임베디드 리눅스를 이용한 IPv6 기반의 트래픽 모니터링 시스템 설계

이용우, 김광현
광주대학교 정보통신공학과
e-mail:lyw@info.gwangju.ac.kr, ghkim@hosim.gwangju.ac.kr

Design of Traffic Monitoring System based on IPv6 using Embedded Linux

Yong-Woo Lee, Gwang-Hyun Kim
Dept of Information and Communciation Engineering, Gwangju University

요 약

급증하는 인터넷 사용자와 함께 인터넷 트래픽도 급격히 증가함으로 인하여, 한정된 네트워크 자원에 대한 효율적인 네트워크 관리의 필요성이 중요한 이슈로 등장하고 있다. 본 논문에서는 Libpcap 라이브러리를 이용하여 패킷을 수집하는 Tcpdump를 임베디드 리눅스 시스템에 적용하여 차세대 인터넷 프로토콜인 IPv6기반에서 트래픽 모니터링을 함으로써, 효율적인 네트워크 관리를 위한 기술을 제안한다. 본 트래픽 모니터링 시스템은 임베디드 리눅스를 이용하여 IPv6 패킷을 수집 및 분석하고, 측정된 트래픽 모니터링의 정보를 바탕으로 네트워크 장비들을 효율적으로 관리 및 제어할 수 있는 트래픽 측정 모델을 설계하였다.

1. 서론

최근 인터넷은 새로운 응용프로그램과 네트워크의 고속화로 인해 그 수요는 한층 더 폭발적으로 증가하고 있다. 이러한 인터넷의 지속적인 발달로 인하여 시간과 공간의 제약없이 인터넷을 사용하고 있으며, 이로 인하여 발생하는 인터넷의 트래픽은 지수적으로 증가하고 있는 추세이다[3]. 또한, 사용자의 요구를 충족시키기 위한 다양한 서비스의 제공으로 인하여, 네트워크의 사용량과 그 활용 분야는 더욱 광범위해지고 있다. 이는 네트워크 및 시스템의 무분별한 사용과 설비에 대한 불필요한 투자를 방지하고, 좀 더 효율적으로 자원을 관리해야 할 필요성을 야기시킨다. 이를 위한 정확한 네트워크 트래픽 분석에 대한 요구가 현재 네트워크 관리 측면에서 중요한 이슈로 등장하고 있다. 이에 따라 어느곳에서, 어떤 형태로, 얼마나 많은 트래픽이 유발되고 있는지를 알아내는 일은 네트워크 관리자들에게 당면한 중요한 과제가 되었다[4]. 이러한 트래픽 증가로 인한 네트워크 관리상의 문제점들은 현재 IPv4 기반의 네트워크 트래픽 측정뿐만 아니라, 앞으로 다가올 차세대 인터넷 프로토콜인 IPv6기반에서 네트워크 트래픽 측정을 통한 패킷 분석도 중요시 되고 있다. IPv6는 무한한 인터넷 주소 공간을 제공할 뿐만 아니라 정보보안, QoS, 이동성 및 자동 네트워킹 등 다양한 기능 등을 제공할 수 있다[6]. 본 논문에서는 앞으로 다가올 IPv6 기반에서 네트워크 및 시스템을 보다 효과적으로 관리하기 위하여, 임베디드 리눅스 시스템에 Tcpdump를 적용하여 IPv6 트래픽 모니터링 시스템을 설계 하고자 한다. 본 논문의 구성은 다음과 같다. 2 장에서는 네트워크 트래픽 측정 방법과, 본 논문에서 제안하고자 하는 임베디드 리눅스 시스템과 트래픽 측정 방법을 기술한다. 3 장에서는 2 장에서 제안한 트래픽 측정 방법을 이용하여, 트래픽 모니터링 시스템 설계 및 동작과정, 트래픽 모니터링 시스템 모듈구조에 대해 제안한다. 마지막으로 4 장에서 결론을 맺고 향후 연구과제에 대

해 언급하고자 한다.

