한국컴퓨터정보학회 동계학술대회 논문집 제22권 제1호 (2014. 1)

임베디드 디바이스를 이용한 포터블 네트워크 트래픽 탐지 시스템

송재오°, 윤다영*, 이상문*
°(주)디엘커뮤니케이션즈
*한국교통대학교 컴퓨터정보공학과
e-mail:jeo@web-d.co.kr°, yunda0616@nate.com*, smlee@ut.ac.kr*

Portable Network Traffic Probing System using Embedded Device

Jeo Song°, Da Young Yun*, Sang Moon Lee*
°Research Center, DLCOMS Co.,Ltd.
*Dept. of Computer Science & Information Engineering, Korea Nat'l Univ. of Transportation

● 요 약 ●

하루가 다르게 최신의 기술이 쏟아져 나오는 정보화 시대에 들어서면서, 세계 ITC 분야는 디지털 기술과 유무선통신에 근간을 둔 인터넷의 확산으로 반도체, 컴퓨터, 콘텐츠 미디어, 정보가전 등 다양한 산업 분야가 융합되어 새로운 부가 가치를 창출하기에 이르렀다. 특히, 스마트 시대를 살아가는 우리의 일상생활은 모바일은 물론 일반적인 PC등을 사용한 인터넷 중심의 네트워크와 커뮤니케이션이 중요시 되고 있다. 이러한 시대의 흐름은 인프라 측면에서 네트워크의 트래픽을 폭증시키고, 많은 보안적인 문제를 야기하고 있다. 이에 임베디드 디바이스를 이용하여 네트워크를 운영하는 관리자에게 큰 도움을 주고, 업무 효율성을 높일 수 있는 포터블 형태의 네트워크 트래픽 탐지 시스템을 연구하게 되었다.

키워드: 네트워크 트래픽(Network Traffic), 네트워크 모니터링(Network Monitoring), 휴대용 임베디드(Portable Embedded)

I. 서 론

네트워크 모니터링 및 분석과 관련한 제품 몇 가지를 나열해 보면, 가장 대표적인 것이 바이러스, 웜, 스파이웨어 등 인터넷을 통해 유입되는 각종 악성코드에 대해 감시하는 기능 중심의 안티바이러스 제품군과 단위 네트워크별 방화벽 장치가 대부분이다. 이러한 제품들은 네트워크 설계 초기부터 구성요소로서 큰 비중을 차지하게 되고, 설치 후 변경이 난해하다. 즉, 네트워크의 관리자 입장에서는 네트워크의 특정 HOP에서 발생하는 트래픽을 위치 가변적으로 감시하고 분석하기가 어려울 것이다. 관리자에게는 보안적인 요소도 매우 중요하지만, 자신에게 편의성이 강조된 관리 도구나 시스템을 원할 것이다. 이에 네트워크상에서 누군가 접속을 끊거나, 어떤 일을 하는지, 어떤 일을 했는지 그리고 어디에서 접속해서 사용하고 있는지 등을 네트워크 HOP을 가변적으로 이동하며 트래픽을 모니터링하고 분석할 수 있는 포터블 형태의 네트워크 트래픽 탐지 시스템을 임베디드 디바이스를 이용하여 구현하게 되었다.

II. 관련 연구

인터넷 기반의 통신은 다양한 프로토콜 타입의 데이터 패킷을 송수신하게 된다.

본 연구에서 제안하는 네트워크 트래픽 탐지는 단순히 인터넷 트래픽의 전체적인 송수신량을 측정하는 것이 아니라, 송수신 데이터를 상기에서 언급한 다양한 프로토콜 타입의 데이터 패킷을 구분하고 각 패킷을 헤더, 플래그, 데이터 등의 비트 구조로 분석 할 수 있도록 도와주는 것을 목적으로 한다. 특히, 네트워크 보안이나 접속폭주 등의 문제가 발생할 때 가장 큰 변화를 보이는 TCP, UDP, IP, ICMP 패킷을 구분하고 그에 대한 상세 내용을 볼 수 있게 할 것이다.

1,500 bytes 이하의 IEEE802.3 프레임과 1,500 bytes 이상의 프레임을 구분하고, 특히 DIX 프레임에 중심적인 기능을 구현한다.[1]

모니터링과 분석을 통한 데이터는 시간에 따른 자료를 다룰 수 있는 도구인 RRD툴(RRDtool, round-robin database tool) 을 사용하여 그 결과를 정리하고, 그래프로 표현한다.

