ISSN: 2277-9655
Impact Factor: 4.116

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

# ANALYSIS TO ENHANCE THE NETWORK MONITORING BY MULTI-CHANNEL PACKET-ANALYSIS SYSTEM (MPAS)

**Ms Bhavya Yagnik*, Dr. Sanjay Kumar**
MTech Scholar(CSE), Jaipur National University, Jaipur, Rajasthan, India
Associate Prof.(CSE), Jaipur National University, Jaipur, Rajasthan, India

**DOI:** 10.5281/zenodo.154198

## ABSTRACT

In the present times it is observed that there is a sudden rise in computer network technology. Its users have also increased in past few years & flow of traffic in networks is also raised. Hence, it has become a need to watch over the activities of user over the network, traffic of network in order to retain smoothness & efficiency of network. For the networks having a complicated structure, it is a hefty job to regulate & watch over the network as the data present is in very huge quantity. Therefore, packet sniffing is applied. Packet sniffing is very much important to watch over the activities of a network that helps the administrators of network to recognize the problems. In previous paper [8], the concentration is over the packet sniffers that are performing their tack in different kinds of environmental conditions, characteristics of existing sniffers, issues related to them & problems faced by them while executing sniffing. For successful completion of a watching job, a software is develop that will eliminate the drawbacks of the present tool. By implementing the packet sniffer, they maintain the traffic as well analyze it. Reports can also be prepared based on the traffic that is analyzed. Several protocols such as IP, TCP, UDP are applied & filtration is performed over them as per the protocol. Alerts are made if any suspicious activity is found. In this paper, a MPAS (multi-channel analysis system) is presented which supports debugging & verification of multi channel protocols. The ratio of packet loss can be minimized by implementing MPAS.

**KEYWORDS**: Packet capture, Network Monitoring, Network analysis, Packet sniffing.

## 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.

**A. 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].

ISSN: 2277-9655
Impact Factor: 4.116

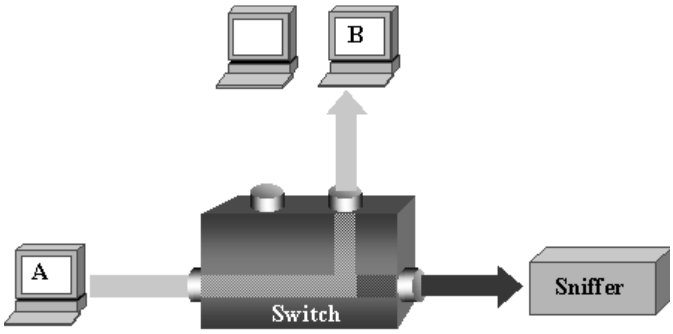


***Fig. 1 Basic sniffing process***

**B . Sniffer Components:** Any sniffer can be divided in following components [3].

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

- *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.

- *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.

- *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.

**C. How Packet Sniffer Works:** Packet sniffer's working can be understood in both switched and non switched environment. For setup of a local network there exist machines. These machines have its own hardware address which differs from the other. When a non switched environment is considered then all nodes are connected to a hub which broadcast network traffic to everyone. So as soon as a packet comes in the network, it gets transmitted to all the available hosts on that local network. Since all computers on that local network share the same wire, so in normal situation all machines will be able to see the traffic passing through. When a packet goes to a host then firstly network card checks it MAC address, if MAC address matches with the host's MAC address then the host will be able to receive the content of that packet otherwise it will forward the packet to other host connected in the network. Now here a need arises to see the content of all packets that passes through the host. Thus we can say that when a host or machine's NIC is setup in promiscuous mode then all the packets that is designed for other machines, is captured easily by that host or machine.

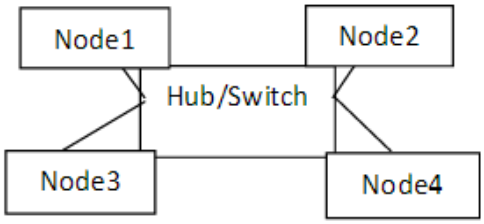


***Fig. 2 IEEE 802.3 network***

When a switched environment is considered then all hosts are connected to a switch instead of a hub, it is called a switched Ethernet also. Since in switched environment packet sniffing is more complex in comparison to non switched network , because a switch does not broadcast network traffic. Switch works on unicast method, it does not broadcast network traffic, it sends the traffic directly to the destination host. This happens because switches have CAM Tables. These tables store information like MAC addresses, switch port and VLAN information. To understand working of packet sniffer in switched environment , an ARP cache table is considered. This is a table that stores both MAC addresses and IP addresses of the corresponding hosts. This table exists in local area network. Before sending traffic a source host should have its destination host, this destination host is checked in the ARP cache table. If destination host is available in the ARP cache then traffic will be sent to it through a switch, but if it is not available in the ARP cache then source host sends a ARP request and this request is broadcasted to all the hosts. When the host replies the traffic can be send to it. This traffic is sent in two parts to the destination host. First of all it goes from the source host to the switch and then switch transfers it directly on the destination host. So sniffing is not possible.

## 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. Wire shark is a free and open-source packet analyzer [6]. It is used for network troubleshooting, analysis, but wire shark does not provide any intrusion detection and have more memory requirement for installation. Tcp dump 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.

## PROBLEM STATEMENT

In the present times it is observed that there is a sudden rise in computer network technology. Its users have also increased in past few years & flow of traffic in networks is also raised. Hence, it has become a need to watch over the activities of user over the network, traffic of network in order to retain smoothness & efficiency of network. For the networks having a complicated structure, it is a hefty job to regulate & watch over the network as the data present is in very huge quantity.

