Network Monitoring and Analysis by Packet Sniffing Method

Pallavi Asrodia[#1], Mr. Vishal Sharma[*2]

[#1]Computer Science & Engineering Department,
Jawaharlal Institute of Technology
Borawan, Khargone (M.P.) India.

[*2] Asst. Professor
Computer Science & Engineering Department
Jawaharlal Institute of Technology
Borawan, Khargone (M.P.) India.

***Abstract*— Today we are seeing that computer networks are increasing in their sizes very rapidly. Number of its user increased in past few years and traffic flows in networks also increased, so it's very important to monitor networks traffic as well as its user's activities to keep the network smooth and efficient. For complex network it's very tough task to maintain and monitor the network, because large amount of data available. For this purpose packet sniffing is used. Packet sniffing is important in network monitoring to watch network activities which help network administrators to find out problems. This paper focuses on packet sniffer working in different environments, Behavior of already existing sniffer; their problems and challenges while performing sniffing. For accomplish of monitoring task, a tool is developed which will remove deficiency of existing tool. By using this packet sniffer we can capture traffic as well as we analyzed capture traffic. We can generate reports on the basis of analyzed traffic. Many protocol like TCP, IP, UDP etc. are implemented and filtering on basis of protocol is also done. Alerts generated on the occurring of suspected activities.**

***Keywords*-Packet capture, Network Monitoring, Network analysis, Packet sniffing.**

I. INTRODUCTION

Packet sniffing is the process of capturing the information transmitted across network [1]. In this process NIC capture all traffic that is flow inside or outside network. Packet Sniffing mainly used in network management, monitoring and ethical hacking. To perform sniffing we use tool named packet sniffer. A packet sniffer, sometimes referred to as a network analyzer, which can be used by a network administrator to monitor and troubleshoot network traffic.

II. PRINCIPLE OF PACKET SNIFFING

When packets transfer from source to destination then it passes through many intermediate devices. A node whose NIC is set in the promiscuous mode receives all information travels in network [2]. Each NIC have physical address which is different from another and network. When packet arrives at NIC then hardware address of frame matched with physical address that NIC have, but if we set it in promiscuous mode then all packets will arrives at that interface. When we use switch which already pass filtered data then we perform some method to capture all data of network. When NIC accept packets, packets are copied to driver memory then it passes to kernel and kernel passes it to user application [5].

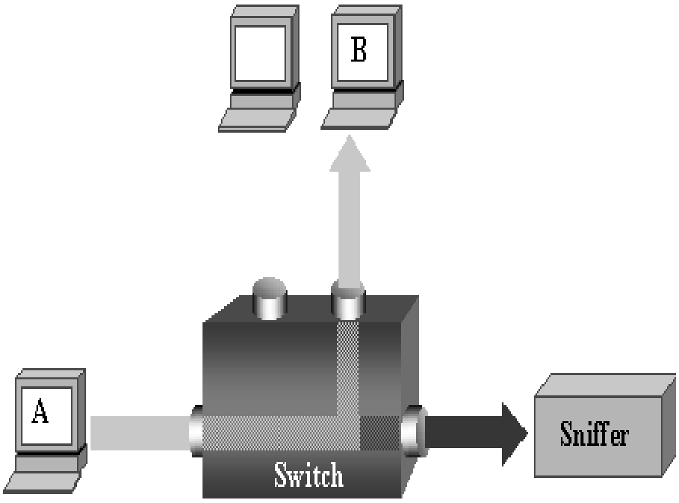


Fig. 1 Basic sniffing process

III. SNIFFER COMPONENTS

Any sniffer can be divided in following components [3].

A. Hardware

When we are working with sniffer, hardware is required sometimes for analyzing hardware problems like voltage problems, cable problems.

B. Drive Program

This is main component of sniffer, each sniffer contain its own drive program. Using this we can capture traffic in network and filter it to restrict data.

C. Buffer

A buffer is a storage device for captured data from network. In general, there are two types of buffer used. First one is where data captured continuously and second one where new packets replace old packets.

D. Packet Analysis

Packet analysis can be done on real time or we can analyze packets after storing it. We can analyze both header and actual data, when we store data in memory or we perform real time analysis, decoder is used to decode the data store in packets.

