ISSN No:-2456-2165

Comparative Study of Network Protocol Analyzer and Existing Tools

Suvarna Chavan, Sachin Patel
Department of Computer Science and Engineering
Swami Vivekanand College of Engineering
Indore, India

Abstract:- In present days use of computer network is increased, on the premise of increased number of users and traffic flows. So it is essential to keep tab on network traffic and user activities for efficient working of network. It is difficult to monitor the complex network due to large data. To monitor such a complex network the Network Protocol Analyzer (NPA) can be used. Network protocol analyzer is important in network monitoring to troubleshoot and to log network. NPA are useful for analyzing & monitoring network traffic over the networks. NPA plays main role in network monitoring to watch network activities which help network administrators to troubleshoot and to log network and it gives detail information about the received data. In this paper we explained network protocol analyzer it's working Principle which used for analysis network traffic and also comparative analysis of NPA and existing tools which are SoftPerfect network protocol analyzer, Netflow analyzer, Riverbed steel Central Packet Analyzer, Debookee Network Protocol Analyzer.

Keywords:- *Network protocol analyzer, NIC, Filters, Packet capture, network monitoring.*

I. INTRODUCTION

Recently, the size of computer network is rapidly increasing; it is difficult to monitor the complex network due to large data. To monitor such a complex network the Network Protocol Analyzer (NPA) can be used.NPA is also known as packet analyzer or network analyzer or packet sniffer.NPA plays significant role in network analysis and monitoring to watch network activities which help to troubleshoot and to log network.

Role of NPA (Network Protocol Analyzer) is to analyze and monitor network traffic. Here, NPA capturing network traffic and then applied for analysis & control by using filters. Filter plays main role for controlling packets which misbehaves**.** Network protocol analyzer is a program running in a network attached device that passively receives all frames passing through the device's network adapter. The NPA captures the data that is directed to other machines and saving it. It can be used for analyzing and monitor, troubleshoot network traffic [27] [13].

- *Promiscuous Mode*

Network interface card (NIC) it can working in two modes promiscuous and non promiscuous. Generally whenever packet is received at network interface card it first compares with its own MAC address. So if matching of MAC address found, then it allows the packet else make it filter. It happens because network interface card discards each and every packet which does not contain its own given MAC address, non promiscuous basically define each network card is reading only own frames which directed to it or reading only the frames instructed to it. For capturing the packets it required to transfer NIC in to promiscuous mode. Its role of network protocol analyzer to do capturing by initiating NIC card of its own system to promiscuous mode and then it receives each and every packet even it has different MAC address [6]. Hence receives all packets even they are not intimates for it. The figure A shows network interface card (NIC).

Fig 1:- Network Interface Card (NIC)

- *Working of Npa*

Suppose there is a machine on network and the network interface card (NIC) of this machine is in promiscuous mode, then NIC of this machine can take over all packets and a frame it receives on network, then this machine is a network protocol analyzer [27]. When as 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 [6] [27]. Network protocol analyzer which do sniffing or capturing by setting the NIC card of its own system to promiscuous mode, and hence receive all packets even they are not intimates for it. So, NPA captures the packets by setting the NIC card into promiscuous mode. The packet reach at the NIC are copied to the device driver memory, which is then passed to the kernel buffer from where it is used by the user application [6].

ISSN No:-2456-2165

II. LITERATURE SURVEY

Form the literature survey; it is observed that there are much software is available for analyzing and monitoring protocols in networks. The details of such software are given in following section.

A. Soft perfect network protocol analyzer

Soft Perfect Network Protocol Analyzer [16] is a free professional tool for analyzing, debugging, maintaining and monitoring local networks and Internet connections and it captures the data passing through the dial-up connection or Ethernet network card, analyses this data and then represents it in a readable form [16]. This is a useful tool for network administrators, security specialists, network application developers and anyone who needs a comprehensive picture of the traffic passing through their network connection and it can defragment and reassemble network packets into streams [16].

The flexible system of fully-configurable filters can be used to discard all network traffic except for the specific traffic patterns you wish to analyze [16]. Here the Fig. A (a) shows soft perfect Packet capturing & which can captures 1001 packets and Fig A (b) shows soft perfect network flow analysis.