Round Robin은 고정된 크기의 데이터와 현재 element에 대한 포인터로 동작하는 기술로 현재 데이터를 읽고 쓸 때 포인터는 다음 element로 이동하게 된다. 시작과 끝이 없는 원과 같이, Round Robin 기술을 사용하면 계속해서 데이터를 읽고 쓰는 작업이 가능하다. 사용하는 중에도 모든 가용 위치에 대한 사용이 가능하며, 자동적으로 이전의 위치에 대한 재사용이 가능하다. 이러한 방법으로 데이터베이스는 크기는 증가하지 않지만 어떠한 인위적인 작업 없이 사용 가능하게 된다.

RRDTool은 이러한 Round Robin 기술을 이용한 데이터베이스를 구현하고 있으며, 데이터의 저장 및 검색이 가능하다. 정리하자면, 일정한 기간 동안 특정 포인트에서의 측정데이터를 취급하기에 유용한 데이터베이스이다. 그림1과 같이 RRDTool은 MRTG (Multi Router Traffic Grapher)를 근간으로 인터넷 회선의 사용량을 스크립트를 이용해 그래프로 표한하는 것으로 현재 온도, 속도, 전압 등의 측정 데이터를 그래프로 표현하는 툴로 널리 사용되고 있다.[2]

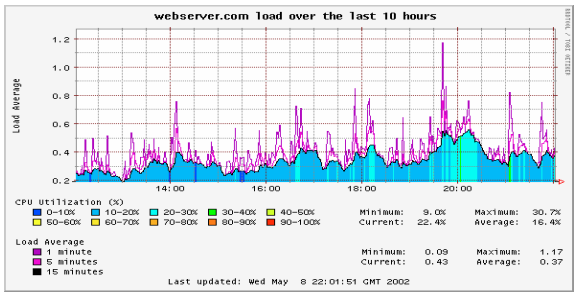

그림 1.RRDTool의 사용 예

III. 구현 및 실험

제안하는 시스템은 효율성을 높이기 위해 Tiny Embedded Device를 사용해 데이터 패킷을 탐지할 수 있도록 구현되었으며, 웹서버를 탑재하여 원격지에서도 실시간으로 감시가 가능하도록 하였다. 제안 시스템은 네트워크의 어떤 위치에서라도 트래픽을 캡처하고 분석 할 수 있고, 캡처되는 패킷은 프로토콜 종류별로 구분하고 그에 대한 카운트 기능을 구현하고 해당 정보를 네트워크 ID별로 데이터베이스화 한다. 아래 그림2는 제안 시스템에 대한 기본 구상도 이다.

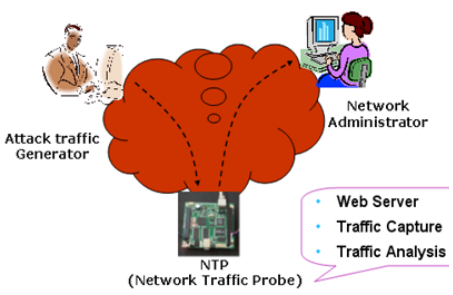

그림 2. 시스템 사용 구상도

패킷 캡처는 Packet_analysis라는 모듈을 중심으로 수행되며, 이를 특정 시간 단위로 실행시켜주는 별도의 보조 모듈로 제어한다. 그림3은 제안 시스템의 구성 개념을 보여주고, 그림4는 작동 흐름을 표현하고 있다.[3], [4]

그림 3. 시스템 개념도

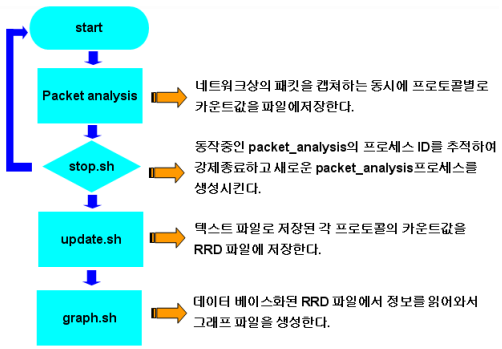

그림 4. 시스템 흐름도

그림5는 포터블 네트워크 트래픽 탐지 시스템의 로컬 작동 결과이다. IP, TCP, UDP, ICMP 중심의 패킷 캡처가 실행되고, 발신지와 목적지의 IP Address를 비롯하여 Port number 등의 상세한 Header 분석이 이루어지며 보다 정확한 통계를 위해 패킷별 카운터가 작동된다.[5]