2. 네트워크 트래픽 측정 방법

네트워크 트래픽 측정은 그 사용 목적에 따라서 측정방법이 다양하게 분류될 수 있다. 트래픽 측정 및 분석 방법에 따라 크게 능동적 측정 방법과 수동적 측정 방법이 있다. 현재 네트워크 관리를 위해서 NMS(Network Management System)에서 사용되는 SNMP(Simple Network Management protocol)기반의 수동적 측정방법이 가장 널리 사용되고 있다[5].

그러나 SNMP는 SNMPv2를 거쳐 SNMPv3 까지 개선되어 있는 상황이지만, 결국 일시적인 MIB(Management Interface Base)값을 보여주는데 그치고 있기 때문에, 관리 프로토콜 자체만으로는 네트워크를 분석하거나 모니터링 할 수 없고, SNMP를 활용하는 부가적인 도구의 개발이 필수 적이다[1][2]. NMS는 우선적으로 장애 관리에 그 초점이 맞추어져 있기 때문에 네트워크 품질을 파악하여, 사용자에게 QoS를 제공하는 것은 여러가지 방법을 동원해야 가능하다.

2.1 능동적 트래픽 측정방법

능동적 트래픽 측정방법은 시험 패킷을 목적지에 주기적으로 전송하여 성능 측정을 위한 트래픽 발생을 이용하는 측정 방법으로, Ping, Traceroute, 등이 있다. 이 방법은 실시간으로 트래픽 분석할 수 있는 장점은 있으나, 기존 트래픽에 부하를 가중시키며 또한 패킷 손실이 아닌 정보의 손실이 존재할 수 있어, 정확한 데이터를 분석하는데 어려움이 있을 수 있다. 이 외에 호스트간 네트워크 성능을 측정하는 방법으로 한정된 시간동안 단순히 TCP/UDP 데이터를 전송 시켜서 측정된 데이터양을 계산하여 트래픽을 측정하는 Netperf, 한 호스트에서 여러 호스트로 트래픽을 측정하는 PingER, 호스트에 트래픽 측정 장치를 구축하고 장치간 트래픽을 측정하는 Surveyor 등이 있다.

2.2 수동적 트래픽 측정방법

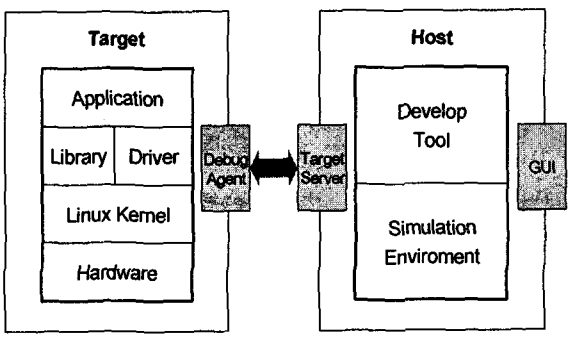
수동적 측정 방법에는 네트워크 장치의 기능을 활용하는 방식으로 NMS 프로토콜인 SNMP MIB정보 등을 읽어 들여, 단순히 네트워크 상황을 수집 및 분석하여 적절한 그래프를 생성시켜 웹 상에서 트래픽을 관찰 할 수 있게 해주는 MRTG(Multi Router Traffic Grapher)가 있다. 그러나 MRTG는 이렇게 인터페이스별 트래픽의 가시화를 통해 네트워크 상의 데이터 흐름 정도를 아주 잘 표현해 주지만, 트래픽의 타입이나 통계와 같은 부가적인 정보를 제공하지 못한다[9]. 이 외에 네트워크 장비에서 패킷 종류를 분류하여 분석하는 형태인 Cflowd, Libpcap 패킷 라이브러를 이용하여 패킷을 수집하는 Tcpdump등이 있다[10][11].