➢ *Features*

- It can decodes packets and displays them in an easy format
- It works in promiscuous mode
- It monitors loopback connections within the system [16].

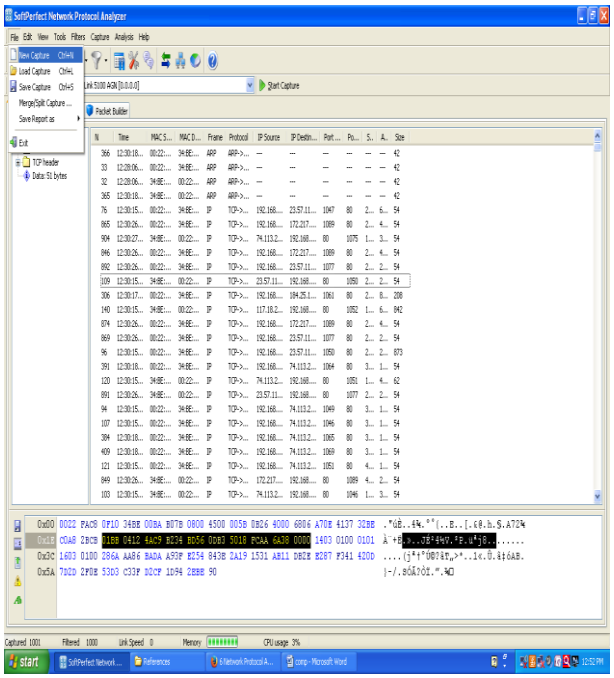

Fig 2:- softperfect Packet capturing & captures 1001 packets

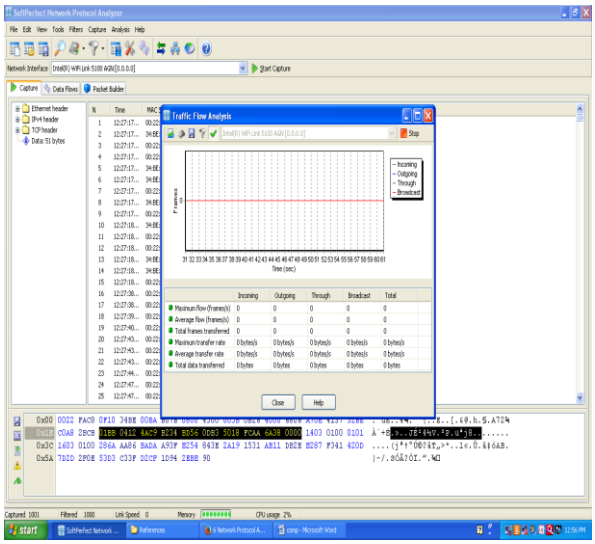

Fig 3:- softperfect network flow analysis

B. Netflow Analyzer

It is a netflow monitoring tool which collects NetFlow packets or other supported flows exported from enterprise routers and switches, generating network traffic reports that help understand the nature of the network traffic and the bandwidth utilization, thus helpful in traffic analysis and bandwidth monitoring and Net Flow monitoring achieves a new level when a solution such as Manage Engine Net Flow Analyzer is aligned to Cisco technologies such as Net Flow, NBAR [28].

It is a protocol developed by Cisco, is used to collect and record all IP Traffic going to and from a Cisco router or switch that is Net flow enabled and that permitted you to collect traffic and analyze it through a program which then organizes the flow records into a format that allows the IT administrator or Network engineer to further analyze the traffic [29]. The protocol permitted you to really drill down into your network traffic to see where the traffic source is coming from and to where it is destined too, when troubleshooting slow LAN or WAN network connections and the protocol itself does not analyze the traffic, but as mentioned previous, when configured properly it sends traffic to a Collector or Analyzer, which is either a hardware device or more often than not, a software program [29].

➢ *Net Flow packet details are as follows*

- It has Source and destination IP address
- It has Input and output interface number
- It has Source and destination port number
- It has Layer 4 Protocol
- It has Number of packets in the flow
- It has Total Bytes in the flow
- It has Time stamp in the flow
- It has Source and destination AS
- It has TCP_Flag & TOS [21].

