TraZer : 효율적인 네트워크 관리를 위한 트래픽 분석기의 구현

이상영*, 민지영**, 이상도*, 장범환*, 정태명**
*성균관대학교 전기전자 및 컴퓨터 공학과
**성균관대학교 전기전자 및 컴퓨터 공학부
e-mail:{sylee, zymin, sdlee, bhchang}@rtlab.skkr.ac.kr
tmchung@ece.skku.ac.kr

TraZer : Implementation of Traffic Analyzer for Efficient Network Management

Sang-Young Lee*, Zee-Young Min**, Sang-Do Lee*,
Beom-Hwan Chang*, Tai-Myoung Chung**
*Dept. of ECE, Sunhkyunkwan University
**School of ECE, Sungkyunkwan University

요약

인터넷의 기하 급수적인 발전과 더불어 네트워크 기반의 서비스가 확대되고 있다. 따라서 이전까지의 호스트 기반의 네트워크 관리와 더불어 트래픽 기반의 네트워크 관리가 요구되고 있으며, 이에 본 논문에서는 트래픽 기반의 네트워크 관리 시스템에 대하여 알아보고자 한다. 현재 개발된 시스템과 같은 단순한 트래픽의 모니터링과 분석뿐만 아니라 통계 정보를 제공하는 시스템을 제안하고, 시스템의 설계와 구현에 대하여 논의한다. 본 시스템은 프로토콜의 발신지와 목적지 그리고 프로토콜의 크기 등의 분석과 통계를 제공함으로서, 네트워크의 성능 뿐 아니라 장애 및 보안 관리에도 유용할 것이다.

1. 서론

인터넷(Intenet)이 1960년대 말 미국 국방성의 컴퓨터 통신망인 ARPANET[1]으로 시작된 후 기하급수적으로 발전하였다. 더욱이 최근에는 초고속 통신망의 보급 확대와 네트워크 기반의 콘텐츠 혹은 서비스가 대량으로 양산됨에 따라, 네트워크의 트래픽은 날로 증가하고 있다. 따라서 기존의 호스트 관리 기반의 네트워크 관리 개념을 넘어서 새로운 네트워크 관리 개념을 요구하게 되었고, 이러한 요구에 따라 네트워크의 트래픽을 모니터링하고 분석하는 시스템이 개발되었다.

모니터링 시스템은 tcpdump[2]와 솔라리스의 snoop, HP-UX의 nettl 등으로 현재 네트워크에 트래픽 정보를 표현하지만 단순한 모니터링에 그치고 있으며, 트래픽을 분석하는 시스템은 MRTG(Multi Router Traffic Grapher)[3] 등이 있다. 분석 시스템은 네트워크 상의 트래픽 정보를 저장·분석하고 그래프 등으로 표현하지만, 트래픽의 과부하나 장애 문제에 대한 정보를 제공해주지 못하는 단점이 있다.

본 논문에서는 트래픽 모니터링을 통한 분석과 통계를 산출하는 관리 시스템에 대하여 설명하고자 한다. 개발된 시스템은 에이전트와 마스터 그리고 클라이언트가 분리된 구조로서, 모니터링한 정보에 대한 분석과 통계 산출 등의 네트워크 성능 및 장애 관리에 활용할 수 있는 장점이 있다. 또한 웹 기반 구조로서 시스템 환경에 독립적이고, 확장성이 있어 트래픽의 과도한 증가 등의 문제에도 성능 저하의 문제가 발생하지 않는다.

본 논문의 구성은 2장에서는 기존의 트래픽 분석 시스템에 대한 비교 설명을 하고, 3장에서는 본 논문에서 개발한 트래픽 분석기의 설계와 구조에 대하

여 살펴본다. 그리고 4장에서는 트래픽 분석기의 구현과 장단점에 대하여 알아보고, 마지막으로 5장에서는 본 논문의 결과와 향후 계획에 대하여 살펴보겠다.

2. 관련연구

기존에 개발되어 있는 트래픽 모니터링 도구 중 Lawrence Berkley National Laboratory의 tcpdump와 Tobias Oetiker의 MRTG에 대하여 비교 설명한다.

2.1 tcpdump

tcpdump는 Lawrence Berkley National Laboratory에서 개발한 네트워크 트래픽 모니터링 도구이다. tcpdump는 네트워크 인터페이스를 거치는 패킷들 중, 주어진 조건식을 만족하는 헤더를 출력해 주는 프로그램으로 Libpcap(Protocol Capture Library)을 사용한다. Libpcap은 플랫폼(Platform)과 상관없이 동일한 방법으로 패킷들을 캡쳐한다.

tcpdump는 사용자에게 로컬 사용자의 외부로의 커넥션들을 감시하고, 또 특정 침입자가 침투 경로로 자주 이용하는 호스트, 혹은 원하지 않는 호스트로부터의 커넥션을 실시간으로 감시할 수 있게 해주는 등 간편하고 강력하다.

