CHAPTER 1

INTRODUCTION

The internet is a network of networks which carries a vast range of information resources and services, such as the exchange of documents on the World Wide Web (WWW) and the frame work to support emails and other applications. Internet has long been researched to tackle vast gamut of problems, including security, attacks and monitoring general health of the network. Network analysis is a process of capturing network traffic and inspecting it closely to determine what is happening in the network. It is also known by several other names: network analysis, protocol analysis, packet sniffing and packet analysis, to name a few. Thus, network traffic analysis is a procedure that helps the network administrators to understand the nature of traffic on per packet or per flow level basis. A flow measurement topology is presented in Figure 1.1.

1.1 REASONS TO INSPECT AND ANALYZE TRAFFIC

- To Identify network or communication issues
- Monitor network performance
- Verify network security
- Track communication transactions
- Log network traffic
- Discover source of unwanted traffic
- Discover compromised workstations
1.2 FUNCTIONALITY OF NETWORK ANALYSIS

1.2.1 Network Troubleshooting

In computer networks a single malfunction in a piece of equipment can disrupt the operation of the entire network or at least degrade its performance significantly. Examples of such scenarios include illegal packet sizes, “broadcast storms”, incorrect addresses and security attacks. In such scenarios, detailed measurements from the operational network can often provide a network administrator with the information required to pinpoint and solve the problem.

1.2.2 Protocol Debugging

Developers often want to test their “new improved” versions of network applications and protocols. Network traffic measurement provides a means to ensure the correct operation of the new protocol or application, its conformance to required standards, and its backward compatibility with previous versions, prior to unleashing it on a production network.
1.2.3 Workload Characterization

Network traffic measurement can be used as input to the workload characterization process, which analyzes empirical data to extract salient and representative properties describing a network application or protocol. Knowledge of the workload characteristics can then lead to the design of better protocols and networks for supporting the application.

1.2.4 Performance Evaluation

A network traffic measurement can be used to determine how well a given protocol or application is performing in the internet. Detailed analysis of network measurements can help to identify performance bottlenecks. Once these performance problems are addressed, new versions of the protocols can provide better (i. faster) performance for the end users of internet applications.

1.2.5 Network Planning

Network analysis enables to capture data over a long period of time in order to track and anticipate the network growth. It helps the internet service providers in network planning which includes peering, backbone upgrade planning and routing policy planning. Thus, it detects the unwanted traffic, validates bandwidth and Quality of service (QOS) and enhances the analysis of new network applications.

1.2.6 Security Analysis

Network traffic measurement identifies and classifies denial of service (DOS) attacks, viruses and worms in real time. Change in network behavior indicates anomalies that are easily identified on a close watch over network. The data collected at regular intervals of time is a valuable forensic tool to understand and replay the history of security incidents.
1.2.7 IP Accounting and Usage Based Billing

For Internet service providers (ISP), knowledge of the applications highly used by the subscribers helps in accounting, usage based charging and even for offering new improved products. Thus, network flow analysis provides the ability to implement competitive pricing schemes and premium services. It also helps the administrators to perform strategic analysis on their point of presence (POP) traffic for network planning, acceptable usage policy enforcement or Service Level Management (SLM).

1.3 NETWORK TRAFFIC MEASUREMENT METHODOLOGY

The network traffic measurement tools can be classified in several different ways as follows:

1.3.1 Hardware-based vs. Software-based Measurement Tools

The primary categorization among network measurement tools is hardware-based versus software-based measurement tools. Hardware based tools are often referred to as network traffic analysers: special – purpose equipment designed exclusively for the collection and analysis of network data. This equipment is often expensive, depending on the number of network interfaces, the type of network cards, the storage capacity and the protocol analysis capabilities. Many vendors offer these types of products.

Software–based measurement tools typically rely on Kernel–level modifications to network interfaces of commodity workstations to convert them into machines with packet capture capability. One widely used utility is TCPdump, a user level tool for TCP/IP packet capture, made possible with the Berkeley Packet Filter (BPF). In general, the software–based approach is much less expensive than the hardware–based approach, but may not offer the same functionality and performance as a dedicated network traffic analyser.
Another software–based approach to workload analysis relies on the access logs that are recorded by Web Servers and Web Proxies on the Internet. These logs record each client request for website content, including the time of day, client IP address, URL requested and document size. Processing of such access logs provides useful insight into web server workloads, without the need to collect detailed network – level packet traces.