C. River Bed Steel Central Packet Analyzer

Riverbed Steel Central Packet Analyzer is a visually rich and powerful analyzer for wired and wireless networks that revolutionizes the use of Wireshark by providing capabilities not found in the world's most popular packet and network analysis tool and fully integrated with Wireshark, Steel Central Packet Analyzer capitalizes on users existing expertise while dramatically increasing efficiency in identifying and diagnosing network problems and Some network and application problems can only be resolved by capturing network traffic and analyzing it in depth, it makes this easy by helping you find the packets you're looking for visualize the data and create professional reports [30].

➢ *System Requirements*

It requires Windows XP, Windows Vista, and Windows 7 [30].

➢ *Hardware Requirement*

- It requires dual-core 2.0 GHz CPU
- It requires 2 GB RAM
- It requires 300MB free disk space plus additional space for trace files and reports [30].

D. Debookee

There are many alternative tools to Wireshark, Debookee is one among them which works only on macos and it allows the user to see what is happening on their network at a microscopic level and we can even use mobile to capture the data that is being transmitted from Mac or any other device [22]. It is a LAN and Wi-Fi packet-capture tool and network analyzer that allows you to see what your devices are sending over the network [23].

➢ *What Is It?*

Debookee is a simple to use network traffic logger, it is a single window application that makes things very simple to work in, it breaks each device into three views: DNS, Http and Other TCP, DNS will show just hostnames and associated IP addresses and it is a great application to check patterns on your network, to see what devices are making far too many requests or build a knowledge base of servers being requested from certain applications [24]. The drawback is that Debookee is with large logs it can get a little slow and take up quite a bit of memory [24].

➢ *Features*

- It decrypt IMAPS email traffic and Full raw data is shown, not only headers[23]
- It has Simple interface
- It has Single window
- It is Easy to read log file
- It has Quick filter [24].

➢ *Requirements For Debookee*

- It requires Intel, 64-bit processor
- It requires MacOS 10.12 [23] [25].

III. OBJECTIVE

A network protocol analyzer (NPA) is used for analyze and monitor network traffic. It's monitoring & controlling is on basis of packet filtration. The packets are filtered with some rules. The network protocol analyzer means it can be used for-

- Analyzing network traffic
- The gaining information for effecting a network intrusion
- Monitoring network
- collect and report network statistics and graphical information
- Finding which Protocol used on network

It shows you the problem on network. The NPA show you the information about protocols, and the traffic seen on network, and the number of users, number of users using each protocol. It also shows statically and graphical representation of different layers protocol. Appropriate network monitoring is essential for improving application performance and network management.

Network Protocol analyzers, have a variety of results and benefits in a network environment. It includes:

- Troubleshooting
- Base lining/Testing
- Monitoring
- Security
- Intrusion Detection

IV. RESULTS

In NPA we are analyzing network traffic by capturing the packets. The fig 4 shows the packet capturing window in which the NPA captures 10000 packets in one cycle or in one phase. The fig.5 shows that the NPA can access multiple window at one time means it we can access multiple windows a time. The fig 6 shows that applying filter in which how to apply constraints over attributes of network & it choose device required for capturing.