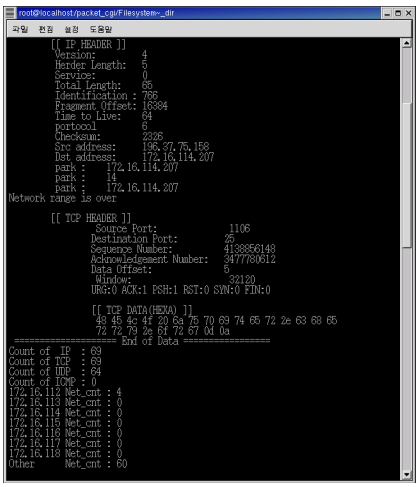

그림 5. 임베디드 디바이스의 로컬 시스템 구동

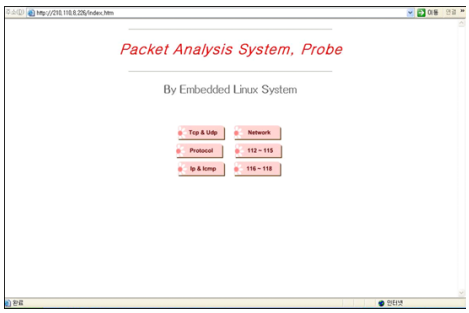

그림 6. 웹을 이용한 원격 접속 메인 페이지

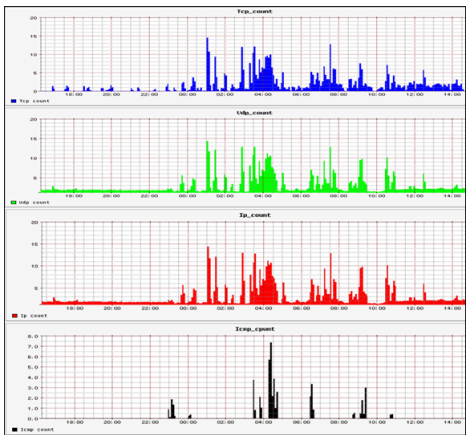

그림 7. 웹을 통한 원격 시스템 구동

그림6과 그림7은 임베디드 디바이스로 구현된 시스템을 바탕으로 웹을 통해 원격지에서 작동시키는 화면이다. 그림7의 가로축은 시간선상이며, 세로축은 각 시간대에 캡처된 패킷의 수를 나타낸다. 평소 상기 그림들과 같이 일정한 패턴으로 그려졌던 그래프가 특정 시간대나 요일에 갑자기 변한다면, 분명 해당 네트워크는 내부 또는 외부적인 요인으로 인하여 문제점이 발생한 것이 틀림없을 것이다. 아래 그림8은 원격지에서 네트워크 ID별로 트래픽을 상세하게 분석하는 화면이다.

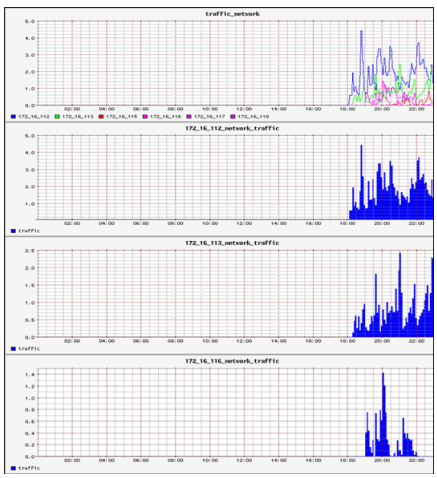

그림 8. 트래픽 상세 분석

본 연구에서는 정확한 네트워크 트래픽의 분석을 위하여 캡처된 데이터를 5분 단위로 정리하여 평균치를 구하여 사용하였다.

