Journal of Analysis and Computation (JAC)
(An International Peer Reviewed Journal), www.ijaconline.com, ISSN 0973-2861
Volume XVII, Issue II, July-Dec 2023

Network Monitoring and AnalysisUsing Packet Sniffing

Md. Rizwan Khan[1], Jirin Jain [2], Dhruv Shringi [3]

[1]*Assistant Professor, Jaipur Engineering College & Research Center, Jaipur, India*
[2] *Student, Jaipur Engineering College & Research Center, Jaipur, India*
[3]*Student, Jaipur Engineering College & Research Center, Jaipur, India*

ABSTRACT

In the past decades computer network have kept up growing in size, complexity and along with it the number of its user is also being increased day by day. For complex network it's very tough task to maintain and monitor the network, because large amount of data available. For this purpose, packet sniffer is used. Packet sniffing is important in network monitoring to troubleshoot and to log network. Packet sniffers are useful for analysing network traffic over wired or wireless networks. This paper focuses on packet sniffer working in different environments, Behaviour of already existing sniffer; their problems and challenges while performing sniffing.

Keywords— Packet capturing, Traffic analysis, Network Monitoring, NIC, switched environment, non-switched environment, Network analyzer, Packet sniffer.

[1] INTRODUCTION

Packet sniffing is defined as a technique that is used to monitor every packet that crosses the network. A packet sniffer is a piece of hardware or software that monitors all network traffic. It is also known as Network or Protocol Analyzer or Ethernet Sniffer. The packet sniffer captures the data that is addressed to other machines, saving it for later analysis. For most organizations packet sniffer is largely an internal threat.

Packet sniffers can be operated in both switched and non-switched environment. Using the information captured by the packet sniffer an administrator can identify erroneous packets and use the data to pinpoint bottlenecks and help maintain efficient network data transmission. This is unlike standard network hosts that only receive traffic sent specifically to them. Packet sniffer is a computer software that runs on a networked device. That passively collects all frames going through the data link layer through means of the devices. In theory, it's impossible to detect these sniffing tools because they are passive in nature.

[2] 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. 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 arrive at that interface.

Fig.1 Packet Sniffing

However, if the network interface of a machine is in promiscuous mode, the NICof this machine can take over all packets and a frame it receives on network, namely this machine (involving its software) is a sniffer. When a packet is received by a NIC, it first compares the MAC address of the packet to its own. If the MAC address matches, it accepts the packet otherwise filters it. This is due to the network card discarding all the packets that do not contain its own MAC address, an operation mode called no promiscuous, which basically means that each network card is minding its own business and reading only the frames directed to it. When NIC accept packets, packets are copied to driver memory then it passes to kernel and kernel passes it to user application.

[3] SNIFFER COMPONENTS

Basic Components of sniffers are: -

A. Hardware: - When we are working with sniffer, hardware is required sometimes for analyzing hardware problems like voltage problems, cable problems. If you use special hardware, you can analyze hardware faults like CRC errors, voltage problems, cable programs, "dribbles", "jitter", negotiation errors.

B. Drive Program: -This is the most important part. This is main component of sniffer; each sniffer contains 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 buffers used. First one is where data captured continuously and

second one where new packet replace old packets.

D Decode: - This displays the contents of network traffic with descriptive text so that an analysis configure out what is going on.

E Packet Analysis: - Packet analysis can be done on real time or we can analyse packets after storing it. We can analyse 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.

[4] RELATED WORK

In There are lots of works done on packet sniffing for LAN or WAN monitoring; lots of tools are available for network monitoring. In this paper some tools behavior is analyzed. Wire shark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, but Wire shark 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. So, we have to design a tool which resolves all problems mentioned above and consume less space.

[5] PROPOSED 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 thebasic of various protocols like IP, TCP, UDP, ICMP andIGMP. 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. Networktraffic volume and packet loss can be determined using this captured information.

[6] RESULT

Network 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 includes various test conducted on data captured from network, these tests 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.

