A Real-Time Network Monitor System Based on WinPcap

Zijuan Luo
Science and Technology on Information Systems Engineering Laboratory,
Nanjing Research Institute of Electronics Engineering,
Nanjing, China
luozijuan2002@hotmail.com

Shuanghua Zhu
Science and Technology on Information Systems Engineering Laboratory,
Nanjing Research Institute of Electronics Engineering,
Nanjing, China
zhushuanghua@hotmail.com

Abstract—This paper provided a real-time network monitor system based on Wincap, which supported packet level and flow level traffic metrics such as link utilization , protocol distribution in 2～7 protocol levels ,various aggravated flow distribution , top N IP host and IP host pair.

Keywords-Network traffic; Traffic measurement and analysis; Wincap; Network monitoring .

I. INTRODUCTION

The network traffic measurement and analysis were neglected in the early days of network development and protocol analysis. The researchers just relied on relatively simple tools (such as SNMP and TCPDUMP) to acquire traffic parameters of network. However, with the development of Gigabyte and other high-speed networks, these simple measurement tools cannot meet the need of traffic measurement and analysis which are crucial to acquirement of network traffic characteristics and parameters, network design and performance optimization. Even more, network measurement and analysis are fundamental to traffic engineering, attack detecting, QoS research and traffic modeling.

In order to understand how a network is being used or whether it is being abused , an administrator needs to inspect the flow of the traffic and "infers" the intent of the users and applications[1].So the network traffic measurement and analysis are crucial to network monitoring , reliable DDoS detecting and attack source locating as well. In this paper, we discuss the principle of real-time network traffic measurement and analysis through embedding a traffic measurement and analysis engine into IP packet-decoding module, and emphasize the implementation of visualizing the real-time network traffic , which are helpful to network monitoring and network traffic modeling[2].

II. BRIEF INTRODUCTION TO WINPCAP AND PACKETCAPTURING

WinPcap is an open source library for packet capturing and network analysis for the Win32 platform. It includes a kernel-level packet filter, a low-level dynamic link library (packet.dll), and a high-level and system – in depend entlibrary (wpcap.dll).

The packet filter is a device driver that adds to Windows OS such that we can capture and send raw data from a network card, filter and store captured packets .Packet.dll is an API that can be used to directly access the functions of the packet driver, offering a programming interface independent of the Microsoft OS. Wpcap.dll exports a set of high level capture primitives that a recompatible with libpcap[3], the well-known Unix capture library. These functions allow users to capture packets in a way independent of the underlying network hardware and operating system .

We can easily carry out the raw network traffic capturing by calling API functions of WinPcap , the primary functions for packet capturing are as follows :(1) pcap_findalldevs_ex : obtains a list of suitable network adapters[4] .(2) pcap_findalldevs : obtains advanced information (i.e.device name, device description, interface address, network masks, broadcast address and destination address) about available devices[5]. (3) pcap_open :opens a device for packet capturing and return a pcap_t pointer . (4)pcap_compile : compiles a packet filter which can be interpreted by the kernel-level filtering engine[6] . (5) pcap_setfilter: associates a filter to a capture .(6) pcap_dump _ open : opens a file to write the network traffic[7]. (7) pcap_dump : saves a packet to disk. (8) pcap_dunp_close : closes the file associated with a capture deviceand frees resources . (9) pcap_open_live : opens a live capture from network[8]. (10) pcap_open_offline : opens asavefile in tcp dump/ libpcap format to read packets . (11)pcap_stats : returns the statistics on current capture . (12)pcap_loop : collects packets from the capture device .In addition to the above primary functions for pack capturing[9], WinPcap also presents the API functions for sending packets from a network card. As to how to carry out packet capturing, many papers have discussed the principle and implementation[10].

III. PRINCIPLE OF TRAFFIC FLOW MEASUREMENT AND ANALYSIS

There are two basic methods of measuring network traffic flow. The first method is Active Measurement: It involves the injection of some user-generated packets , the purpose of which is to provide some insight into the way that real network traffic is treated within the network , and probe the Internet and measure network characteristics .

Examples of this approach are ping and trace route utilities .Through selecting appropriate targets and sending ICMP or UDP packets, we can implement active probe into the network. One of the advantages of active measurement is that it doesn't require full access to network resources (e.g. routers) . Its limitation is that it may disturb the normal network traffic because of the injection of p robin packets. Network performance monitoring and network topology measuring are usually carried out through active measurement. The other approach is Passive Measurement: It is used to observe and record the packet traffic on a real network, without injecting any

user-generated traffic into the network. That is, the measurement device is non-interferential. This approach can be implemented by incorporating some additional intelligence into network devices to enable them to identify and record the characteristics. One of the main limitations of passive measurement is that it can only monitor the network traffic of a limited network segment .Passive Measurement is usually used f or network traffic measurement and analysis .Taking passive measurement as an example , this paper discusses the principle and implementation of real-time network measurement and analysis , including Packet-rate ,Byte-rate , Packet-length series , Packet inter-arrival timing, Packet size distribution, In/out Packet/Byte rate ,Protocol-usage distribution , Packet loss and delay and other traffic characteristics as well . Figure 1shows the flow chart of IP network traffic measurement and analysis.

