PDA용 프로토콜 분석기의 설계 및 구현

이재종*, 김영웅, 정인환
한성대학교 컴퓨터공학과
{ejejo*, yukim, ihjung}@hansung.ac.kr

Design and Implementation of Protocol Analyzer for PDA

Jaejong Lee*, Youngung Kim, Inhwan Jung
School of Computer Engineering, Hansung Univ.

요 약

프로토콜 분석이란 이더넷(Ethernet)의 특성인 동보 기능(broadcasting)을 이용하여 LAN에 흘러 다니는 모든 패킷들을 실시간으로 수집하여 OSI 7 Layer별로 분석하는 것을 의미한다. 아직까지는 프로토콜 분석기가 일반 PC에서 사용이 가능한 형태로 개발되어 있는 실정이며 무선 LAN을 대상으로, 특히 PDA 상에서 사용 가능한 프로토콜 분석기는 찾아보기 어렵다. 무선 LAN은 중계기 역할을 하는 Access Point가 곳곳에 지역적으로 분산되어 설치되어야 한다. 본 논문에서는 이러한 무선 LAN 특성상 이동이 용이한 PDA 상에서 무선망의 운영 상태를 파악하고 검사할 수 있는 프로토콜 분석기를 설계하고 구현한다.

1. 서 론

일반적으로 네트워크 진단 도구로서 가장 많이 활용하는 것이 프로토콜 분석기이다. 프로토콜 분석기는 네트워크에 흘러 다니는 모든 패킷을 수집하여, 패킷의 세부 내용을 보여주는 프로토콜 분석 기능 뿐만 아니라 네트워크의 사용 통계를 보여주는 트래픽 측정 기능을 가지고 있다. 최근 들어 대부분의 학교들이 교내에 무선 LAN을 설치하여 학생 및 교직원들에게 보다 편리한 네트워크 환경을 제공하고 있다. 무선 LAN 환경이 활성화되고 활용도가 증가하고 있지만 무선 LAN 진단 도구가 부족하고 또한 무선 LAN 특성인 이동성을 만족시킬 만한 도구는 더욱 찾아보기 힘들다.

본 논문에서는 WinCE 운영체제를 사용하는 PDA용 프로토콜 분석기에 대하여 기술하고자 한다. 구현된 프로토콜 분석기는 유/무선 LAN의 진단과 네트워크 관리를 위해 활용될 수 있다.

본 논문의 구성은 다음과 같다. 2장에서는 본 논문에서 연구 개발하고자 하는 프로토콜 분석기의 설계 및 구현에 대해 논하고, 마지막으로 결론 및 향후 연구 과제를 3장에서 언급하겠다.

2. 설계 및 구현

2.1 프로토콜 분석기의 구조

본 논문에서 구현한 프로토콜 분석기는 그림 1과 같은 구성으로 되어 있다. 그림 1에서 연구한 대상은 패킷 드라이버(Packet Driver) 부분과 응용 프로그램(Application) 부분이다. 패킷 드라이버(Packet Driver)는 이더넷의 특성인 동보기능(broadcasting)을 이용하여 LAN 카드를 통해 무선 LAN에 흘러 다니는 모든 패킷을 수집하게 된다. 응용 프로그램(Application)은 수집된 패킷 헤더의 내용을 분석하여 패킷의 내용을 표시해주고 프로토콜 통계 등을 표시해 준다.

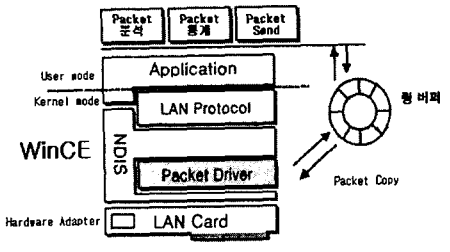

그림 1. 프로토콜 분석기의 구조

2.2 패킷 드라이버(Packet Driver)