IV. RELATED WORK

There are lots of works done on packet sniffing for LAN or WAN monitoring [2]; lots of tools are available for network monitoring. In this paper some tools behavior is analyzed. Wireshark is a free and open-source packet analyzer [6]. It is used for network troubleshooting, analysis, but wireshark does not provide any intrusion detection and have more memory requirement for installation. Tcpdump is common packet analyzer that uses command line programming. It allows the user to capture and display TCP/IP and other packets being transmitted or received over a network. Some more tools are analyzed, they have different types of problem like memory, functioning problem etc [7]. So we have to design a tool which resolves all problems mentioned above and consume less space.

V. PRAPOSED WORK

After analyzing current tools, a proposed scheme for network monitoring and analysis is designed, in this scheme first packets are captured and capturing is done on real time. After packet capturing, packets are stored in memory for analysis task. This type of analysis can be performed for finding critical issues by administrator. Content of packets can be converted in the readable format which helps the administrator to understand information very easily. Packets are filter on the basic of protocol for reducing traffic. Filtering can be done on the basic of various protocols like IP, TCP, UDP, ICMP and IGMP. Capturing can be done on high speed LAN contain GBPS data rate. Attacks can be detected for suspicious activities and after detecting suspicious user we can close all work done by user at that time. Network traffic volume and packet loss can be determined using this captured information.

VI. RESULT

Main goal of thesis is evaluation of any network for better performance and security. This means use of system resources like memory and processor must be less, packet loss should be less as compared to other system. This section include various test conducted on data captured from network, these test are conducted on the basic of various parameters. Result is analyzed and compared with others results. Data play main role in result analysis. Real time data collected from the network. Packets are captured from the live environment from different sites .Data collected for analysis known as datasets. We have different datasets, I have presented only two. Data collected at the same time in different days and pattern of traffic is analyzed. Traffic volume is also calculated by this test.

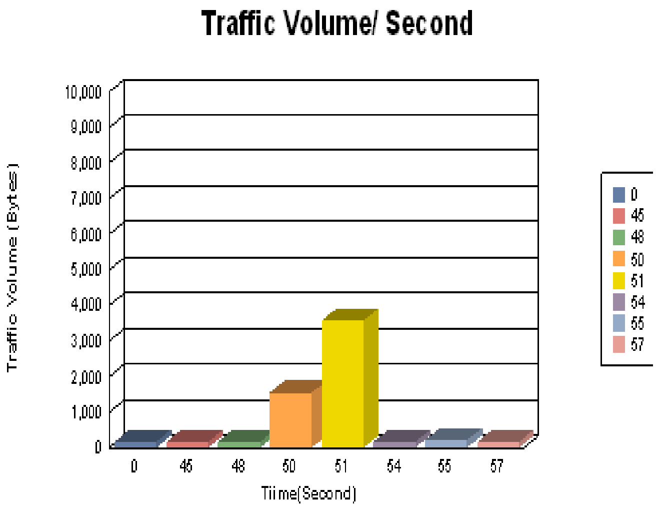


Fig. 2 Traffic volumes at network for dataset 1

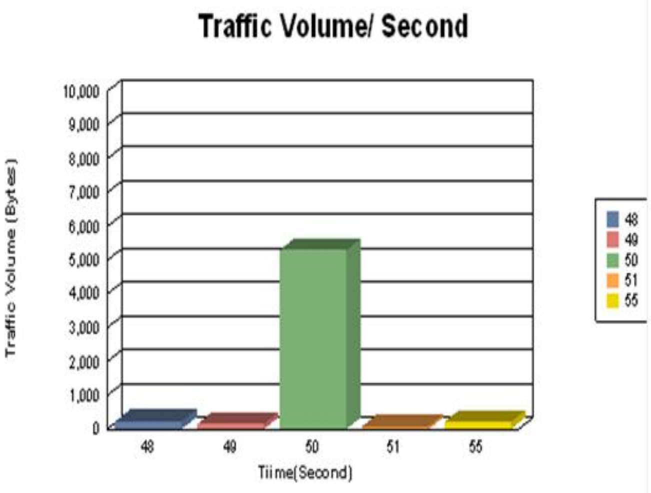


Fig. 3 Traffic volumes at network for dataset 2

After this experiment packet loss can be determined .Packet loss occurs when one or more packets of data travelling across a computer network fail to reach their destination. In TCP/IP protocols a packet loss below 0.1% (1 lost packet in every 1000 packets) can be tolerated; anything higher will have more or less impact (depending on circumstances) and needs to be addressed. Packet loss ratio can be calculated as - Packet loss ratio= Number of lost packet / (Number of lost packet + Number of packets received successfully).We have generated 1000 packet using packet generator and got packet loss ratio 0.15 and this result is compared with v6sniff sniffer which have 0.19 packet loss ratio [4].