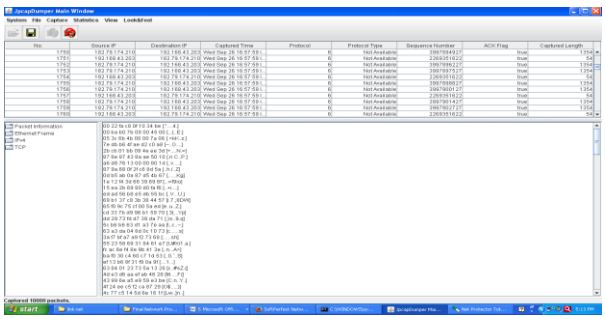

Fig 4:- NPA Capturing 10000 packets

ISSN No:-2456-2165

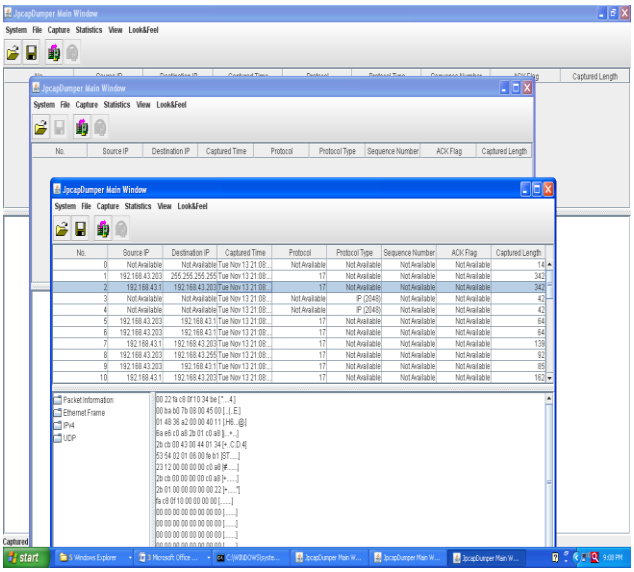

Fig 5:- Accessing multiple windows

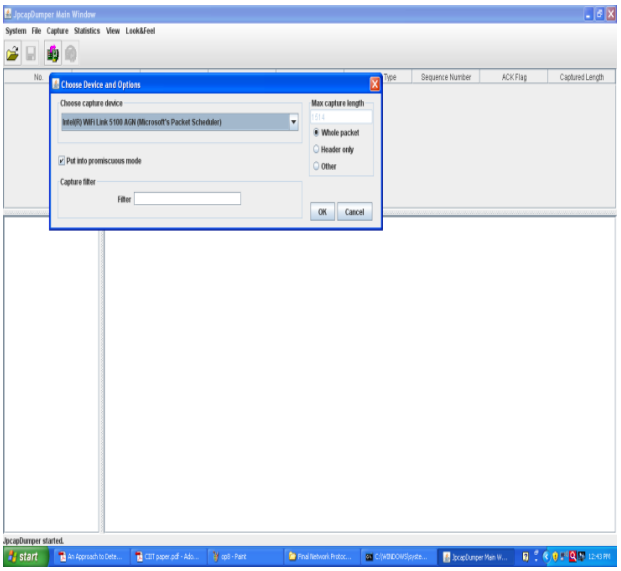

Fig 6:- Applying Filter

In NPA we are analyzing network traffic by using two ways one as runtime graphical representation of traffic in network and another is runtime statistical representation.

Graphical presentation is allows to show runtime graphs according with the traffic. Fig. 7 shows Graphical Representation of Transport Layer Protocol Ratio, the same can be shown for network and application layer.

Statistical presentation is allows to show runtime numbers according with the traffic. Fig. 8 shows statistical Representation of network Layer Protocol Ratio, fig. 9 shows statistical Representation of application Layer Protocol Ratio, the same can be shown for transport layer.