이더넷은 이론적으로는 LAN 카드에서 LAN에 흘러 다니는 모든 패킷을 볼 수 있다. 그러나 일반적인 TCP/IP 및 이더넷 응용 프로그램들이 수행되는 환경에서는 LAN 카드가 모든 패킷을 읽지만 해당 LAN 카드의 MAC(medium access control) 주소에 맞는 패킷만 선택하여 상위 계층인 응용 프로그램으로 전달하고 다른 주소로 보내지는 패킷들은 버리게 된다. 그렇지만 프로토콜 분석기는 해당 PDA로 보내지는 패킷 뿐만 아니라 모든 패킷들을 볼 수 있어야 한다. 따라서 LAN 카드에서 모든 패킷을 수집하여 응용 계층으로 전달해 주는 기능이 필요하다. 이러한 기능을 담당하는 부분이 패킷 드라이버이다. 패킷 드라이버에서는 해당 PDA의 주소로 보내지는 패킷 뿐만 아니라 LAN 카드에서 버려지는 모든 패킷들을 상위 계층인 프로토콜 분석기로 전달 할 수 있도록 LAN 카드를 직접 조작하는 기능이 필요하다.

패킷 드라이버에서 H/W인 LAN 카드를 직접 조작하기 위해서는 PDA의 운영체제인 WinCE의 커널 모드(kernel)에서 수행되는 장치 드라이버(device driver) 형태로 개발이 되어야 한다. 패킷 드라이버에서 수집된 패킷들은 링 버퍼(ring buffer)또는 원형 큐(circular queue)를 통해서 사용자 모드(user mode)에서 수행되는 응용 프로그램으로 전달되게 된다. 원형 큐를 사용하는 이유는 응용 프로그램에서는 패킷 드라이버에서 수집한 패킷을 순서대로 분석해야 하며 패킷 드라이버는 실시간으로 패킷을 수집하여 상위 계층인 응용 프로그램으로 순서에 맞게 전달하여야 하기 때문이다. 이 때 원형 큐를 사용하면 패킷을 수집하는 속도와 패킷을 분석하는 속도의 차이로 인한 버퍼링을 효과적으로 할 수 있다.

패킷 드라이버는 응용 프로그램에서 동적으로 함수 호출이 가능하도록 API(application programming interface)를 제공하여야 한다. 예를 들면 LAN 카드를 선택하여 패킷 수집을 시작하는 API 와 패킷 수집을 중지하는 API, 또 특정 주소 또는 프로토콜 등을 선택적으로 수집할 수 있도록 필터(filter)를 지정하는 API 등이다.

2.3 응용 프로그램(Application)

프로토콜 분석 프로그램은 WinCE 사용자 모드(user mode)에서 수행되며 패킷 드라이버에서 정의된 API(application programming interface)와 WinCE의 사용자 GUI(Graphical User Interface) 함수를 이용한 프로그램이다. 본 논문에서 연구하고 구현한 내용을 기능별로 기술하면 다음과 같다.

2.3.1 실시간 패킷 수집 기능

패킷을 수집하는 기능은 주로 패킷 드라이버가 담당하지만 패킷 드라이버는 수집된 패킷을 원형 큐를 사용하여 응용 프로그램으로 전달하게 되므로 응용 프로그램에서는 전달된 패킷들을 분석을 위해 메모리에 복사하여 보관하여야 한다. 이 때 수집되는 패킷의 양이 너무 많아지면 PDA의 메모리의 한계상 모든 패킷을 보관할 수 없으므로 일정한 메모리까지만 패킷을 보관하도록 제한을 두어야 한다. 그러므로 PDA의 메모리 크기와 수집되는 패킷 양을 고려하여 효과적으로 패킷들을 보관할 수 있도록 자료구조와 알고리즘을 구현하였다.