1.3.2 Passive vs. Active Measurement Approaches

A passive network monitor is used to observe and record the packet traffic on an operational network, without injecting any traffic of its own onto the network. That is, the measurement device is non-intrusive. Most network measurement tools fall into this category.

An active network measurement approach uses packets generated by a measurement device to probe the internet and measure its characteristics. Examples of this approach include the ping utility for estimating network latency to a particular destination on the Internet, the trace route utility for determining Internet routing paths, and the path characteristics tool for estimating link capabilities and latencies along an Internet path.

1.3.3 On-line vs. Off-line Traffic Analysis

Some network traffic analyzers support real-time collection and analysis of network data, often with graphical displays for on-line visualization of live traffic data. Most hardware based network analysers support this feature. Other network measurement devices are intended only for real-time collection and storage of traffic data, while analysis is postponed to an off-line stage. The TCPdump utility falls into this category. Once the traffic data is collected and stored, a researcher can perform as many analysers as desired in the post processing phase.
1.3.4 LAN vs. WAN Measurement

The early network traffic measurement research in the literature was undertaken in Local Area Network (LAN) environment, such as Ethernet LANs. LANs are easier to measure for several reasons. First a LAN is typically administered by a single well known organization, meaning that obtaining security clearance for traffic analysis is a relatively straight forward process. Second, the broadcast nature of an Ethernet LAN means that all packets transmitted on the LAN are seen by all hosts. Network measurement can be done in this context by simply configuring a network interface into promiscuous mode, which means that the interface will receive and record the packets destined to other hosts on the network. Later measurement work, extended traffic collection and analysis to Wide Area Network (WAN) environment. The greater challenges here include administrative control of the network security and privacy issues. For organizations with a single access point to the external internet, measurement devices can be put in-line on an internet link near the default router for the organization.

1.3.5 Protocol Level Measurement

Measurement tools differ in the protocol level at which data is collected and traffic analysis is performed. Many network traffic analyzers support multi-layer protocol analysis, but a specified network card must be used for each type of network on which traffic data is to be collected. For example, specialized network cards exist for Ethernet, Frame Relay, Asynchronous Transfer Mode (ATM) and wireless networks, but the back-end protocol analysis engines for IP and higher-layer protocols may be the same.

1.4 NETWORK MODEL AND REVIEW OF PROTOCOLS

This section provides an overview of the Internet model followed by the protocols used at the network and transport layers. The definition for
Flow is also included since it is applied in many areas including packet filtering, IP routing, dynamic traffic pattern identification and measurement.

1.4.1 The 5- Layer TCP / IP Model

The phenomenal achievement of the Internet has led to the rapid approval of the Internet Protocol (IP) technology to build all types of communication networks, including private commercial networks (intranets), military communication networks, private home networks, smart devices (smart phones, Internet TV) and the emerging Fourth-generation (4G) cellular networks. The traffic in the modern IP networks is disparate and most of the applications used in the networking environment prefer IP as a medium to transmit the data. The traffic generated by these applications has highly deviating characteristics and compulsion to examine the protocols separately becomes credible. Even though several models have been developed to categorize the communication protocols, the 7-layered OSI model and 5-layered TCP/IP model are commonly used in IP network studies. In this thesis 5-layered TCP/IP model as illustrated in Figure 1.2 is considered. Out of the 5 layers, this thesis limits the study to two layers: network and transport layer; and their associated protocols which contribute much for the analysis point of view of the network when inspecting packet traffic.

![Figure 1.2 Layers of TCP / IP model](image)

**Figure 1.2 Layers of TCP / IP model**
1.4.1.1 Network and Transport Layers

The network layer in TCP/IP model is responsible for the transfer of data in the form of packets in an interconnected network. The study of network traffic starts from this network layer, as the first two layers do not contribute much from the aspect of end-to-end traffic study. The main function of network protocols is to establish connectivity between all layer 3 (L3) routers and hosts in the network, thereby allowing communication between the direct or indirect connections. It performs network routing, fragmentation and reassembly functions together with report delivery error handling. In internet, currently IPV6 and IPV4 protocols are responsible for transfer of packets between end machines on a hop-by-hop basis.