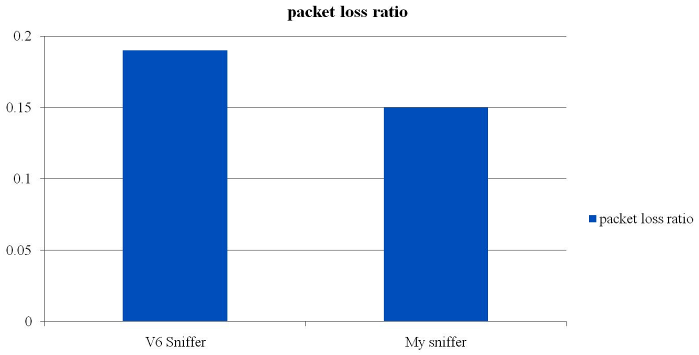
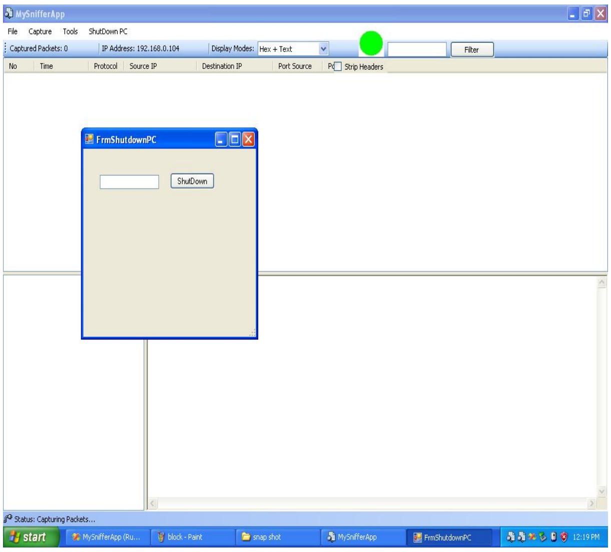


Fig. 4 Packet Loss Ratio Comparisons

Above analysis of result is based on the performance of network determined by my sniffing method. We can also analyze the result on the basic of working of sniffer, for this purpose I studied many tool and found some deficiencies in those tools. My tool can capture data as well as notify the problems or any attack occurred in system, if any attack is detected then we can shutdown the system. Following figure show snapshot of system shutdown in developing tool.



Captured Packets: 0

IP Address: 192.168.0.104

Display Modes: Hex + Text

Status: Capturing Packets…

Fig.5 System Shutdown

VII. CONCLUSIONS

Packet sniffer is not just a hacker's tool. It can be used for network traffic monitoring, traffic analysis, troubleshooting and other useful purposes. Packet sniffers can capture things like passwords and usernames or other sensitive information. Networks Sniffing in non switched network is easy but sniffing in switched network is difficult because we use switches in network which narrow the traffic and send to particular system, so for sniffing in this type of network we use some methods. There are many available tools. Packet sniffer can be enhanced in future by Incorporating features like making the packet sniffer program platform independent, and making tool by neural network. 10 GBPS LAN which are used currently, sniffing can done on this rate in future very effectively.

REFERENCES

[1] Qadeer M.A., Zahid M., Iqbal A., Siddiqui M.R "Network Analysis and Intrusion Detection Using Packet Sniffer ICCSN ' Second International Conference, 2010, Page(s): 313 – 317

[2] S. Ansari, Rajeev S.G. and Chandrasekhar H.S, "Packet Sniffing: A Brief Introduction", IEEE Potentials, Dec 2002- Jan 2003, Volume: 21 Issue: 5, pp: 17 – 19

[3] Daniel Magers "Packet Sniffing: An Integral Part of Network Defense", May 09, 2002 SANS Institute 2000 – 2002.

[4]Seong-Yee Phang, HoonJae Lee, Hyotaek Lim "Design and Implementation of V6SNIFF: an Efficient IPv6 Packet Sniffer" Third 2008 International Conference on Convergence and Hybrid Information Technology

[5] Liqiang Zhang, Huanguo Zhang "An Introduction to Data Capturing" International Symposium on Electronic Commerce and Security.

[6] A. Dabir, A. Matrawy, "Bottleneck Analysis of Traffic Monitoring Using Wireshark", 4th International Conference on Innovations in Information Technology, 2007, IEEE Innovations '07, 18-20 Nov 2007, Page(s):158 – 162

[7] All about Tools [Online] Available: http://www. sectools.org/