Win-32 플랫폼 기반의 웹 트래픽 감시 시스템 설계 및 구현

권용철[0] 차현철
동양대학교 컴퓨터 공학과
{gm014101 , hccha}@phenix.dyu.ac.kr

A Design and Implementation of the Web Traffic Monitoring System on the Win-32 Platforms

Yong-Chul Kwon[0], Hyun-Chul Cha
Dept. Computer Eng. Dong-Yang University

요 약

현재 전 세계 근로자의 상당수가 업무와는 무관한 인터넷 사용을 위해 많은 시간을 소모하고 있는 실정이다. 본 논문에서는 이러한 불필요하고 불건전한 인터넷의 사용을 감시하여 네트워크 상에 불필요한 트래픽의 발생을 억제함으로써 업무생산성을 높이고 회선 비용 절감 효과를 가질 수 있도록 하기 위해, 네트워크 상에서 발생하는 웹 트래픽을 감시하는 시스템을 설계하고 구현하였다. 본 논문에서 개발한 시스템은 Windows 계열 운영체제에서 실행될 수 있도록 하기 위해 BNF와 호환이 되는 "Winpcap" API를 사용하였으며, 또한 다중 쓰레드를 사용하여 실시간 처리가 가능하도록 하였다. 본 시스템은 현재 웹 트래픽 만을 분석 처리하도록 되어 있지만, 향후 다른 프로토콜들에 대한 처리를 보안할 경우, 네트워크 감시 프로그램으로도 사용될 수 있을 것이다.

1. 서론

지속적인 고속 네트워크의 확산으로 이제는 언제 어디서든 초고속으로 인터넷에 접속 할 수 있는 기반으로 구축되었다. 이러한 네트워크 인프라의 눈부신 발전은 이제 기업의 업무 처리 및 정보 공유 차원을 넘어 쇼핑, 주식 거래, 은행 업무 처리 등 개개인이 일상 생활에 필요한 일을 처리하는데 있어 깊숙이 자리를 잡아나가고 있다. 이와 같은 인터넷의 빠른 변천은 시간에 쫓겨 생활하는 현대인에게 편리함과 효율성을 제공하였지만, 인터넷 오사용으로 인한 문제점도 확산되고 있다.

갤럽과 Vaultreports.com , MSNBC의 연구 조사 결과에 따르면 전 세계 근로자의 상당수가 업무와는 무관한 인터넷 사용을 위해 매일 20분에서 1시간 가량을 소모한다고 한다. 그리고 이들이 방문하는 대부분의 웹사이트는 대량의 네트워크 트래픽을 발생시키는 포르노그래피, 온라인 증권, 쇼핑, 게임 사이트들인 것으로 드러났다[1-3].

향후, 전 세계적으로 2억 7천만의 근로자들이 인터넷을 사용하게 될 2003년[4], 기업들이 근로자들의 비업무용 인터넷 사용으로 인해 얼마나 많은 비용과 시간을 허비하게 될지는 쉽게 예상할 수 있다.

이러한 자료를 토대로 고려해 볼 때 많은 사업장에서 불필요한 웹 서핑을 모니터링하고 호스트의 웹 서핑 시간을 실시간으로 체크하여 경과 시간을 측정할 수 있는 시스템이 절실히 요구되고 있는 사점이다.

본 논문에서는 이러한 요구에 따라 네트워크 내에 송수신 중인 패킷을 분석하여 호스트들의 웹 서핑과 관련해서 호스트의 웹사이트 접속 현황을 알아보고 접속한 시간과 접속해서 진행되는 시간을 알아볼 수 있는 시스템을 설계 및 구현하였다.

논문의 구성은 다음과 같다. 1장의 서론의 이어 2장에는 본 논문에서 개발된 시스템의 설계 대한 내용을 설명하였으며, 3장에는 시스템 구현 방법과 특징을 기술하였다. 마지막으로 4장에서는 결론 및 향후 연구과제를 서술하였다.