It offers a connectionless and best-effort delivery service to the upper transport layer. The connectionless service does not require a virtual circuit to be established prior to the process of data transfer thereby offering a packet switched transfer medium where fidelity of the data is not guaranteed. The connectivity between the end hosts is established by incorporating the routing protocols such as EGP, OSPF, RIP and BGP. The task of resolving host’s physical and IP addresses is managed by ARP and RARP. Maximizing the usage of IP address space allocation to the hosts can be automated by designing a DHCP environment to the network. Error reporting and delivery of control messages are handled by ICMP.

1.4.1.2 Transport Protocols

Transport protocol utilizes the services offered by the underlying network layer protocols and runs on top of the IP. TCP and UDP are the two most frequently used protocols to support a wide range of applications. TCP provides reliable, connection-oriented stream service over IP. It sets up a logical full-duplex connection between two end-hosts across a datagram network. It also provides flow and congestion control, thereby allowing
receivers to control the rate at which senders transmit information preventing buffers from overflowing. Source IP, destination IP, source port and destination port are the four tuple attributes which help TCP in uniquely identifying each connection. TCP ensures connection establishment using three-way handshake by incorporating bidirectional connection which involves the exchange of SYN, SYN+ACK and ACK packets respectively. It is commonly known as a three-way handshake procedure for connection establishment and termination. TCP provides two means for connection termination that is either by FIN packet or through RST. Each FIN packet is reciprocated with an ACK packet. Data reliability is achieved by the use of retransmission timeouts. Hence, TCP uses acknowledge packets and retransmission to guarantee successful transmission of the data.

Unlike TCP, UDP provides a much simpler service to the application. The UDP is an unreliable, connection-less and non-stream oriented transport layer protocol. It is a very simple protocol which aids in demultiplexing and error checking on the data. It is specified by source and destination ports to identify the connection. Flow and congestion control mechanisms are not utilized by UDP. Since UDP is connection-less, it does not implement connection establishment and termination procedure. Thus, the absence of ACK and retransmission mechanism makes it an unreliable protocol. However UDP proves to be very helpful in multicasting, network management, routing table updates and real - time multimedia. The header formats of TCP, UDP and IP packets are illustrated in Figure1.3, 1.4 and 1.5 respectively. A detailed study on TCP/IP network model and function of each layer is presented in the book on Data communication and Networking by Behrouz A.Forouzan (2006). Similarly, a detailed description on TCP/IP layers and their associated protocols is present in the book titled Computer Networks by Andrew. S.Tanenbaum (2001).
Figure 1.3 TCP Frame Format

Figure 1.4 UDP Header Format

Figure 1.5 IP Header Format
1.4.1.3 TCP / UDP Ports

The study of applications and services incorporated in a network is of prime importance to network operators. The best way to conduct this study is to consider transport layer port numbers. The service port numbers and an ephemeral port number are the two port numbers used by TCP and UDP packets. The service port number or well-known port number is a destination port number encountered in TCP SYN packet which aids in identifying applications. Internet Assigned Numbers Authority (IANA) port assignment catalog is utilized for mapping ports to applications. The port numbers are broadly categorized as: well - known ports (0 - 1023), registered ports (1024 - 49151) and dynamic or private or ephemeral ports (49152 - 65535).

1.4.2 Network Processing and Underlying Functions

The main underlying functions in network processing focus on two planes: the data plane and the control plane. The processing in the data plane focuses on layers 1 and 2, while processing in the control plane focuses on layers 3 and 4. Network processing in the data plane involves analysing and modifying incoming packets, managing an input/output queue, scheduling packets in the queue, and forwarding the packets towards their destination.

The underlying functions in the data plane are:

- Media Access Control (MAC): The term MAC address is often used as a synonym for physical address. Each host and routers in the network have their own physical address. But the physical address is not adequate in networking environment since every network will have its own address format. Hence a universal addressing system is designed in which each host is identified by a unique address, which is called as IP addressing format. Thus the delivery of packet to a host requires
both physical address and IP address. The mapping between an IP address and physical address is done by ARP and RARP protocols.

- Data parsing and classification: It involves classification of packets using a set of rules, based on the packet header information.

- Data transformation: It involves many different operations like changing the content of a packet, modifying the packet when passing through different networks and segmenting, fragmenting and reassembling the packet. These operations differ significantly in complexity. For example, a packet may be encrypted by using some encryption algorithms for security purposes or, a packet may be encapsulated as a payload in a new packet with a new header when packet passes from an IP network to an ATM network.

- Queuing and scheduling: Manages the input and output buffer, make the decision on inserting packets to queues and dequeue packets, and schedule packets for different applications. The packets are scheduled by many different policies and their priorities.