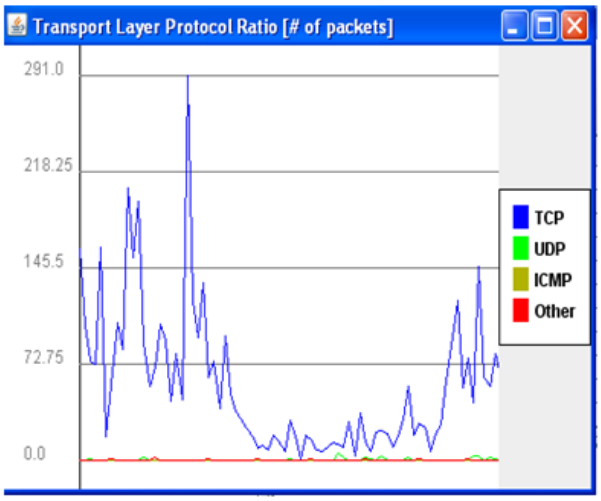

Fig 7:- Graphical representation of Transport layer protocol ratio

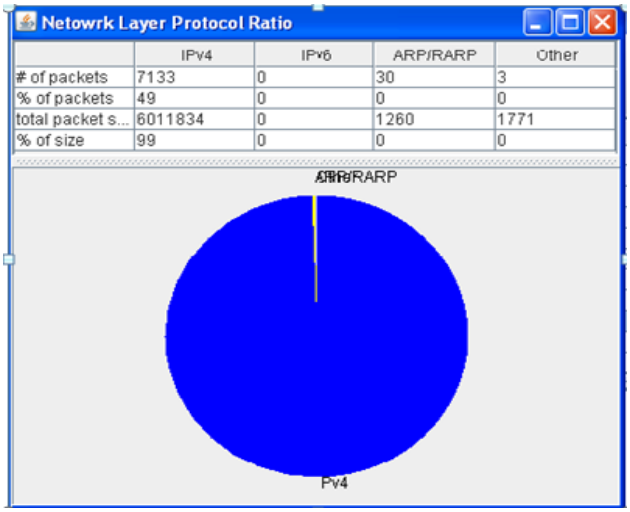

Fig 8:- Statistical representation of network layer protocol ratio

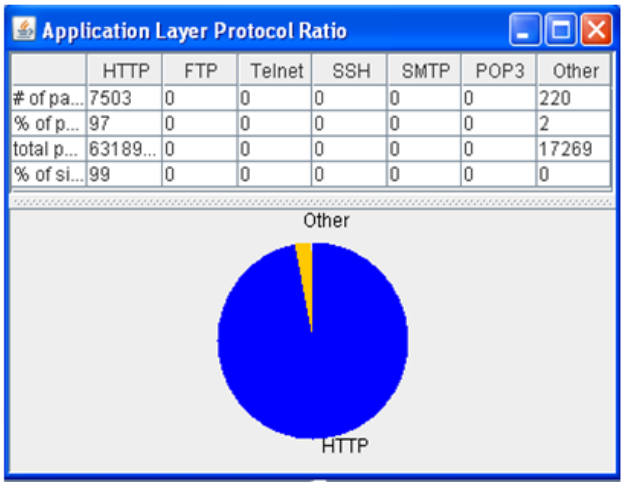

Fig 9:- statistical representation of Application layer protocol ratio

V. COMPARATIVE STUDY

Property/Tools	NPA	Softperfect	Netflow Analyzer	Riverbed steel Central Packet Analyzer	Debookee Network Protocol Analyzer
Applying Filter	Easy in NPA	Complex in Softperfect	No Filters to be used	Not Defined	Complex
Graphical Analysis	Easy to handle & understand	Complex to handle & understand	Complex to handle & easy to understand	Complex Analysis	Easy to handle & understand
User friendliness	More user friendly	Less user friendly	User friendly	Less user friendly	User friendly
Multiple window access	Allowed to access multiple windows at same time.	Not allowed. Only one window access at time.	Not allowed. Only one window access at time.	Not allowed. Only one window access at time.	Allowed multiple interfaces.
Packet Capturing	Captures 10,000 packets in one cycle	Captures 1001 packets in one cycle.	Not specified	Captures till 100 MB Space used	Not Specified
Cost	Free	Free	Starts from $795	Non Free	$29.90 to $129.90

Table 1:- Comparison of NPA and other existing tools

VI. CONCLUSION

A network protocol analyzer is used for analyze and monitor network traffic. It is monitoring & controlling is on basis of packet filtration. The packets are filtered with some rules. The main role of network protocol analyzer is that can be used to analyzing network traffic, network intrusion detection, Monitoring network traffic, collect and reporting on network statistical and graphical information, network protocols used on network, network problems and filters plays an important role to control network traffic. There are many tools available in market for network monitoring and analysis but some tools have limitation like for packet capturing, packet analysis, for using filters or other problems like memory limitation, for multiple window accessing etc. So NPA is a tool that done almost users requirements. In future it is possible to use filters at large level i.e. we can apply constraint to any attributes which belongs to packets or protocols.