2.3.2 프로토콜 분석 기능

프로토콜 분석은 저장된 패킷의 헤더를 분석하여 각각의 헤더 내용을 프로토콜의 필드별로 설명하는 기능이다. 일반적으로 프로토콜 분석기는 패킷 목록과 헤더 분석 부분 그리고 패킷의 Dump 내용이 한 화면에 나온다. 그러나 PDA의 작은 화면에 전체를 동시에 표시할 수는 없다. 따라서 그림 2와 같이 일단 목록을 보여주고 목록을 선택하면 헤더의 내용 그리고 다시 전체 패킷 내용을 표시하는 사용자 인터페이스를 가진다.

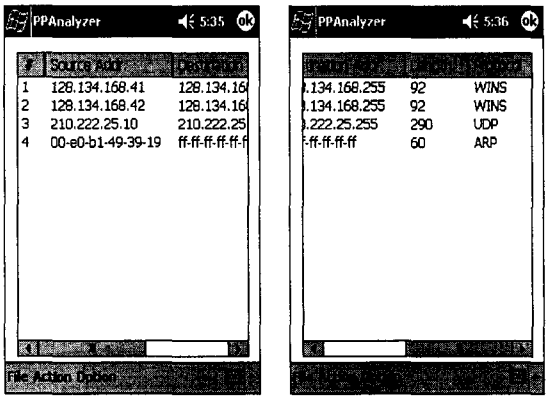

그림 2. 패킷 목록 화면

그림 3은 그림 2에 나타난 목록을 선택하면 표시되는 패킷 헤더의 내용이다.

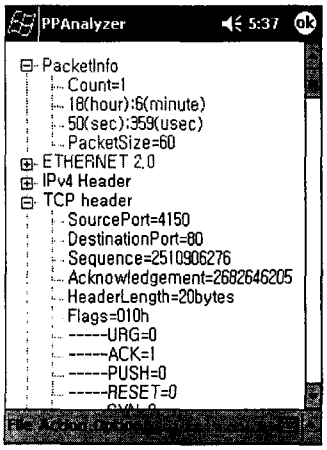

그림 3. 패킷 헤더 내용

일반적으로 이더넷의 패킷(또는 프레임)은 그림 4와 같은 구조로 되어 있다. 그림의 예를 들어, 프로토콜 분석은 이더넷 헤더, IP 헤더, TCP 헤더 그리고 응용 데이터 순서로 분석이 된다. 이를 위해서는 각각의 프로토콜 별로 프로토콜 정의(protocol definition)를 이해하고 각각의 필드의 내용을 표시하여야 한다.

Ethernet Header	IP Header	TCP Header	응용 DATA

그림 4. 이더넷 패킷 구조의 예

2.3.3 조건적 패킷 수집을 위한 필터(filter) 지정 기능

필터링 기능은 프로토콜 분석기가 특정 조건에 맞는 패킷들만 수집하여 분석이 가능하도록 사용자에게 선택권을 주는 기능이다. 예를 들면, 특정 주소와 주소사이에 교환되는 패킷만을 분석하거나 특정 프로토콜만 분석하기 위해서 지정할 수 있다. 응용 프로그램에서는 사용자에게 패킷 필터를 지정하도록 메뉴를 제공하여야 하며 지정된 필터를 패킷 드라이버에게 설정함으로써 패킷 드라이버는 조건에 맞는 패킷만을 수집하여 응용 프로그램에게 전달하게 된다. 패킷 필터를 지정하는 방법으로 가장 많이 사용되는 것은 BPF(BSD packet filter)[1]이다. BPF는 논리 연산자를 이용하여 패킷에 대한 조건을 정의할 수 있는 프로그램과 같다. 예를 들어 IP 주소가 128.134.165.1 인 컴퓨터와 128.134.165.2 인 컴퓨터 사이에 교환되는 패킷만을 수집하고자 한다면 아래와 같이 정의하면 된다.

```
Filter = (src host 128.134.165.1 and dst host  128.134.165.2)
                              or
Filter = (src host 128.134.165.2 and dst host 128.134.165.1)
```

또, 웹(Web, HTTP) 패킷만 수집하기를 원한다면 아래와 같이 정의한다.

```
Filter =  tcp and port 80
```

본 논문에서는 일반적으로 가장 많이 사용되는 필터링 조건인 IP 주소, MAC 주소, 그리고 TCP/UDP의 포트(port)를 지정할 수 있도록 편리한 사용자 인터페이스를 제공하고, 그 밖의 일반적인 BPF 정의를 위한 인터페이스를 구현하였다.

