Chapter 2

Measurement Classification

2.1 Passive Measurement

With passive measurement we mean the standard approach of tracking the performance and behavior of packet streams by monitoring the traffic passing by the measurement points. The passive approach uses devices to watch the traffic as it passes by, and these devices are special purpose devices such as routers and known host. Thus, to follow the behavior of flows coming from the destination, we have to rely upon sufficient traffic to obtain statistically useful quantities of data. Then the traffic obtained is filtered in different ways to isolate different streams and groups of streams according to criteria such as destination address, protocol or application and it is then polled periodically. Thus information is collected to access network performance and status. Passive measurements at an origin and destination can be combined to form passive end-to-end measurements, and time-stamps on the same packets are compared at each end to capture, as a function of known Origin-Destination pairs and measures loss and delay. For this to be possible time-stamp synchronization and packet identification problems must be solved as well as the logistics of retrieving, comparing and merging of the collected data.
CHAPTER 2. MEASUREMENT CLASSIFICATION

Also, the passive measurement and analysis, provide a better understanding of workload profiles. This in turn allows for better network engineering and the creation of advanced networking technology. Workload measurement requires collecting traffic information from a point within a network where data is collected by the router or switch or by any independent device passively monitoring traffic as it traverses a network link. Network traffic is carried in discrete units called "packets" and they vary in size. Generally packet lengths are given in terms of byte. Collected data allows for a variety of traffic analysis like the packet size distribution, cumulative packet size distribution, and users versus time plots, which includes TCP and UDP users.

It is important to note that as the passive approach uses devices or tools to watch the traffic as it passes by, it does not increase the traffic on the network for the measurement. Therefore it is said that the passive approach measures real traffic. Since the passive approach may require the viewing of all packets on the network, there should be an issue of privacy and security about how to access and protect the data that is gathered. Since the passive measurements depend entirely on the presence of appropriate traffic on the network under study, it has a significant advantage that the data can be prepared without affecting the traffic carried by the network during the period of measurement, but at times difficulty arises in extracting some of the desired information from the available data.

Certain applications of passive monitoring include the followings:

- Identifying, characterizing and tracking, security compromises to one's infrastructure;

- The elasticity of flows and effectiveness in congestion control algorithms;

- The extent to which traffic growth is due to additional users versus an increase in per user traffic;

- Changes in profile of popular protocols and applications and penetration and impact
of emerging technologies and protocols.

Packet header traces can generate an immense amount of data, and, unless the desire is to keep the whole data set, it is usually critical to abstract the data locally as quickly and as thoroughly as possible. However, this process loses information contained in the full traces. Abstractions can occur at a central data collection location, or, if possible, at the location where the data is being collected.

### 2.1.1 Passive Monitoring Tools

Different Tools used in the Internet Measurement are as follows:

<table>
<thead>
<tr>
<th>TYPE</th>
<th>EXAMPLE TOOLS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Icmp-based</td>
<td>pathchar</td>
</tr>
<tr>
<td>Per-hop analysis</td>
<td>ottool</td>
</tr>
<tr>
<td>Throughput</td>
<td>T Reno</td>
</tr>
<tr>
<td>Web availability</td>
<td>tcpdump, libpcap, pcaputure</td>
</tr>
</tbody>
</table>

### 2.2 Active Measurement

By active measurement we mean the injection of artificial probe traffic into the network and the measurement of its characteristics at different points. As the initial structure of the probe traffic is known, and by measuring how it is affected by the portion of the network it traverses, network condition can be inferred. In an active measurement a user sends data to the network, gets the response, and computes the parameters like throughput, packet loss, jitter and latency etc. Also the measurement can take place at both the ends or only at
CHAPTER 2. MEASUREMENT CLASSIFICATION

one end. Active measurement can be divided into three categories depending on how they produce the information of the network structure and state of the network,

1. End-to-end  2. Hop-by-hop  3. link-by-link

- **End-to-end**
  
  It tells about the end-to-end characteristics of the network as shown in Figure 2.1. This is the only measure that is of interest to an end user i.e. total quality of an application. Typical measurements are availability, delay and throughput measurements.

![Figure 2.1: End-to-end measurements](image)

- **Hop-by-hop**
  
  In this we get the state of each hop on the path of the packet. This is shown in Figure 2.2. Tool like Traceroute is used for this purpose, which gives the delay to each node on the path.

- **Link-by-link**
This measurements differs from hop-by-hop measurements in the sense that it tries to characterise the links between the nodes. Details of this methodology are described in studies like [7], [8] and [9]. This is depicted in Figure 2.3.

Most of the tests are based on the ICMP Echo Request and Responses. In Active mea-
CHAPTER 2. MEASUREMENT CLASSIFICATION

Measurement, controlled probe traffic is generated, injected into a network, and measured at a receiving node. This measurement is becoming increasingly important due to its greater flexibility, intrinsically end-to-end nature, and freedom from the need to access core network switching elements. It provides explicit control on the generation of packets for its measurement. This includes control on the nature of traffic generation, the timing frequency packet size, the path and function chosen to be monitored.

2.2.1 Active Monitoring Tools

Different Tools used in the Internet Measurement are as follows:

<table>
<thead>
<tr>
<th>TYPE</th>
<th>EXAMPLE TOOLS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Icmp-based</td>
<td>ping, nikhef, fping, gnuplotping, imeter/lachsis Traceroute, nikhef traceroute, traceroute servers, pathchar</td>
</tr>
<tr>
<td>Throughput</td>
<td>TReno, Bing, b/c probe</td>
</tr>
<tr>
<td>Bulk throughput</td>
<td>netperf, ttcp, nettestc</td>
</tr>
</tbody>
</table>

2.3 Comparison Between Active and Passive Measurements

1. As already defined, Active measurement is the injection of artificial probe traffic into the network, and the measurement of its characteristics at different points, typically back at the origin (round-trip end-to-end measurement), or at some terminating destination (one way end-to-end) where as, Passive measurement is a standard approach of tracking the performance and behavior of packet streams by monitoring the traffic passing by the measurement point.
CHAPTER 2. MEASUREMENT CLASSIFICATION

2. Active measurement methods are used to obtain end-to-end statistics such as latency, loss and availability, whereas passive metrics is pertaining to a certain network element, i.e. at a point metrics such as throughput and packet size statistics.

3. The performance and topology measurements rely on active measurement method to a large extent whereas workloads and routing measurement utilizes passive measurement method.

4. Active measurements rely on sending of test traffic through the network that generates additional load on the network links and routers, which significantly affects the measurement results. In contrast, a passive measurement is based on already existing traffic in the network.

5. In Active measurement test traffic may bother intermediate providers especially if test traffic is not recognizable as such, and it may also lead to additional cost in case of usage based charging while passive method avoids the negative impact of test traffic.