Therefore, packet sniffing is applied. Packet sniffing is very much important to watch over the activities of a network that helps the administrators of network to recognize the problems. In base paper, the concentration is over the packet sniffers that are performing their tack in different kinds of environmental conditions, characteristics of existing sniffers, issues related to them & problems faced by them while executing sniffing. For successful completion of a watching job, a software is develop that will eliminate the drawbacks of the present tool. By implementing the packet sniffer, they maintain the traffic as well analyze it. In base paper, my sniffer technology is suggested for minimizing the proportion of loss of packets. This proportion can be minimized by the suggested technology.

## PROPOSED METHODOLOGY

MPAS (multi-channel packet-analysis system) is demonstrated that leads to verification & debugging of multiple-channel protocols. Every module of sniffer detects the packet of wireless network & time stamps them in MPAS for every channel. The preprocessing of packets is performed & relayed to an analyzer constituted over GUI which further parse these packets received & presents them in a particular order. Here, the outcomes of implementation & designing of MPAS are presented & its performance is analyzed when it is put in contrast to a packet sniffer. MPAS will be able to minimize the proportion of loss of packets & compare the outcomes with the base paper.

The MPS is constituted over several modules of sniffer that are scalable type & a module of time synchronizer. Ever module of sniffer watch over one out of 16 channels of IEEE 802.15.4 over 2.4 GHz & it is easy to scale the MPS to a bigger level to sniff other channel by incorporating a new module of sniffer. The module of time synchronizer helps in synchronizing all the modules of sniffer in MPS by using a button for synchronization which is responsible for triggering the protocol of time synchronization simultaneously on each of the module of sniffer. A hardware button is implemented for minimizing the uncertainty on the approach based over software. As the synchronization

in module of sniffer is executed, it capture each packet in the channel, confines the packet in UART (universal asynchronous receiver/transmitter) format of message & then conveys it to MPA. At last, the message is received by the MPA from MPS, it is analyzed & the packets are presented in the window of output.

## RESULTS

In the Results session , we are showing the packet Loss Ratio for MPAS system . As we can see from figure 3 , three options of Network Monitoring , Generate Attack and Exit are mention . Network monitoring is using for show the process of MPAS system and generate Attack is using for generate attack in Packet Sniffing . As the Attack will generate the system will get shut down . Due to limitation of Hardware , we are using Generate Attack Button which is working like as a Packet sniffing hardware module .

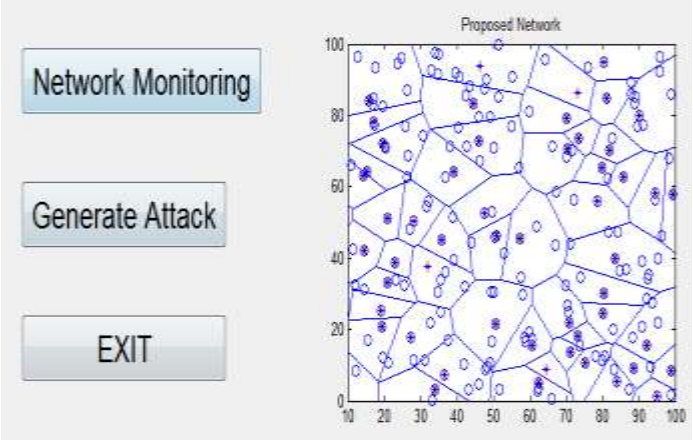


***Fig. 3 Network Monitoring based GUI***

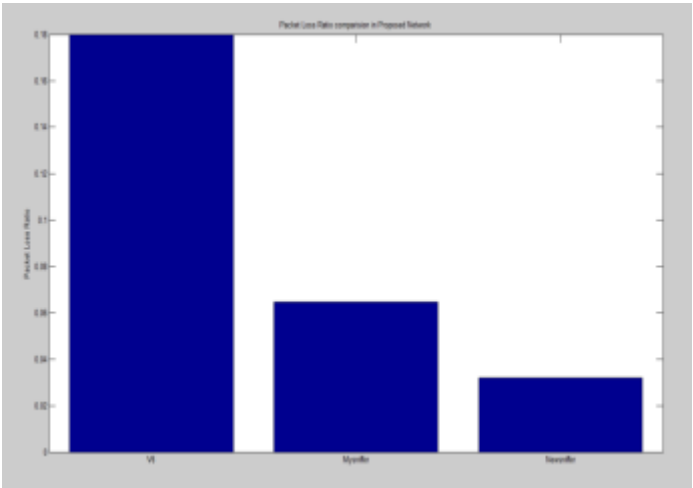

***Fig. 4 Packet Loss Ratio Comparison***

From the Fig. 4 , it is clear that Packet loss Ratio get decrease by use MPAS system.

## CONCLUSION

The packet sniffer is just not considered as a tool for hacking. It can be applied for tracking the traffic over a network, analyzing the traffic, troubleshooting & various other applications. Packet sniffers are used to gather the sensitive information such as usernames or passwords and other sort of data. It is easy to implement network switching in that network that is not switched but implementing sniffing in a network that is switched is not an easy task as by switching is applied over that network in which passage of traffic is short & is sent to a defined system. Hence, some different techniques are applied for implementing the sniffing. There are various tools provided for this

in the market. Further, it is required to improvise the packet sniffer by indulging the characteristics such as making the program independent from any platform & making a tool by neural network. The presently implemented 10 GBPS LAN is used where sniffing can be applied on the same rate in an efficient manner.

## 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/.

[8] Pallavi Asrodia, Mr. Vishal Sharma," Network Monitoring and Analysis by Packet Sniffing Method". International Journal of Engineering Trends and Technology (IJETT) - Volume4Issue5- May 2013.