하지만, 이미 정의되어 있는 조건식 등이, 오히려, 사용자에게는 한계가 되기도 한다. 그리고 GUI 환경을 제공하지 않기 때문에, 분석 및 통계 시스템으로는 한계가 있다.

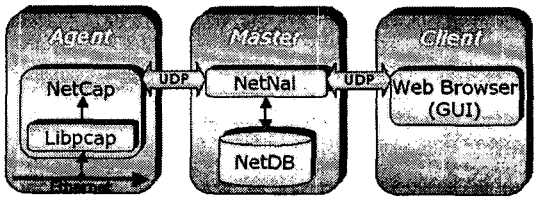
2.2 MRTG(Multi Router Traffic Grapher)

MRTG는 SNMP(Simple Network Management Protocol)[4]를 이용한 네트워크 링크 간의 트래픽 부하량 측정 도구로서, 트래픽을 모니터링하여 MIBII (Management Information BaseII)[4]의 In/Out 옥텟(octet) 정보를 알려주며 PNG(Portable Network Graphics) 혹은 GIF(Graphics Interchange Format) 형식의 그래프를 생성한다. 이 정보는 HTML로 문서화되며, SNMP의 요구를 수행하는 Perl과 SNMP로 수집된 트래픽 데이터의 로그 계산을 수행하는 C로 작성된 모듈로 구성 되어있다.

MRTG는 다양한 플랫폼을 지원하고, 트래픽 정보를 로그 파일에 저장하고 있어 정보를 기간별로 제공해줄 수 있다. 그러나 네트워크 관리자가 장애 문제 해결에 있어서 가장 필요한 정보들을 제공해 주지 못한다는 단점이 있다.

3. TraZer(Traffic Analyzer)의 구조와 기능

TraZer는 에이전트, 마스터 그리고 클라이언트 구조로 되어있으며, [그림 1]과 같이 구성되어 있다.



[그림 1] 트래픽 분석기의 구조

에이전트는 단일 세그먼트(Segment) 내 링크 레이어(Link Layer) 상의 패킷 헤더를 읽어서 마스터로 전송하며, 마스터는 전송된 패킷 정보를 NetDB(데이터 베이스, NETwork DataBase)에 저장한다. 그리고 클라이언트에서 패킷 정보 즉, 트래픽 분석 및 통계에 대한 요구가 있을 때, 그 요구에 맞게 정보를 클라이언트로 전달한다. 마지막으로 클라이언트는 웹브라우저에서 구동되며, 마스터에서 전달된 분석과 통계 정보를 표현한다.

TraZer의 각 구성 요소들은 UDP로 통신을 하며, 이는 TCP보다 오버헤드(Overhead)가 적고, 대기 시간이 적기 때문이다.

3.1 에이전트(Agent)

에이전트인 NetCap(NETwork CAPturer)은 Libpcap 0.4[5]을 사용하여 모니터링하고, 패킷 정보를 마스터로 전달하는 역할을 한다. 클라이언트로부터 전달된 설정, 즉 모니터링 간격(Interval)을 바탕으로 주기적으로 패킷 정보를 마스터로 전달한다. 트래픽의 과도한 증가에도 패킷 정보를 잃지 않기 위하여 패킷 캡쳐 부분과 마스터의 통신 부분을 독립적인 쓰레드로 구성하였고, 그 결과 패킷 정보의 유실을 최소화 하였다.

모니터링 대상은 단일 세그먼트, 즉 동일 네트워크 상을 대상으로 하며, 프로토콜이나 서비스에 관계없이 모든 패킷의 정보를 가져온다. 패킷 정보는 패킷을 현재 날짜와 시간, 패킷 헤더의 필드 정보를 말한다. 패킷의 헤더에서 얻을 수 있는 정보는 발신지(Source) IP 주소와 포트(Port) 번호, 목적지 IP 주소와 포트 번호 그리고 서비스별 프로토콜 정보와 패킷의 크기(Size) 등이다.

종합해보면, 에이전트는 UDP를 통하여, 마스터의 제어를 받고, 마스터에게 읽어온 패킷 정보를 전

달한다.

3.2 마스터(Master)

마스터의 구성 요소인 NetNal(NETwork aNALyser)은 NetCap에서 주기적으로 전달된 패킷 정보를 NetDB에 저장하고, 저장된 정보를 클라이언트의 요구에 맞게 전달하는 역할을 한다.