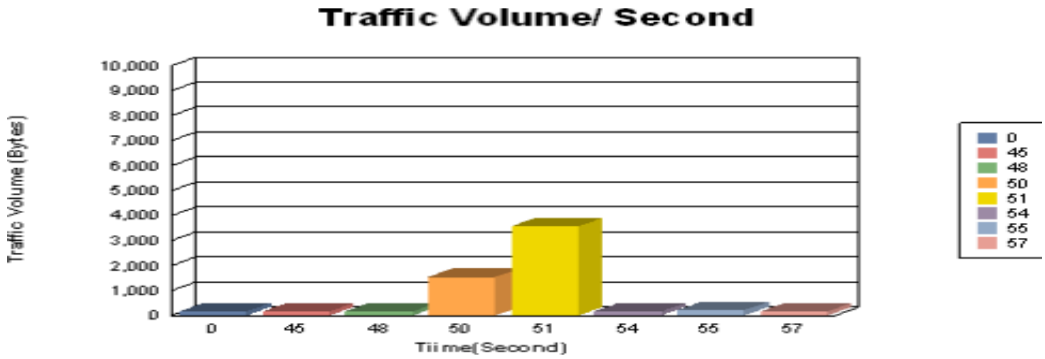


Fig. 2 Traffic volumes at network for dataset 1

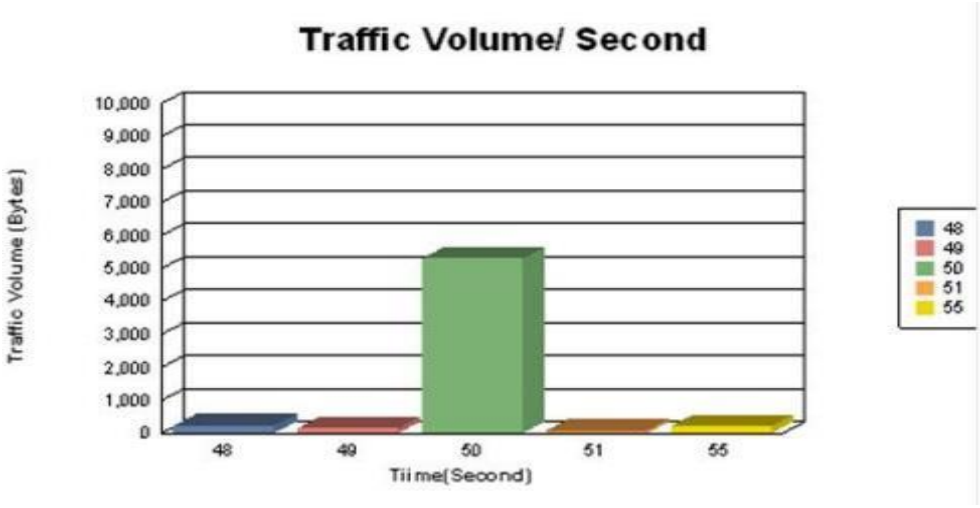


Fig. 3 Traffic volumes at network for dataset 2

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 packets + 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.

