 개체의 패킷 전달율을 구할 수 있다. 이것은 해당 개체가 라우터의 역할을 담당한다는 것을 나타내는 ipForwarding의 값이 1일 때만 측정 가능하다.

$$pkt_{trans} = \frac{\sum_{i=0}^{T} ipForwDatagrams}{\sum_{i=0}^{T} ipInReceives}$$

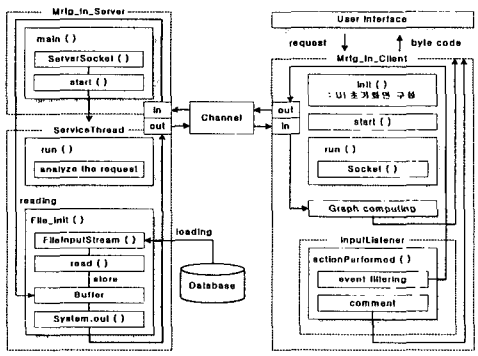
◉ 관리 트래픽율

전체 트래픽에 대한 관리 트래픽의 비율을 나타내는 것으로 관리 트래픽은 전송 서비스와 snmp 개체간에 주고 받는 메시지의 합을 나타내는 snmpInPkts과 snmpOutPkts로 이루어진다[2][3].

$$manage_{traffic} = \frac{\sum_{i=0}^{T} (snmpInPkts + snmpOutPkts)}{\sum_{i=0}^{T} (ipInReceives + ipOutRequests)}$$

2.3.3 관리자 인터페이스 제공자

관리자 인터페이스 제공자는 관리자 인터페이스로부터의 요청을 받아들여 자료 분석 처리 모듈에서 생성한 파일을 읽어 요청 받은 분석 항목의 데이터를 그래프로 화면에 보여주는 역할을 하게 된다. 이를 위해 관리자 인터페이스 제공자는 자바 클라이언트와 자바 서버로 구성된다. 자바 서버에서는 자바 클라이언트로부터의 접속을 기다리며 요청이 있을 경우, 요청 받은 데이터를 데이터베이스로부터 불러들여 이를 바이트 코드로 클라이언트에 전달하게 된다. 클라이언트는 이 데이터를 그래프로 화면에 나타낸다. [그림 3]은 관리자 인터페이스 제공자의 동작 과정을 도식화 한 것이다.

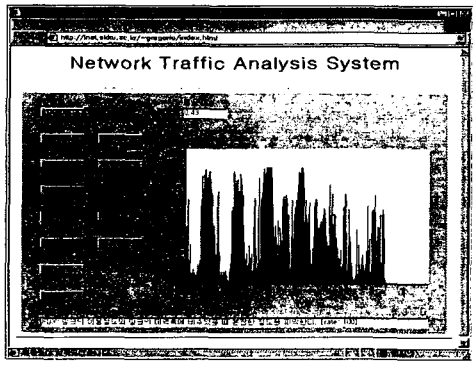


[그림 3] 관리자 인터페이스 동작 과정

자바 서버는 Mrtg_In_Server 클래스와 Service Thread 클래스로 구성되어 있다. .

3. 결과 분석

성균관대학교 라우터의 MIB 값을 중심으로 모니터링, 관리 정보를 수집, 이를 바탕으로 4.2 절에서 제시한 분석 항목들을 계산하였다.



[그림 4] 시스템의 가시화 화면 (활용율)

[그림 4]에서 보는 바와 같이 수집 기간동안 성균관대학교 라우터의 시간대별 활용율의 편차가 두드러지게 크게 나타나 사용시간대에 따라 혼잡(congestion) 상황이 발생할 수도 있음을 알 수 있다.

4. 결론 및 차후 연구과제

본 논문에서는 로컬 시스템에 저장되어 있는 관리정보를 원격지 시스템에서도 불러내어 이용함으로써, 웹 브라우저만 있는 곳이면 어디서든지 관리자가 한 눈에 네트워크의 이용현황을 파악할 수 있는 네트워크 관리 시스템을 구현하였다. 또한 일반적인 텍스트 기반의 정보가 아닌 그래픽 환경을 사용함으로서 사용자가 네트워크의 현황을 보다 더 직관적으로 파악할 수 있게 하였다. 이와 같은 시스템 분석 항목을 추출하여 가시화 하는 네트워크 분석 가시화 시스템은 네트워크의 활용, 관리, 유지측면에서 많은 도움이 될 것이며, 이러한 점은 현재의 TCP/IP 사용증가 추세에 비추어 볼 때 본 시스템의 활용도는 매우 크다고 하겠다. 추후 연구과제로써는 실시간적인 관리정보 데이터를 제공함으로서 현재 시간의 네트워크 관리 현황을 파악하도록 하는 것이다. 그리하여 어떤 네트워크 분석 항목의 값이 임계치를 초과할 경우에 이를 관리자에게 통보하여 보다 효율적인 네트워크 환경을 구축하도록 하는 것이다. 이와 같은 실험 환경을 위해서는 실제 라우터를 구축하는 일이 필요하다. 구축된 라우터를 통해 전달되는 패킷이 어느 특정 인터페이스에 집중되어 있다면, 나머지 패킷의 출력 경로를 다른 인터페이스로 재조정함으로서 각각의 인터페이스마다의 부하 정도를 조절할 수 있어 보다 나은 네트워크 운영이 가능할 것이다.

7. 참고문헌

[1] Mark A. Miller, "Managing Internetworks with SNMP" 3rd Ed, M&T Books, 1999

[2] Allan Leinwand, Karen Fang Conroy, "Network Management : A Practical Perspective", 2nd Ed, Addison-Wesley Publishing Company, pp. 8-56, 1996

[3] William Stallings, "SNMP, SNMPv2, and CMIP : The Practical Guide to Network-Management Standards", 2nd Ed, Addison-Wesley Publishing Company, 1993

[4] Jae-Oh Lee, "Enabling Network Management using Java Technologies", IEEE Communications Magazine, January, 2000

[5] William Stallings, "SNMP, SNMPv2, SNMPv3, and RMON 1 and 2", 3rd Ed, Addison-Wesley Publishing Company, 1995

[6] 신상철, 안성진, 정진욱, "Design and Implementation of SNMP-based Performance Parameter Extraction System", APNOMS, October, 1997