As Figure 1shows, the Measurement and Analysis Engine is embedded into IP packet decoding module. First, the engine filters the IP packets so as to measure those packets we are concerned about. Then those filtered packets a resample (the sampling interval and precision can be set by users).Finally, the Packet-length series, Packet-rate/Byte-rate and other traffic parameters are recorded respectively.

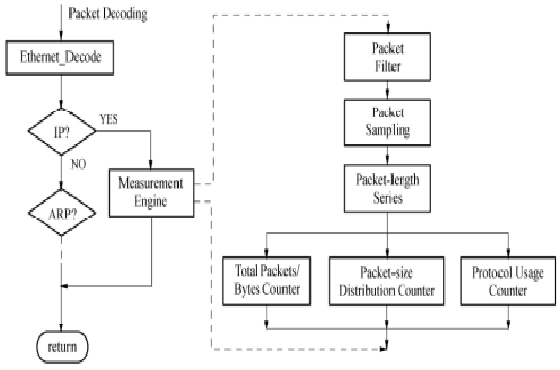

Figure 1. Flow-Chart of IP Packet Measurement

I. System Design and Realize

- Network card select and enactment module

Network card select and enactment module include capture network equipment list、select network card and enactment network card mode. In order to capture whole data of the network equipment, we always set the work module as intermix module.

- Capture module of data packet

Data packet capture module mostly responsible for data packet captures function. The first step is enactment capture time, users also can control capture process by hand. In actual application process, some data packet also should leave for examine and analyse. So, after the capture, software will prompt user the data packet save in the local disk whether or not.

- Analyse module of data packet

Data packet analyse module include the analyse of source IP and the analyse of transport layer agreement and application layer agreement. Every time start up the data packer capture module, software will parse all information of the data packet which including traffic flow statistics by time、 traffic flow statistics by protocol ,traffic flow statistics by IP pair address.

- Traffic flow module

Firstly, install traffic flow collection software in host computer which need monitor traffic. Then, install flow display software in host computer which need display network traffic. The collection software setup the name of network card ,then collect the traffic flow. Traffic flow display terminal send a subscription request to the host which can subscription the time statistics flow, protocol statistics flow, IP traffic statistics flow and IP pair traffic statistics flow and no longer subscribe the time statist flow ,protocol statistics flow, IP traffic statistics flow and IP pair traffic statistics flow. Traffic flow collection terminal received display terminal message after the subscription request to the flow of send traffic data that is needed. For example, when the subscription protocol flow, transfer protocol traffic data of the host. When the subscription time flow, transfer time traffic data of the host. When the subscription protocol flow, transfer protocol traffic data of the host. When the subscription protocol flow, transfer protocol traffic data of the host. All the traffic information has been sent to save, and further statistical classification. Then the time statistics flow, protocol statistics flow, IP traffic statistics flow and IP pair traffic statistics flow of the whole network will get.

IV. Traffic Flow of Real-time Display base on the Teechart

The TEECHART control is adopted to show the traffic flow for display. Interface as shown in Figure 2, the top of the chart display the time traffic flow by second, horizontal axis is time, Vertical axis is flow value, the bottom of the chart is large flow time and flow value. The protocol traffic flow interface is shown in Figure 3.The top of the chart display the second protocol traffic flow, horizontal axis is second, Vertical axis use different color represents different protocol flow value. The bottom of the chart display the minute protocol traffic flow, horizontal axis is minute, Vertical axis use different colour represents different minute protocol flow value.Figure 4 using histogram and pie charts show the IP traffic flow interface. The image below for IP flow top ten list. Figure 5 using histogram and pie charts show the IP pair traffic flow interface ,chart for the diagrams of IP to connect information.