2.3.4 무선 LAN 프로토콜 통계 표시 기능

프로토콜 통계 기능은 프로토콜 분석 기능과 더불어 프로토콜 분석기의 가장 핵심적인 기능이다. 본 논문에서는 필터링 조건에 맞는 패킷들의 사용 통계를 다음과 같은 세부 조건 및 기준으로 표시한다.

- 패킷 량(bits, Byte, 패킷 수) 기준
- 프로토콜별 기준
  (ARP, TCP, UDP, IP, HTTP, FTP, Telnet, 등등)
- 패킷의 크기별 기준
  (64 byte 이내, 64~128 byte, 128~256, 등등)
- 통계를 표시하는 시간 간격 설정
- 통계를 표시하는 방법 설정
  (선 그래프, 막대 그래프, 원 그래프, 수치 값)

특히 통계를 표시하는 방법으로 그래프를 사용함으로써 무선 LAN의 상태를 쉽게 판단할 수 있다. 그림 5는 선 그래프를 이용하여 프로토콜 통계를 표시한 그림이다.

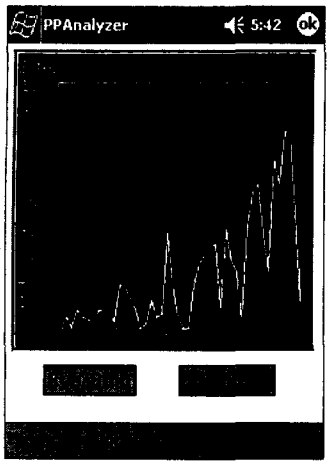

그림 5. 프로토콜 통계

2.3.5 트래픽 발생기(traffic generator) 기능 설계

본 논문에서는 무선 LAN의 진단을 위해 프로토콜 분석 기능 외에도 강제적으로 트래픽을 발생시키는 트래픽 발생기를 구현하고자 한다. 트래픽 발생기는 특정 조건에 맞는 트래픽을 발생시킴으로써 무선 LAN에 접속되어있는 컴퓨터, Access Point, 허브 및 라우터 등에 대한 부하 테스트를 할 수 있다. 그림 6은 일반 Windows 환경에서 사용이 가능한 트래픽 발생기이다[2].

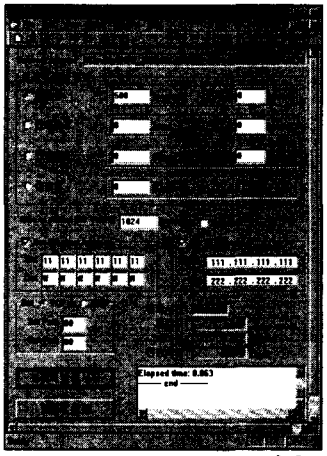

그림 6. 트래픽 발생기의 예[2]

본 논문에서는 그림 6과 같은 트래픽 발생기를 PDA용 프로토콜 분석기의 모듈 중 하나로 통합하여 구현한다. 이를 위해서는 패킷 드라이버에 저수준 패킷을 송신할 수 있는 기능이 필요하며 트래픽 발생 모듈에서 패킷 송신을 위한 API를 호출하게 된다. 그림 6에서와 같이 트래픽 발생기는 사용자가 지정한 MAC 주소, IP주소 및 PORT 번호를 이더넷 헤더, IP 헤더 및 TCP/UDP 헤더에 각각 설정하여 패킷수, 전송시간, 전송속도 및 전송량을 기준으로 트래픽을 발생하게 된다.

본 논문에서는 트래픽 발생기를 PDA의 사용자 인터페이스에 맞게 설계하고 구현하며 그밖에 실제 운영 환경과 같은 다양한 조건으로 트래픽이 발생 될 수 있도록 트래픽 모델링 방법을 연구한다.

