IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

A REVIEW: IMPROVED NETWORK MONITORING AND ANALYSIS BY MULTI-CHANNEL PACKET-ANALYSIS SYSTEM (MPAS)

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

DOI: 10.5281/zenodo.61607

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. 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. Previous paper[8] focuses on packet sniffer working in different environments, Behavior of already existing sniffer; their problems and challenges while performing sniffing. To accomplish monitoring task, a tool is developed which will remove deficiencies of existing tool. By using this packet sniffer we can capture traffic as well as analyze captured traffic. We can generate reports on the basis of analyzed traffic. Alerts generated on the occurring of suspected activities. In this paper , We present a multi-channel packet-analysis system (MPAS) that helps in debugging and verification for multi-channel protocols or applications. By using MPAS we will reduce the packet loss ratio.

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].

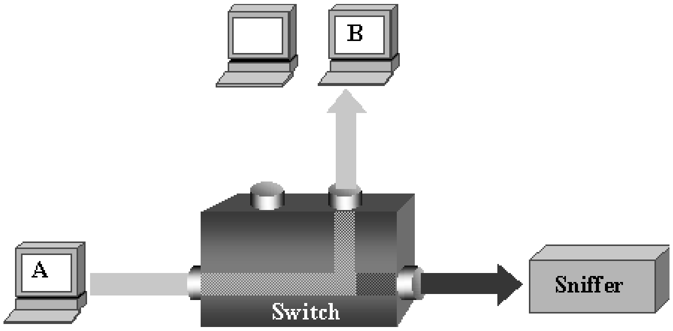

Fig. 1 Basic sniffing process

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.

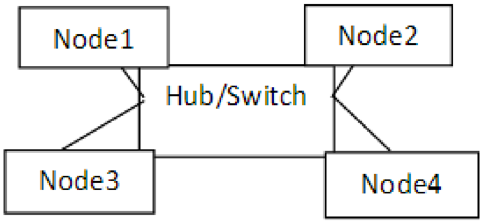

Figure 1: IEEE 802.3 network

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

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. In the base paper they 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 they capture traffic as well as we analyzed capture traffic. In the base paper , they propose the my sniffers methodology for reduce the packet loss ratio. We can further reduce the packet loss ratio by our proposed methodology .

PROPOSED METHODOLOGY

We present a multi-channel packet-analysis system (MPAS) that helps in debugging and verification for multi-channel protocols or applications. Wireless packets are detected and time stamped by each sniffer module in the MPAS for each channel, and packets are preprocessed and transmitted to a GUI-based analyzer, which then parses the received packets and shows them in order. We present the design and implementation results of the MPAS and evaluate its performance by comparing it against a widely used packet sniffer. By use MAPS we will reduce the packet loss ration and comparer the results from the base paper results .

The MPS is based on multiple scalable sniffer modules and a time synchronizer module. Each sniffer module monitors one of the 16 channels for IEEE 802.15.4 at 2.4GHz, and the MPS can be easily scaled up to sniff another channel by adding a new sniffer module. The time synchronizer module synchronizes all the sniffer modules in the MPS through the use of a synchronization button that stimulates the start of a time synchronization protocol concurrently on all the sniffer modules. The hardware button is used to reduce the uncertainty of a software based approach. As long as each sniffer module is synchronized, it captures every packet in its channel, wraps the packet in the universal asynchronous receiver/transmitter (UART) message format, which is explained in Section 3.2, and then sends it to the MPA. Finally, the MPA receives the message from the MPS, analyzes it, and displays the packets in the analysis output window.

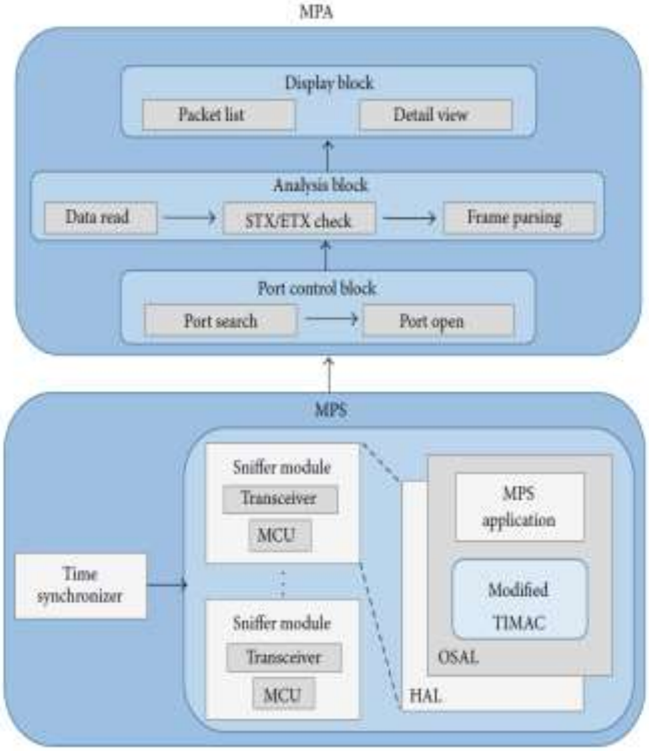

Figure 1: Multi-channel packet-analysis system (MPAS) overview.

Multi-Channel Packet Sniffer: The MPS is a scalable and easily extendable sniffer that consists of multiple sniffer modules and a time synchronizer module. Rather than designing a new hardware platform for the sniffer module, we adopt a COTS platform, the MSP-EXP430F5438 , from Texas Instruments Inc., based on anMSP430F5438 microcontroller unit and a CC2520EM IEEE 802.15.4 transceiver module, as seen in Figure. To monitor multiple channels simultaneously, each sniffer module fixes its channel without switching the monitoring channel dynamically while sniffing. We build another component of the MPS, a time synchronizer module with a low-pass filter hardware reset switch. To start packet sniffing, we initiate time synchronization between sniffer modules by pressing the reset switch, and the time synchronizer generates a hardware signal to all the attached sniffer modules. A general purpose input/output (GPIO) pin in each sniffer module is used to capture the hardware signal from the time synchronizer to synchronize the sniffer modules with each other. The hardware signal triggers an interrupt on each sniffer module, and the sniffer module initializes its time reference. The software platform of each sniffer module is based on TIMAC1.4.0 [17], and we modified TIMAC to promiscuously capture every frame in the radio communication range. To receive the packet regardless of the destination address, the MAC radio RX frame filtering function needs to be turned off.

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. 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/.

[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.