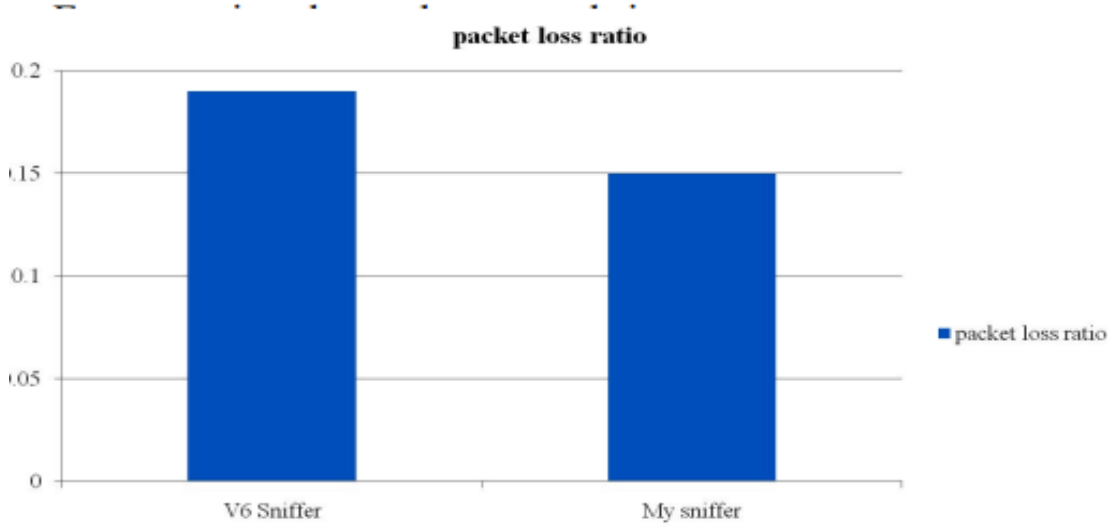
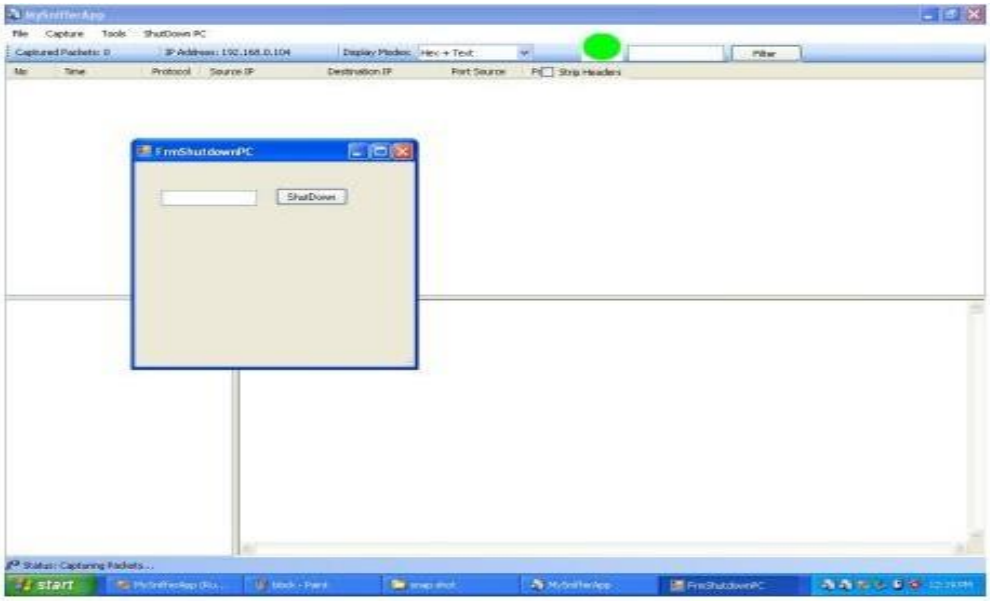


Fig. 4 Packet Loss Ratio Comparisons

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 tools 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 shut down the system. Following figure show snapshot of system shutdown in developing tool.

Fig.5 System Shutdown

[7] CONCLUSION

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 and Data is sent across the internet in the form of packets. Detection of packets can be used for any network or malicious purposes. Sniffing is possible on non- switched and switched networks. There is software to help detect a crawler in a network. Business systems often set up to maintain their information security. Without using modern security and best practices, attackers can easily view data transmitted over the network. We can conclude that packet sniffers can be used in intrusion detection. There exist some tools also that can be used for intrusion detection. Thus, we can say that packet sniffing is a technique through which we can create an intrusion and through which we can detect an intrusion.

REFERENCES

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

[2] Pallavi Asrodia, Hemlata Patel, "Network traffic analysis using packet sniffer", International Journal of Engineering Research and Application (IJERA), Vol.2, pp. 854-857, Issue 3, May-June 2012.

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

[4] Qadeer M.A., Zahid M., Iqbal A., Siddiqui M.R "Network Traffic Analysis and Intrusion Detection Using Packet Sniffer" ICCSN '10 Second International Conference, 2010, Page(s): 313 - 317

[5] G.Varghese, "Network Algorithmic: An Interdisciplinary Approach To Designing Fast Networked Devices", San Francisco, CA: Morgan Kaufmann, 2005.

[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 – 16