2. 시스템 설계 및 구현

2.1 패킷 캡쳐 모듈 설계

네트워크 상에 송수신 중인 패킷을 캡쳐하려면 운영체제에 맞는 패킷 API(application program interface)를 사용하

여야 한다. 거의 대부분의 유닉스 계열 운영체제는 패킷 캡쳐와 관련된 커널 모듈을 가지고 있고, 그 대표적인 것이 'libpcap' 이다. 이 'libpcap'은 사용자 수준에서 사용 시스템과 운영체제에 관계없이 쉽게 패킷을 캡쳐 할 수 있도록 도와주는 라이브러리이다. 하지만, 윈도우 운영체제에서 사용 가능한 몇 가지 API들이 있지만 대부분 심각한 제약사항을 가지고 있다. 예를 들어, "Netmon" API는 프리웨어가 아니며, 확장성이 매우 제한되어 있다. "IP filter driver"는 Windows 2000 상에서만 수행되며 IP를 제외한 다른 프로토콜들을 지원하지 않는다. "PCAUSA"는 BPF 호환 필터를 포함한 패킷 캡쳐를 위한 인터페이스를 제공하는 상용 제품이고, 사용자 인터페이스가 매우 저수준(low-level)이며 필터 생성과 같은 추상적 기능들은 제공되지 않는다[5].

본 논문에서는 위의 상황을 고려하여, 이탈리아 Politenico di Torino 대학의 Netgroup에서 만든 "Winpcap"을 패킷을 캡쳐하는데 사용하였다. Winpcap은 Win32 플랫폼에 대해 패킷 캡쳐와 네트워크 분석을 하기 위한 구조로서 'libpcap'과 호환성을 갖는다. Winpcap은 Netgroup Packet Filter(NPF)라 불리는 커널 모드 드라이브와 저수준 동적 링크 라이브러리(packet.dll) 및 고수준의 시스템의 독립적 라이브러리(wpcap.dll) 등 세 개의 부분으로 구성되어 있다[6,7].

Winpcap의 구조 및 본 논문에서 설계 된 시스템과의 관계는 그림 1과 같다.

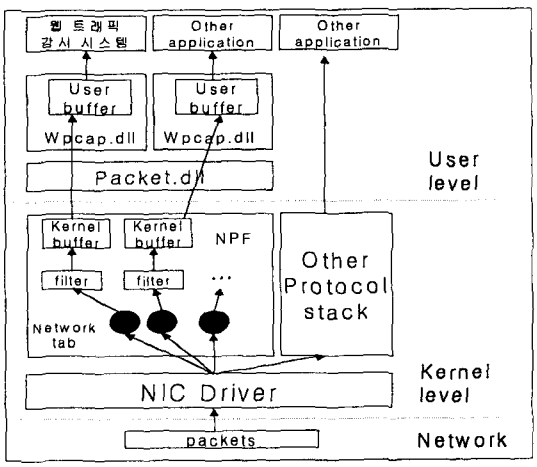

그림 1 Winpcap 구조와 제안 시스템과의 관계

2.2 처리 모듈 설계

쉬운 사용자 인터페이스와 프로그램의 편리를 위해서 Visual C++(MFC)를 선택하였다. 또한 처리 속도의 향상을 위해서 다중 쓰레드와 필터(filter)를 사용하여 운영체제에 대해 부하를 최소화 시켰다. Winpcap API를 사용하게 되면, 여러 가지 장점을 가지게 되는데 그중 한 가지가 필터 기능이다. bpf과 호환이 되므로 사용법도 상당히 쉬운 편이다. filter를 사용하여 tcp 패킷만을 추출하도록 하여TDmau 이를 통해 시스템에서 과부하가 생기지 않도록 하였다. 시간 처리에도 MFC에서 제공되는 함수를 이용하여 프로그램에 호환을 고려하였다. 전체적인 처리 모듈 구조는 그림 2와 같이 설계하였다.

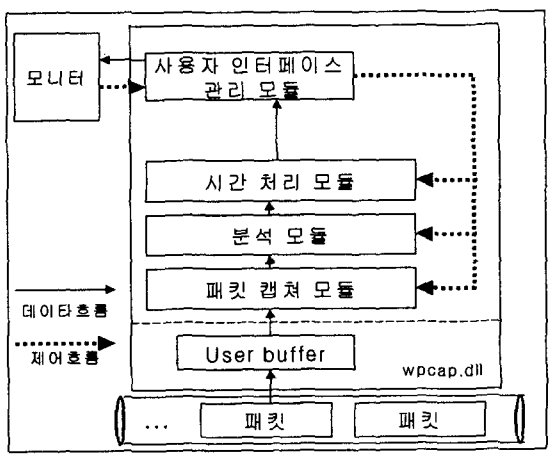

그림 2 시스템 구조도

본 논문에서는 웹 트래픽과 관련된 패킷만 캡쳐하도록 구현하였으며, 그 패킷 중에서도 URL 부분만 분석하여 처리하도록 하였다.