The underlying functions in the control plane are:

- Topology management and network management: It consist of the following operations: monitoring network activity, distributing a database, generating real-time graphical views of the network topology, and updating a dynamic routing table. A routing table is used to forward a packet to the destination or to the next hop. It is updated as soon as there is a change in the network. The routing tables of all the routers on the internet are updated using routing protocols such as Routing Information Protocol (RIP) or the Shortest Path First (OSPF) protocol.
• Signaling: Signaling ensures quality of services since the IP-based network only provides best-effort services. Two groups have proposed signaling standards for IP telephony. The International Telecommunication Union (ITU) has defined a suite of protocols known as H.323 and the Internet Engineering Task Force (IETF) has proposed a signaling protocol known as the Session Initiation Protocol (SIP). Some other signaling protocols, such as Resource Reservation Protocol (RSVP) and Multi-Protocol Label Switching (MPLS) are also utilized in IP networks.

• Policy application: Policy application is a set of rules which are used to execute routing algorithms and to update routing table.

1.4.3 Traffic Flows

The nature of internet traffic can be better understood by knowing the concept of the flow. Flow is the sequence of packets or a packet that belonged to certain network sessions between two hosts but delimited by the setting of flow generation or analysing tool. Alternatively flow can also be defined as a series of packets that share the same source IP, destination IP, source port, destination port and the protocol. This is mostly known as five-tuple IP flow. The most important thing is that all traffic in a flow is unidirectional. Network flow data symbolizes a summary of sessions between two end hosts. It further aids in network analysis and security issues. The flow tool or analyzer is dependent on the amount of information collected from packet headers and its relevant metrics. In addition, the network flow data deeply enhances the visualization of discrete network events such as protocol analysis or length distribution without the need for payload analysis. Further, the knowledge of flow data aids in understanding how different flows compete in a network to acquire network resources. Packets having similar five tuple information belong to the same flow. It is inferred that there is a strong
correlation between the number of flows detected and the length of the timeout value. The number of flows varies inversely with the length of the timeout value. The impact of timeout values is depicted in Figure 1.6.

The flow timeout is an important parameter when defining a flow. It refers to the duration during which flow can be idle before considering it as dead. Thus, a flow timeout value cannot be too short or too long. A short timeout would lead to dissemination of flow into several small flows thereby impacting the workload on the system and a long timeout value may discard several short flows, thereby preventing us from tracking real traffic. Further, an extremely long timeout value prevents a flow from getting expired because of which the numbers of flows keep increasing. Thus in a flow an acceptable flow timeout should be defined in order to overcome misunderstandings in traffic classification and accounting.

![Figure 1.6 Illustration of Flow Timeout](image-url)
1.5 FLOW MEASUREMENT METRICS

In Real time Traffic Flow Measurement (RFTM) architecture, the knowledge of flow attributes and metrics is necessary in proper flow identification, classification and measurement. The flow attributes are derived from endpoint attribute values, metric values like packet and byte counts, time values as well as summary information like mean or average values, jitters and distributional informations. Definitions of the flow attributes are presented in this section.

1.5.1 Path

A sequence of links from a source node S to destination node D is called a (network) path. Also, the nodes connecting the links can be considered to be a part of the path.

1.5.2 Link Capacity

The capacity of a link is the maximum transfer rate possible for that link. The link capacity is defined per protocol layer. This means that the link capacity on layer 2 is different from the link capacity on layer 3 although the physical link is the same. The capacity C of an end-to-end path is the minimum link capacity $C_i$ in the path.

$$ C = \min C_i $$  \hspace{1cm} (1.1)

1.5.3 Delay (Latency)

The term Delay includes processing delay, propagation delay, queuing delay and transmission delay in the telecommunication network. Thus, delay can also be mentioned as end-to-end delay.

$$ D_{E2E} = D_{Processing} + D_{Transmission} + D_{Propagation} + D_{Queuing} $$  \hspace{1cm} (1.2)
1.5.4 Processing Delay

It is the sum of delays caused by all the intermediate nodes on the network path processing the packet. For example, a router examines all the incoming packet headers in order to determine where to direct the packet. It also does some bit-level error checking. All these adds to the delay, caused by the processing.

1.5.5 Transmission Delay (or Serialization Delay)

It is the time taken by the router to send out a packet at the bit rate of the link.

\[ D_{Transmission} = \frac{L}{R} \quad (1.3) \]

Where \( L \) is the length of the packet and \( R \) is the transmission rate of the link.