REFERENCES

[1]. Shrutika Suri,"Comparative Study of Network Monitoring Tools", http://www.ijitee.org, ISSN: 2278-3075, Volume-1, Issue-3, Aug14.
[2]. Pallavi Asrodia, "Network Monitoring and Analysis by Packet Sniffing Method", http://www.ijettjournal.org ISSN: 2231-5381 .Page 2133 Volume4, Issue5- May 2013
[3]. AshishKulkarni, Nimish Kate , RohitGhadshi , Rushikesh Date, "Signature Based Packet Sniffer", International Journal of Advance Research in Computer Science and Management StudiesVolume 2, Issue 3, March 2014 pp.155
[4]. Shilpi Gupta, "Intrusion Detection System Using Wireshark", www.ijarcsse.com, Volume 2, Issue11, Nov-12, ISSN: 2277 128X.
[5]. Rupam, Atul Verma, "An Approach to Detect Packets Using Packet Sniffing", www.IJCSES.com, Vol.4, No.3, June 2013 DOI: 10.5121/ijcses.2013.4302 page: 21.

[6]. Pardeshi Shailendra, "Network Protocol Analyzer for Analyzing and Monitoring Network Traffic by Using Filters", www.ijmrae.com,ISSN 0975-7074, Vol. 3, No. IV (October 2011), pp. 313-322.
[7]. Mohammed Abdul Qadeer, Mohammad Zahid, MisbahurRahmanSiddiqui, "Network Traffic Analysis and Intrusion Detection using Packet Sniffer", 2010 Second International Conference on Communication Software and Networks, 2010, pp: 313-317.
[8]. Daeji Sanai, "Detection of Promiscuous Nodes Using ARP Packet", http://www.securityfriday.com
[9]. S. Ansari, Rajeev S.G., et al, "Packet Sniffing: A brief Introduction", IEEE Potentials, Dec 2002- Jan 2003, Volume: 21, Issue: 5, pp: 17 – 19
[10]. Wireshark2012. About Wireshark [online]. Available: http://www.wireshark.org/about. Html [accessed: July 2012].
[11]. G. Varghse, "Network Algorithmic: An Interdisciplinary Approach to Designing Fast Networked Devices", San Francisco, CA: Morgan Kaufmann, 2005.
[12]. J. Cleary, S. Donnelly, I. Graham, "Design Principles for Accurate Passive Measurement," in PAM 2000 Passive and Active Measurement Workshop (Apr 2000).
[13]. Behrouz Forouzan, "Data Communications and Networking", TMH, 4th Edition
[14]. https://en.wikipedia.org/wiki/Promiscuous_mode.
[15]. www.wikipedia.org/wiki/Packet_analyzer
[16]. All about softperfect [Online] Available http://www.softperfect.com/products/networksniffer/
[17]. www.etsecurity.about.com/od/securitytoolprofiles/.../wireshark.htm
[18]. www.softpedia.com/get/...Tools/Protocol-Analyzers-Sniffers.
[19]. www.softsea.com/software/Protocol- Analyzer.html
[20]. www.windowsitpro.com/hardware/6-network-protocol-analyzers.
[21]. All about netflow analyzer [Online] Available https://www.manageengine.com/products/netflow/cisco-netflow.
[22]. All about debookee [Online] Available https://techwiser.com/wireshark-alternatives-for-windows-and-macos/
[23]. All about debookee [Online] Available ttps://www.macupdate.com/app/mac/45535/debookee.
[24]. All about debookee [Online] Available http://bestosx.software/software/debookie
[25]. All about debookee [Online] Available https://alternativeto.net/software/debookee/.
[26]. All about debookee [Online] Available https://debookee.com/
[27]. Anshul Gupta, "A Research Study on Packet Sniffing Tool TCPDUMP", International Journal of Communication and Computer Technologies, Volume 01 – No.49 Issue: 06 Jul 2013, ISSN NUMBER: 2278-9723
[28]. https://www.manageengine.com/products/netflow/netflow-monitoring.html
[29]. https://www.pcwdld.com/what-is-netflow
[30]. All about Riverbed SteelCentral packet analyzer [Online] Available https://www.wansolutionworks.com/SteelCentral-Packet-Analyzer-PE.asp.