3. 구현 내용 및 특징

본 논문에서 구현한 시스템은 Visual C++를 사용하여 디자인되었으며, 쉽고 간단한 사용자 인터페이스를 갖는다. 사용자인터페이스는 한 눈에 알아볼 수 있도록 하였으며, 버튼으로 처리하여 초보자도 쉽게 사용할 수 있게끔 구현하였다. 구현 시스템의 실행화면은 그림 3에서 볼 수 있는 것처

럼, 본 웹 트래픽 감시 시스템은 웹 연결에 해한 정보를 웹 서버의 URL뿐만 아니라 해당 서버의 IP주소까지 출력을 함으로써 호스트가 해당 URL의 어느 서버에 접속되어 있는지도 판독이 가능하도록 하였다. 캡쳐 시간 및 진행되고 있는 시간을 출력하여 호스트의 사용시간을 알 게 쉽게 구현하였다. 접속 상태를 표시하도록 하여 호스트가 접속이 연결 혹은 종료가 되었는지도 확인이 가능하도록 하였다. 일반적인 캡쳐를 사용하는 프로그램은 캡쳐한 시간을 나타내는 것이 대부분이다. 하지만 이 시스템은 호스트가 사용할 시점(캡쳐한 시간)부터 접속이 끊어질 때까지 시간을 처리하는 부분을 추가시켰다. 그래서 이 호스트가 얼마만큼 이 호스트를 이용했는지를 실시간으로 알 수 있게끔 처리하였다.

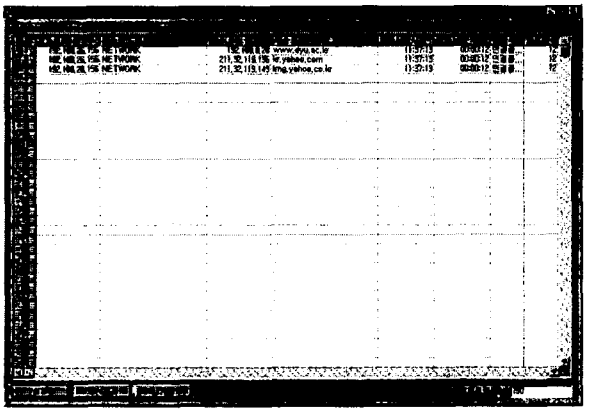

그림 3. 구현 시스템 초기화면 및 실행 후 화면

또, Windows NT/2000 등 Windows 서버 계열 운영체제뿐만 아니라 Windows 95/98, ME, XP 등 거의 대부분의 Windows 운영체제에서도 실행이 가능하게 설계 및 구현되어서 기존의 제품들이 서버 계열 운영체제에서만 실행되었던 제약성을 없앴다.

4. 결론 및 향후 연구 과제

본 논문에서 설계 및 구현한 시스템은 패킷을 캡쳐해서 웹 트래픽 패킷 부분만을 분석하여 처리하는 시스템이다. 또한 효율적인 패킷 캡쳐를 위해서 Windows 운영체제에서 유닉스의 bpf와 호환이 가능한 "Winpcap" 이라는 API를 이용하여 사용하였으며, API에서 지원하는 필터를 이용하여 본 논문에서는 웹 트래픽 패킷만 추출하였다. 또한 시스템 프로그램에 효율적인 Visual C++를 이용하여 시스템에 좀 더 빠르게 접근하였다. 패킷에서 분석한 호스트와 IP 그리고 접속하는 웹사이트 주소(URL)를 보면서 해당 호스트의 접속상태를 파악할 수가 있었다.

본 논문에서는 사용한 시스템은 NPF의 필터를 이용하여 웹 트래픽만을 분석하여 처리하였다. 향후 이 필터를 수정 보완하여 SMTP, POP3와 같은 E-mail 관련 프로토콜과 ftp, telnet 등과 같은 여러 가지 프로토콜에 대한 분석을 추가해 나갈 것이며, 이러한 확장이 성공적으로 이루어질 경우, 다양한 네트워크 트래픽 감시 도구로서 확장이 무궁무진할 것으로 기대된다.

[참 고 문 헌]

[1] http://www.gallup.com

[2] http://www.vaultreport.com

[3] http://www.msnbc.com

[4] International Data Corp. at http://www.idc.com

[5] PCAUSA, Rawether, Available at http://www.rawether.net

[6] Netgroup Lab. Politenico di Torino, WinPcap: the free Packet Capture Architecture for Windows, Available at http://www.netgroup.polito.it/winpcap/docs/

[7] Tim Carstens, Programming with pcap, tutorial, Available at http://broker.dhs.org/pcap.htm

[8] W. R. Stevens, TCP/IP Illustrated, Vol. 1, Addison-Wesley, 1994

[9] RFC 2068, Hypertext Transfer Protocol -- HTTP/1.1 ,1996