1.5.6 Propagation Delay

It is the time required for the signal to travel from one end of the transmission medium to the other. The delay depends on the physical medium and thus the delay is the distance between two end-points divided by the propagation speed.

\[ D_{Propagation} = \frac{d}{\eta c} \quad (1.4) \]

Where \( d \) is the distance, \( c \) is the speed of light and \( \eta \leq 1 \).

1.5.7 Queuing Delay

It is the amount of time a packet spends inside routers queue on its way from source node to the destination node. Queuing delay is proportional to the buffer size and the amount of cross-traffic entering the router.

Delay measurements may be one-way or two-way. One-way delay is the end-to-end delay of a packet from the sending host to the receiving host.
Two-way delay (Round trip time RTT) is the delay of a packet from sender to receiver and back.

1.5.8 Packet Delay Variation and Inter Arrival time Variation (Jitter)

The variation of packets one way delay is called Jitter. Instantaneous packet delay variations (PDV) can be calculated from two successive packets one-way delays:

\[ PDV_{\text{instantaneous}} = D_{n+1} - D_n \]  \hspace{1cm} (1.5)

Where \( D_{n+1} \) and \( D_n \) are one-way delays of two consecutive packets.

These delay variations are due to the congestion in the network, routing changes or timing drift. The variation in the time between packets arriving to a host is called packet inter-arrival time variation. It can be calculated from two successive packets arrival time as:

\[ IAT_{\text{instantaneous}} = A_{n+1} - A_n \]  \hspace{1cm} (1.6)

Where \( A_{n+1} \) and \( A_n \) are the arrival times of two consecutive packets.

1.5.9 Throughput

The network throughput is a measure of amount of data transferred across a link or a network in a certain time. Usually throughput is measured in bits per second or bytes per second.

1.5.10 Available Bandwidth

The available bandwidth of a link is the unused capacity of a link at a certain time period. If \( C_i \) is the capacity of a link and \( U_i \) is the average utilization of the link during the time period \( T \), then the available bandwidth for the link is \( A_i \).

\[ A_i = (1 - U_i)C_i \]  \hspace{1cm} (1.7)
Therefore the available bandwidth of a path of N hops is

\[ A = \min_{i=1,2,...,N} A_i \]  

(1.8)

1.5.11 Bulk Transfer Capacity (BTC)

It is the measure of maximum TCP connections obtainable throughput.

\[ BTC = \frac{sent\_databits}{Elapsed\_time} \]  

(1.9)

Where `sent_databits` represents the number of unique data bits sent.

1.5.12 Goodput

The Goodput means the effective throughput experienced by a user and it is also called as an application level throughput.

1.6 OBJECTIVES OF THE THESIS

The work presented in the present thesis belongs to the framework of network flow analysis. The main objectives of the research are as follows:

- To develop a real time network traffic modeling employing probability distribution function.
- To propose hardware architecture for network flow analysis.
- To implement both hashing and decision tree algorithm for flow identification in the proposed architecture.
- To analyze the performance of this proposed architecture against real time traffic patterns generated using probability distribution.
- To compare the performance of the analyser against various link speeds and conclude that the hardware based system supports the growing link speed better than software based systems.
1.7 ORGANIZATION OF THE THESIS

The rest of the thesis is organized as follows. Chapter 2 presents all the existing methodologies in network flow analysis under the title of Background and related works. All different categories of flow analysers are discussed in detail. Also the different varieties of existing packet classification techniques are highlighted while discussing the packet based flow analysis. The various real time traffic modeling schemes and the selection of parameters for different traffic conditions are discussed in Chapter 3. Chapter 4 presents the idea of proposed hardware architecture for network flow analysis and its associated modules. The function of each module related to flow analysis is described clearly. This chapter also covers the concept of technology independent analysis; an analytical discussion on the measurement of maximum operating frequency of the architecture. It also discusses the extent of parallelism that can be included in the architecture. Chapter 5 presents Flow identification scheme employing hashing technique. The performance of the architecture on implementing the new algorithms is studied under various traffic conditions. Chapter 6 discusses the proposed Decision tree algorithm for Flow identification. The performance of the architecture in terms of Flow identification time under different traffic patterns are estimated and compared against the existing techniques. Chapter 7 provides the summary of conclusion for the present research and the scope for the future extension of this work.