Interval = 시간 단위
n = 검출 패킷 수
x = 평균 패킷 수

위와 같이 가정한다면, 구하고자 하는 x의 값은 아래와 같은 비례식에 의해 구해질 수 있다.[6]

Interval:n = 1sec:x
1*n = x*Interval
∴ x = n/Interval

그림9는 본 연구에서 구현한 최종 결과물이다. 데이터베이스화를 위하여 하드디스크를 장착하였다. 그림10은 해당 데이터베이스의 내용이다. 데이터베이스 파일에는 각각의 날짜와 시간을 기준으로 발신지와 목적지 패킷에 대한 내용을 저장한다.[7], [8]

그림 9. Portable Network Traffic Probe

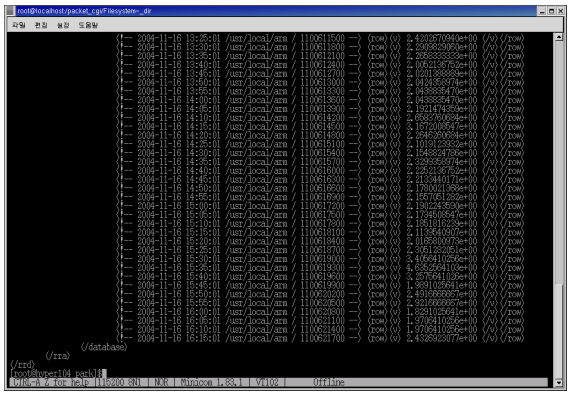

그림 10. 데이터베이스의 구성과 저장

본 시스템은 아래와 같은 시스템 환경에서 구현되었다. 표1은 하드웨어적 환경이며, 표2는 소프트웨어 환경이다.

표 1. Hardware Specification

Item	Description
Processor	Intel SA1110 400Mhz
SDRAM	Samsung 32Mbyte
FLASH	Intel strata flash 16Mbyte
Ethernet	CS8900A 10BaseT
USB	USB Slave
Serial	2 Port
JTAG	1 Port
RTC	RTC4513(Real Time Clock)
Connector	PC104 Interface, PC104 Plus Interface

표 2. Software Specification

Item	Description
O/S	LInux 2.4.x kernel
Device driver	CS8900 Ethernet
	Frame buffer
	USB Slave
	RTC4513(Real Time Clock)
File System	JFFS2, Ramdisk
GUI	TIny X Server

IV. 결 론

임베디드 디바이스를 이용한 포터블 네트워크 트래픽 탐지 시스템은 네트워크를 관리하는 실무자를 고려하여 연구를 시작하였다. 휴대성 그리고 업무적 효율성과 시스템 가용성 부분에서 네트워크 관리자에게 상당히 뛰어난 도구로서의 역할을 할 것이라 기대한다. 특히 휴대성과 더불어 웹 서버를 통한 원격 제어는 임베디드 라눅스의 뛰어난 장점이라고 판단되고 활용성을 높일 수 있다고 사료된다.

현재 시각화 수치의 결과는 꺽은 선형의 그래프만을 제공한다. 필요에 따른 다양한 종류의 그래프를 제공할 수 있다면 다각도의 분석도 가능할 것이다. 또한 데이터베이스 파일의 내용은 네트워크 트래픽 분석에 충분하다고 생각되지만, 해당 데이터베이스의 구성과 구조에 대한 사전 지식이 준비되지 않았을 경우 쉽게 이해될 수 없는 상태이므로, 이를 보다 일반적인 데이터베이스로 개선한다며 보다 사용자 중심적인 시스템이 될 것이다. 현재는 웹을 통해 네트워크 트래픽 탐지 결과에 국한된 수치와 그래프 정보만을 확인할 수 있다. 향후 웹을 통해 저장된 데이터베이스를 확인 할 수 있고, 그 방법 또한 검색 엔진 등을 통해 구현된 사용자 인터페이스를 제공한다면, 네트워크 관리자의 입장에서는 매우 효용성 및 활용성이 높은 시스템이 될 것이라 예상한다.

참고문헌

[1] Behrouz A. & Forouzan, "TCP/IP Protocol Suit", 2nd Edition, McGraw-Hill, 2003.

[2] Tobias Oetiker, “Round Robin Database, RRD”, http://oss.oetiker.ch/rrdtool/, 2008.

[3] Koohong Kang et al., “A Real-Time Network Traffic Anomaly Detection Scheme Using NetFlow Data”, Journal of KIPS, Vol.12-C, No.1, pp 19~28, 2008.

[4] Allen, J.R., “IBM PowerNP network processor: Hardware, software, and applications,” IBM J. RES. & DEV. vol. 47, No. 2/3, 2003.

[5] Michael Barr, “Programming Embedded Systems”, O'Reilly Media, 2001.

[6] P. Ferguson and D. Senie. Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoong. RFC 2267, January, 1998.

[7] Al Kelly & Ira Pohl, “A Book on C”, 4th Edition, Addison-Wesley, 2002.

[8] Neil Matthew & Rick Stones, “Beginning Linux Programming”, 4th Edition, WROX, 2008.