2.3 임베디드 리눅스 시스템을 이용한 트래픽 측정방법

2.3.1 임베디드 리눅스 시스템

임베디드 리눅스 시스템이란 마이크로 컨트롤러를 비롯한 하드웨어와 특정 기능을 수행하는 소프트웨어를 지원하기 위하여 운영체제로서의 리눅스를 의미한다. 그 응용 범위는 네트워크 장비를 비롯하여 가전제품, PDA, 셋톱박스 등에 이르기 까지 그 응용 범위가 매우 다양하다.

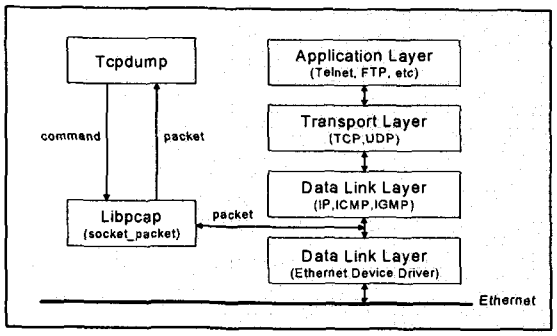
임베디드 리눅스 시스템은 WidowsCE, VxWorks 및 PalmOS 등의 상용 내장형 커널도 많이 사용된다[7]. 상용 운영체제가 가격이 비싸고 커널자체에 대한 수정이 불가능하다는 단점을 가지는데에 반하여 리눅스는 많은 장점을 가지고 있다. 예를 들면, 상용 커널과 동일한 기능을 제공하고 있으며, 커널에 대한 소스코드의 수정이 매우 용이하고 원하는 기능만으로 구성되는 작은 크기의 커널도 만들 수 있다. 또한, 개발과정에 필요한 많은 도구 소프트웨어는 물론 응용 프로그램들이 공개되어 있기 때문에 추가 소프트웨어 구입 비용 없이도 양질의 소프트웨어를 사용 할 수 있어서 개발 시간을 단축시킬 수 있다[12][13]. 본 논문에서 이러한 이유로 인하여 임베디드 시스템으로 리눅스를 탑재하여 트래픽 모니터링 시스템 모델 설계를 제안하고자 한다. [그림 1]은 임베디드 리눅스 개발 환경 구성도이다[8].



[그림 1] 임베디드 리눅스 개발 환경 구성

2.3.2 임베디드 리눅스 기반의 트래픽 측정방법

임베디드 리눅스는 많은 드라이버 소스코드와 커널 소스코드가 오픈 되었기 때문에 커널 프로그래밍을 설계하고 구현하는 것이 용이하다. 본 논문에서 트래픽 모니터링 시스템은 수동적인 트래픽 측정방법으로 Libpcap 이라는 독립적인 패킷캡처링 라이브러를 이용하여, 다양한 운영체제에서 널리 이용되고 있는 Tcpdump를 적용하여 네트워크 상태 정보를 모니터링 할 수 있는 트래픽을 측정 시스템을 설계하고자 한다. Tcpdump의 막강한 패킷필터는 네트워크 상에서 발생되고 있는 특정한 패킷들을 실시간으로 기록해 줄 수 있으며, 이를 이용하여 네트워크에서 벌어지는 일들을 네트워크 관리자 원하는 대로 모니터링할 수 있게 해 준다. 또한, 네트워크 상에서 전송되는 패킷의 헤더 정보를 다양한 옵션들을 가지고 자세하게 보여주는 장점을 가지고 있다. [그림 2]는 Tcpdump를 이용한 패킷수집 과정으로서 socket_packet 타입의 소켓을 사용하여 데이터 링크 계층에서 이더넷 디바이스를 통해 수신된 패킷을 필터링한 후 처리된 값들을 캡쳐한다.



[그림 2] Tcpdump를 이용한 패킷 수집과정

Tcpdump는 수집된 패킷의 결과값을 [그림 3]과 같은 파일 형식으로 저장한다.