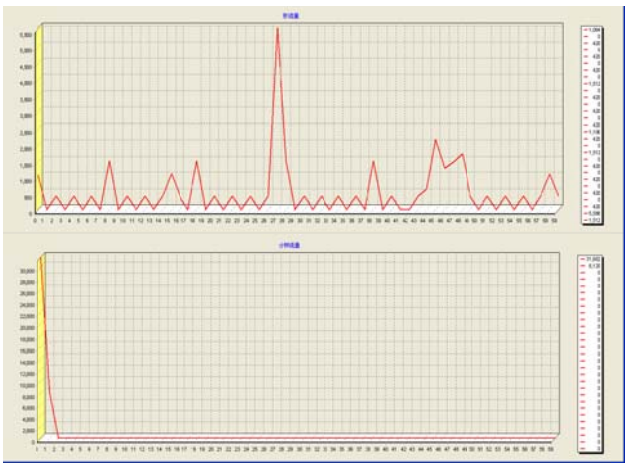

Figure 2. Time Traffic Flow

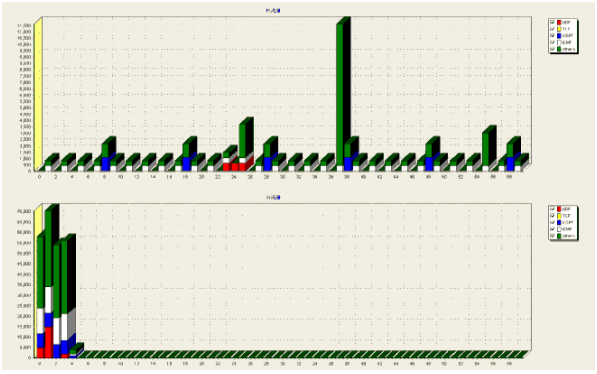

Figure 3. Protocol Traffic Flow

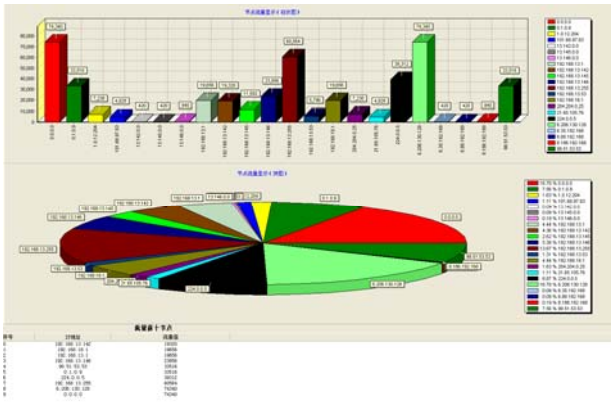

Figure 4. IP Traffic Flow

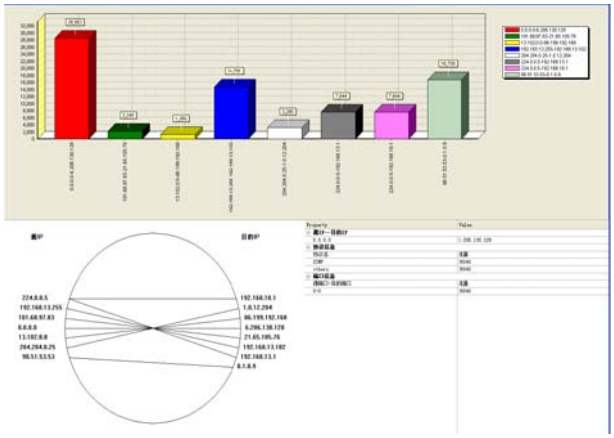

Figure 5. IP Pair Traffic Flow

V. CONCLUSION

This paper implements a traffic detection system based on software capture in Windows environment. For network behavior analysis and traffic modeling user to define different levels, different time granularity ,different dimensions of statistical data ,for the network traffic detection provides the effective data in real time.

REFERENCES

[1]. R.Kawahara,K.Ishibashi,T.Hirano,H.Saito,S.Asano,andMatsukata, ComputerCommunications,2001,24 (15 16) , 1508 – 1524.

[2]. M. Van den Nieuwelaa rand R. Hunt , Computer Communications , 2004 , 27 (1) , 128 140.

[3]. WinPcap : The Windows Packet Capture Library , http ://winpcap.cs. pu. edu. tw [OL] . 03. 22. 2005.

[4]. G. Chen and J . Gong , A research on traffic measurement in a large scale high-speed network , Comp uter Engineering and Application , 2002 , 17 19 , China .

[5]. C. 2X. Zhuang and Q.2Z. Peng , Comp uter a nd Modernization , 2002 , 11 13.

[6]. M. Li , Computer &Security , 2004 , 23 (7) , 549 558.

[7]. S. S. Kim , A. L . N. Reddy , and M. Vannucci,Detecting traffica nomalies at the source though aggregate analysis of packet header data , May 2004 , LNCS 3042 , 1047 1059.

[8]. ZHANG Xin-jie, WANG Xu-ren, WU Gang,Design and implementation of distributed net auditing system, Computer Engineering and Design, 2010,31 (17): 3797-3844.

[9]. XIE Kun1 , ZHANG Da-fang2 , WEN Ji-gang1 , XIE Gao-gang, A Real-Time Network Monitor System Based on WinPcap,2006,4(2):118-121

[10]. ZHOU Ling, DINGWei-x iong, YANG Wen-yin, Software desigh and protocol analysis for network monitor system based on WinPcap 2012,7(4):59-66