2.3.6 무선 LAN 환경 진단 기능(Ping, Traceroute 등)

일반적으로 LAN의 상태를 점검할 때 많이 사용하는 도구가 **Ping**과 **Traceroute**[3]이다. **Ping**은 ICMP(internet control message protocol) 반향(echo) 요구 패킷을 해당 IP 주소로 보내고 그 응답을 확인하여 해당 컴퓨터 또는 네트워크 장비가 정상적으로 동작 중인지 검사하는 프로그램이다. 또 **Traceroute**는 ICMP 패킷의 TTL(time to live) 값을 이용하여 출발지에서 목적지 컴퓨터까지 중간 경로를 추적하는 프로그램이다. 본 논문에서는 이 두 가지 프로그램을 프로토콜 분석기의 모듈로 추가하여 프로토콜 분석기 안에서 **Ping**과 **Traceroute** 기능을 사용할 수 있도록 하였다.

IP scanning 기능은 네트워크에 연결된 컴퓨터들의 NETBIOS(network basic input output system)[4] 이름들을 확인하는 기능이다. NETBIOS 이름이란, 주로 Windows 계열의 컴퓨터들에 설정되어 있는 논리적 컴퓨터 이름으로, Windows 의 네트워크 환경에 표시되는 이름이다. 일반적으로 이 컴퓨터 이름은 컴퓨터의 사용자 또는 부서명이 표시되는 경우가 대부분이다. 따라서, IP scanning 프로그램은 IP 이름을 NETBIOS 이름으로 찾아줌으로써 해당 IP를 가진 컴퓨터가 누구의 소유인지를 역으로 추적할 수 있는 단서를 제공한다. 그렇게 함으로써 프로토콜 분석 과정에서 확인된 특정 IP를 가진 컴퓨터를 보다 쉽게 확인할 수 있다. 이 **IP scanning** 기능도 **Ping**과 **Traceroute** 명령어와 함께 프로토콜 분석기의 하나의 모듈로 통합하여 구현하였다.

그밖에 대부분의 컴퓨터에서 사용 가능한 도구로서 프로토콜 분석기에 통합한 네트워크 진단 도구들로 다음과 같은 것들이 있다.

- **DNS(domain name server)** 이름 확인 기능
  : URL을 IP 주소로 변환하는 기능
- **Reverse DNS** 기능
  : 특정 IP의 DNS 이름이 무엇인지 역으로 확인하는 기능. 이 기능은 해당 컴퓨터가 DNS에 PTR(pointer)정보를 등록하였을 경우, DNS 질의(query)의 PTR(pointer) 정보로 확인이 가능하다.
- **NETSTAT(network status)** 기능
  : PDA에 현재 설정되어 있는 네트워크 상태 및 라우팅 테이블 등을 확인하는 기능.

3. 결론 및 향후 연구

본 논문에서는 무선 LAN을 대상으로 PDA용 프로토콜 분석기를 설계 및 구현하였다. 현재 많이 사용되고 있는 무선망을 진단하는데 있어 PDA를 이용하면 이동성이 좋고 휴대하기 편리하여 기존의 진단체계들을 개선할 수 있다.

향후 연구는 설계된 트래픽 발생기를 구현하고 성능 평가를 통해 구현된 기능들의 검증과 사용자 인터페이스의 개선 등이다.

참고문헌

[1] S. McCanne and V. Jacobson, The BSD Packet Filter: A New Architecture for User-level Packet Capture., Proceedings of the 1993 Winter USENIX Technical Conference (San Diego, CA, Jan. 1993), USENIX.

[2] 정인환, 김진환, 비쥬얼 이더넷 트래픽 발생기의 설계 및 구현, 제 18 회 정보처리학회 추계학술대회, 2002.

[3] Ping, Traceroute, RFC 792(ICMP)

[4] IBM LAN Technical Reference, IEEE 802.2 and NetBIOS Application Program Interfaces Second Edition, 1996