SEQ-NO	Src-Node	Dest-Node	Protocol	Port

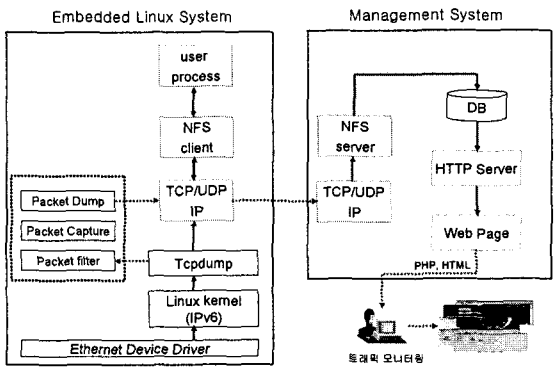
[그림 3] Tcpdump 파일 저장 구조

SEQ-NO는 패킷을 카운트하는 일련번호이고, Src-Node, Dest-Node는 특정 패킷의 전달과 관련한 송수신 노드를 의미한다. Protocol 필드는 TCP나 UDP등의 프로토콜 번호를 저장하고, Port 필드는 각 응용서비스의 포트번호를 저장하여 각 노드별, 프로토콜별, 포트별 패킷 량과 노드 상태 등을 본 논문에서 설계할 관리시스템에서 웹 인터페이스 애플리케이션으로 트래픽 모니터링을 할 수 있다.

3. 임베디드 리눅스 시스템을 이용한 트래픽 모니터링 시스템 설계

3.1 임베디드 리눅스 트래픽 모니터링 설계

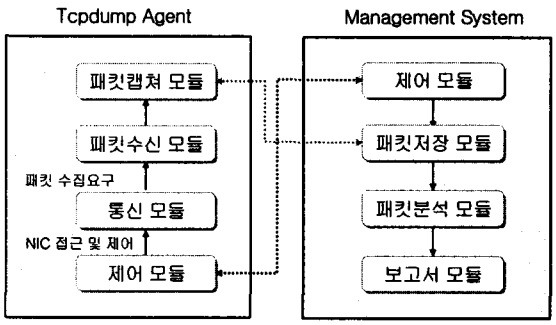
본 논문에서 설계하고자 하는 임베디드 리눅스 트래픽 모니터링 시스템은 네트워크 장비 및 트래픽을 분석 및 관리하며, 이를 기반으로 네트워크의 원할한 동작을 감시할 수 있는 기능을 제공하고자 한다. 네트워크 관리자가 웹 브라우저를 통해 관리시스템에 접속함으로써 일련의 네트워크 및 시스템의 트래픽 모니터링을 할 수 있도록 한다. 본 트래픽 모니터링 시스템은 [그림 4]와 같이 임베디드 리눅스 시스템, 관리 시스템으로 구성된다. 구체적으로 살펴보면 클라이언트 역할을 수행하는 임베디드 리눅스 시스템은 Tcpdump를 에이전트화 하여 네트워크 상에서 이동중인 모든 패킷들에 대한 정보를 읽어 들여 필터링 한 후 처리된 값들을 캡쳐한다. 이렇게 저장된 패킷은 Tcpdump 에이전트와 서버 역할을 수행하는 관리시스템 사이에 네트워크를 통한 NFS(Network File System)를 설정하여 관리시스템에 있는 DB에 저장하게 된다. 관리시스템에는 네트워크 관리자가 패킷의 트래픽을 관찰할 수 있도록 DB에 저장되어 있는, 패킷의 파일 자료를 액세스하여 웹 브라우저로 모니터링 할 수 있도록 웹 인터페이스 애플리케이션이 있다. 또한 리눅스 커널을 IPv6로 구성함에 따라 IPv4 패킷 뿐만 아니라 IPv6 패킷도 읽어들여 패킷 필터링과 패킷을 캡쳐하여 패킷 분석이 가능하도록 구성하였다.