NetDB는 NetCap으로부터의 패킷 정보를 저장하는 데이터베이스로서, 날짜와 시간, 발신지 IP 주소, 발신지 포트 번호, 목적지 IP 주소, 목적지 포트 번호, 서비스 프로토콜 그리고 패킷 크기 등의 8개의 필드를 가지며, 이후 필드는 확장 가능하다.

NetNal은 두 개의 UDP 포트를 가지고 있으며, 하나는 NetCap으로부터 주기적인 패킷 정보를 기다리는 포트이고, 다른 하나는 클라이언트의 요구를 받아 패킷 정보를 전달하는 포트이다.

3.3 클라이언트(Client)

클라이언트는 웹브라우저 상에서 동작하는 웹 기반의 Java 애플릿으로서, TraZer 독자적으로 동작하는 형태와 네트워크 성능 및 장애 관리 시스템에 포함되어 트래픽 분석 역할을 하는 두 가지 형태가 있다. 클라이언트는 GUI를 제공하며, 조회하고자 하는 기간과 시간의 설정할 수 있는 설정부분과 NetNal로부터의 조회 정보를 표현하는 부분으로 나누어져 있다.

클라이언트는 단순히 패킷의 정보만을 열람하는 것이 아니라, 사용자의 요구에 따른 혹은 기본적인, 정보 조회 설정에 따른 트래픽의 분석을 한다. 따라서 단순히 트래픽의 모니터링이나 분석이 아닌 정확한 분석과 통계 정보가 산출된다. 이러한 정보는 네트워크 성능 및 장애 관리 시스템에서 유용한 정보가 되며, 사용자는 조회 설정을 통하여 자신에게 필요한 정보를 얻을 수 있다.

4. 시스템 구현

이 장에서는 TraZer의 구현된 시스템의 구조와 기능에 대하여 설명하고, 장단점에 대하여 알아본다.

4.1 개발 환경

웹 기반의 TraZer의 개발 환경은 다음과 같다. [표 1]은 에이전트의 개발 환경이다.

구성 요소	개발 환경
운영체제(커널)	Linux Kernel 2.4.2
모니터링 도구	Libpcap 0.4
컴파일러	gcc 2.96

[표 1] 에이전트의 개발 환경

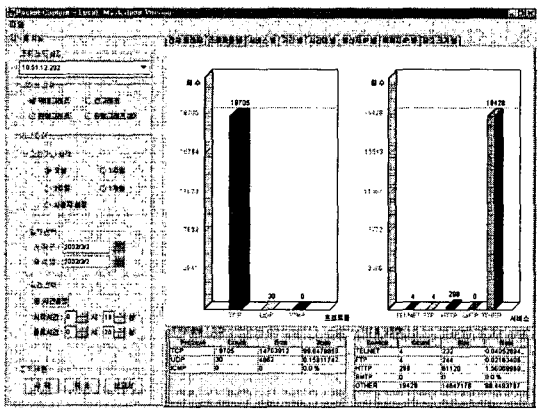
에이전트는 C로 작성되어 있고 마스터는 Java로 되어있다. [표 2]는 마스터의 개발 환경이다.

구성 요소	개발 환경
운영체제	Solaris 7
데이터베이스	MySQL 3.23.36
웹 서버	Apache 1.3.20(Unix)
컴파일러	jdk 1.3

[표 2] 마스터의 개발 환경

4.2 시스템 기능

이 절에서는 실제 구현된 TraZer의 실행 결과 화면을 살펴본다. [그림 2]는 TraZer의 프로토콜 별 통계 화면이다.



[그림 2] TraZer의 프로토콜 별 통계

[그림 2]에서 좌측은 조회 설정 패널이고 우측이 결과 패널이다. 설정은 기간과 시간 등이 설정 가능하고 프로토콜이나 서비스 별로 조회 설정이 가능하다. 또한 발신지와 목적지의 IP 주소와 포트 번호별 설정이나 크기별 설정도 할 수 있다.

그리고 결과 화면 중 왼쪽은 프로토콜별 트래픽 분포이며, TCP, UDP 그리고 ICMP로 분류한다. 그

래프는 프로토콜 별로 패킷의 개수로 표현한 것이고 아래의 테이블은 프로토콜 별로 패킷의 개수와 크기 그리고 비율을 나타내고 있다.

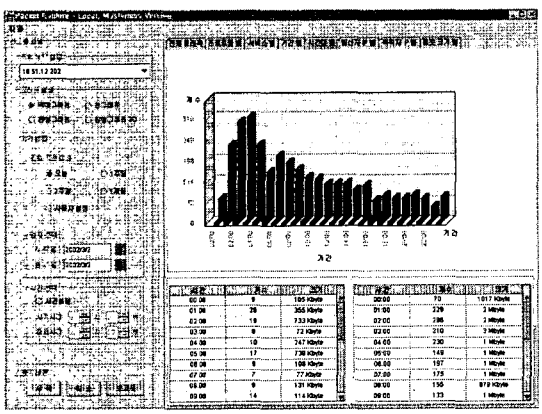
오른쪽의 서비스별 트래픽 분포에서는 TELNET, FTP, SMTP, HTTP, POP 등의 서비스 별로 분류되고, 프로토콜 별 트래픽 분석과 마찬가지로, 그래와 테이블로 표현된다.

이 외에도 설정한 기간별, 시간대별, 발신지와 목적지의 IP별로 분석을 할 수 있으며, 패킷의 크기별로 통계를 계산할 수도 있다.

4.3 장점 및 활용

TraZer는 이전의 트래픽 분석기나 모니터링 도구와는 달리 에이전트와 마스터 그리고 클라이언트가 다른 컴퓨터에 존재하여도 되기 때문에 네트워크의 과부하와는 상관없이 시스템 저하 등의 일이 발생하지 않는 것이 큰 장점이다. 그리고 단순히 트래픽의 모니터링과 분석이 아닌 모니터링과 분석에 이은 통계 정보를 통하여 장애나 네트워크의 특성을 분석할 수 있다. 이것은 트래픽 분석기로서 뿐만 아니라 네트워크 관리 시스템에서도 유용한 정보가 된다. 또한 각 패킷의 시간과 크기 등의 자세한 정보를 저장하는 것도 장점이다.

이전의 트래픽 분석기는 네트워크 성능과 관련된 컨설팅 용도로 사용되었다. 그러나 TraZer는 트래픽의 자세한 분석과 통계 산출을 바탕으로 컨설팅뿐만 아니라 장애 및 성능 그리고 보안 관리에도 사용될 수 있다. 예를 들어, 어떤 세그먼트 상의 컴퓨터가 Nimda 바이러스에 감염되었다고 가정하자. 감염된



[그림 3] TraZer의 시간대 별 통계 화면

컴퓨터는 세그먼트에 대량의 트래픽을 발생할 것이다. 이런 경우, TraZer는 평소의 트래픽과는 다른 상황을 그래프 혹은 테이블로서 명확히 나타낼 것이다. [그림 3]은 TraZer의 시간대별 분석 화면이다.

이와 같이 어떤 바이러스나 서비스 거부 공격(Denial of Service) 등의 사이버 공격에 대한 보안 관리를 할 수 있다. 또한 세그먼트 상의 불특정 컴퓨터나 링크의 장애와 성능 관리를 할 수 있다.

5. 결론 및 향후 계획

인터넷이 대중화되고 보편화되면서, 산업 자체도 네트워크 기반으로 변하고 있다. 제공되는 서비스 또한 다양해지고 있으며, 콘텐츠도 VOD(Video On Demand), AoD(Audio on Demand) 등의 Streaming 서비스가 주류를 이루고 있다. 따라서 대역폭의 소모가 높은 정보의 서비스가 많아지면서, 이제는 호스트 기반의 관리뿐만 아니라 네트워크 트래픽 기반의 관리가 필요하게 되었다.

TraZer는 단순한 트래픽 모니터링 시스템이 아닌 트래픽의 분석과 통계 정보를 제공하는 시스템이다. 따라서 트래픽 분석을 통하여 발신지 혹은 목적지 통계 분석을 수행하고, 대역폭의 조절 등의 네트워크 성능 관리를 할 수 있고, Nimda와 같은 특정 프로토콜, 발신지의 폭주 등을 분석하여 장애 및 보안 관리 또한 할 수 있다.

앞으로 패킷의 헤더의 정보뿐만 아니라 패킷의 데이터(Payload의 정보)의 분석에 대한 연구가 필요하다.

참고문헌

[1] Michael Hauben, "History of ARPANET", http://www.dei.isep.ipp.pt/docs/arpa-Contents.html.

[2] Lawrence Berkley National Laboratory, "tcpdump 3.4".

[3] Tobias Oetiker, Dave Rand, "MRTG : Multi Router Traffic Grapher", http://people.ee.ethz.ch/~oetiker/webtools/mrtg/mrtg.html.

[4] William Stallings, "SNMP, SNMPv2, SNMPv3, and RMON 1 and 2", Addison Wesley Longman, Inc., 1996.

[5] Steve McCanne, Craig Leres, and Van Jacobson, "PCAP library, README", Lawrence Berkeley National Laboratory, Network Research Group, 1996.