[그림 4] 임베디드 리눅스 트래픽 모니터링시스템 설계

3.2 임베디드 리눅스 트래픽 모니터링 시스템 모듈 구조

본 논문에서 설계하고자 하는 임베디드 트래픽 모니터링 시스템 모듈구조를 살펴보면 [그림 5]와 같이 Tcpdump 에이전트와 관리시스템 사이의 패킷 수신 및 분석 모듈이 있다. Tcpdump 에이전트와 관리시스템은 네트워크를 통한 NFS로 설정되어 있다. Tcpdump 에이전트의 모듈 과정을 살펴보면 패킷 수신, 패킷 캡쳐로 이루어진다. 네트워크 관리자로부터 요청이 들어오면 네트워크로부터 NIC버퍼에 수신되는 모든 패킷을 필터링 하여, 각 프로토콜 계층에 따라 패킷 저장과 분석을 통해 네트워크 관리자가 트래픽 모니터링을 할 수 있는 구조이다.



[그림 5] Tcpdump 에이전트와 관리시스템의 모듈구조

4. 결론 및 향후 연구과제

네트워크 기반의 다양한 응용 프로그램 개발에 따른 급속한 네트워크 트래픽 증가로 인하여, 네트워크 트래픽 측정 및 분석 작업이 필수적인 요소로 인식되고 있다. 이러한 트래픽 증가로 인한 네트워크 관리상의 문제점들은 현재 IPv4 기반의 네트워크 트래픽 측정뿐만 아니라, 앞으로 다가올 차세대 인터넷 프로토콜인 IPv6 기반에서의 네트워크 트래픽 분석도 중요시 되고 있다. 본 논문에서는 IPv6 기반에서의 네트워크 및 시스템을 보다 효과적으로 모니터링 함과 동시에 일관성 있고 통합된 방식으로 한정된 네트워크 자원을 관리하기 위한 방법으로, 저 비용의 임베디드 리눅스 시스템을 이용하여 IPv6 기반에서 트래픽 모니터링 시스템을 설계하였다.

향후 연구과제로는 본 논문에서 제안한 설계 모델을 기반으로 트래픽 모니터링 시스템을 직접 구현하고자 한다. 또한, IPv6 기반에서의 트래픽 측정을 통하여 실제 구현상의 문제점을 살펴보고, 효율적인 네트워크 관리를 위해 추가할 수 있는 제어 기능들에 대한 연구가 필요하다. 네트워크 관리는 QoS와 같은 네트워크 품질보증 서비스와 차별화된 서비스 제공을 위해 다가올 IPv6 기반 네트워크에 필요하며, 정책기반 네트워크 관리에 많은 도움을 줄 수 있을 것이다.

참고문헌

[1] RFC 1157, A Simple Network Management Protocol(SNMP), May. 1990.

[2] W. Stallings, SNMP, SNMv2, SNMPv3 and RMON 1 and 2, Addison Wesely, 1999.

[3] 김대은 외 3명, "멀티에이전트를 이용한 인터넷 트래픽 측정", 한국정보처리학회, 춘계 학술 발표대회, 2003년 5월.

[4] 오도은, 이진기 "Netflow 기반 실시간 네트워크 트래픽 분석 시스템 설계 및 구현", 한국통신학회, 추계종합학술 발표회, 2002년 2월.

[5] 정태수, 윤승현, 양지호 "인터넷 트래픽 측정 시스템 개발", 한국정보처리학회, 추계 학술발표 논문집 제 8권 제2호, 2001년 11월.

[6] IPv6 포럼 코리아, "차세대 인터넷 프로토콜 IPv6", 2002.

[7] 노영욱, 변정용, 이정배 "임베디드 리눅스 개발 도구 기술 동향", 한국정보처리학회지, 제 9권 1호, 2002년 1월.

[8] 은성배, 한상숙, 진성기 "임베디드 시스템 프로그래밍 교육론 및 교육용 장비 개발사례, 한국정보과학회, 제 20권 7회, 2002년 7월.

[9] Tobias Oetiker and Dave Rand, MRTG http://people.ee.ethz.ch/~oetiker/webtools/mrtg/

[10]CAIDA,"cflowd"http://www.caida.org/tools/measurement/cflowd

[11] http://www.tcpdump.org

[12] http://www.kelp.or.kr

[13] http://www.linux-nm.org