IP Traffic Monitoring: An Overview and Future Considerations †

Dong Wei and Nirwan Ansari

Advanced Networking Lab
Department of Electrical & Computer Engineering
New Jersey Institute of Technology, University Heights
Newark, New Jersey 07102
{dxw3077, nirwan.ansari}@njit.edu

Abstract. An overview on emerging IP traffic monitoring is presented. Important parameters to characterize the traffic, network and QoS, are discussed. The infrastructure and methodology to measure those parameters directly or to compute them based on other measurements are described. We also present a discourse on coping with the challenge of new transport architectures and technologies. In summary, a framework of IP traffic monitoring is presented.

1. Introduction

Rapid growth of the Internet is evidenced by unceasing increased traffic volumes due to new applications and users. Main reasons for the necessity to understand and measure traffic patterns and characteristics are: 1) network optimization and planning, i.e., more efficient usage of the network resources, 2) appropriate provisioning of QoS for all applications, and 3) detection of network security violations. However, Internet traffic is heterogeneous and highly dynamic, and, as a consequence, is difficult to predict. Furthermore, it is also difficult to observe Internet traffic owing to large network size, huge traffic volume, relatively distributed administration, and heterogeneous media. Current understanding of the traffic pattern and measuring methods are rather rudimentary, and further study on IP monitoring becomes increasingly important and urgent as traffic grows exponentially.

This paper presents current state of the art on IP traffic measurement and characterization, and attempts to answer the following questions:

- Why is IP traffic monitoring necessary?
- What parameters can characterize the traffic, the network, and QoS?
- How can these parameters be collected? By measuring directly or computing based on other measurements?
- What kinds of network infrastructures or protocols are needed for these methods?

† This work was supported in part by OpenCon Communication Systems Inc., the New Jersey Commission on Science and Technology via the NJ Wireless Telecommunication Center, and the New Jersey Commission on Higher Education via the NJI-TOEWR project.

- How can these measurements be used to improve the efficient usage of the network resources?
- How can these measurements be employed to provision appropriate QoS for all applications?
- What should be considered to meet the rapid growth of traffic and new technologies, especially with the emergence of traffic engineering technology?

The rest of the paper is organized as follows. Section II presents the background and motivations of IP traffic monitoring. Section III discusses IP traffic pattern, modeling and characteristics. The infrastructures and methods to collect measurements and compute parameters are presented in Section IV. Further discussion on efficient IP traffic measurement is presented in Section V. This paper ends with some concluding remarks in Section VI.

2. Motivations Behind IP Traffic Monitoring

Network traffic measurements and characterizations are needed by ISPs for the following reasons [1]-[5]:

1) To understand macroscopic, infrastructure-wide traffic behavior (from the perspective of the entire network) for network optimization and planning:

- Network design, operation and flow management, i.e., traffic load balance, and efficient resource usage by adapting network configuration to tackle problems such as congestion and so forth.
- Identify and eliminate unnecessary protocols, hence increasing the efficiency of IP networks
- Identify sub-optimal routing
- Billing and pricing

Long-term measurement and optimization as a whole are needed to meet the above requirements.

2) To provision appropriate QoS for each application (from the microscopic perspective, per flow, session, or connection):

Network configuration should be dynamically and autonomously adapted, and resources should be re-allocated to provision appropriate QoS in terms of 1) transmission rate; 2) delay; 3) delay jitter; 4) packet loss rate, and so forth. Real time measurement and control are needed to meet the QoS requirement.

3) Detection of network security violation and abnormalities

This task includes detecting potentially dangerous traffic conditions, pinpointing where and understanding how they are originated, performing designated actions to block the abnormalities, and hence limiting their extension to the entire network.

For different motivations, measurements can be classified as 1) long-term, and 2) real time. They span on different time scales, from months, weeks down to seconds and even milliseconds.

3. IP Traffic Pattern, Modeling and Characteristics

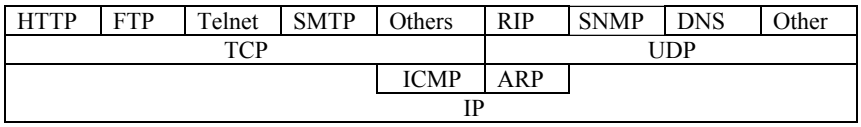

Fig. 1. The Composition of IP Traffic

Fig. 1 shows various protocols in the IP protocol suite [7]. Roberts [8] showed that about 90 to 95% of Internet packets use TCP and correspond to the transfer of digital documents of one form or another (Web pages, data transfer, MP3 tracks, etc.). Thompson, *et al*, showed [9] that:

- Of IP traffic, TCP accounts for 95% or more of bytes, 85-95% packets, and 75-85% of the flows. ICMP packets account for less than 1% of all packets. UDP makes up the remaining IP traffic.
- About 40% of all packets are 40 bytes (TCP ACK, RST and FIN, SYN), 5% of 44 bytes, 5% of 552 bytes, 6% of 576 bytes, 10% of 1500 bytes. 90% of packets are 576 bytes or smaller.

The above data show that TCP packets dominate the IP traffic, and short packets (40 or 44 bytes long) occupy more than half of the IP packets. Thus, the statistical characteristics of TCP packets dominate the statistical characteristics of IP.

According to different QoS requirement, Roberts [8] classified the IP traffic into two categories: 1) elastic flow, where the packets of a document are transferred, requiring zero packet loss rate; and 2) streaming flow, where the packets represent an audio or video signal being transferred, requiring end-to-end delay and delay jitter guarantees.

The development of new Internet applications could change the composition of IP traffic through new protocols or QoS requirement, and thus could change the statistical characteristics of IP traffic. Nevertheless, the study of current IP pattern is still necessary and urgent for both the academic and industry.

Traditionally, analysis of IP traffic is based on two assumptions: 1) the arrival of traffic is independently Poisson distributed; 2) the service time is exponentially distributed. Thus, Markov process can be employed to predict the average performance in terms of queuing delay, packet queue size, and so forth. However, in the past few years, many studies [10]-[15] showed that IP traffics do not follow those two assumptions and show self-similarity in different time scales. There are two important characteristics with IP traffic: burstiness and long-dependency, i.e., packets come in burst and the autocorrelation of traffic can span a large time scale. It is tempting to think that the aggregation of IP traffics should be Gaussian distributed, and the burstiness could be smoothed by aggregation, but on the contrary, reference [10] and [12] demonstrated by experiments that the aggregation of IP traffic can intensify burstiness.

Paxson and Floyd [11] showed that, in conventional Markov process, self-similarity in a network is ignored, the burstiness of traffic is underestimated, and the performance is overestimated. As a consequence, resource allocation based on

Markov assumption is inadequate, resulting in the unexpected bigger delay, bigger queue size, and higher packet loss rate.

Many studies showed the existence of self-similarity in IP traffic. However, no model can provide both qualitative insights and quantitative predictions on the performance of IP networks so far.

In order to simulate IP traffic, three most widely used methods to generate self-similar traffic are:

- Pareto distribution [11]
- Fractional Brownian motion [16][17]
- ON-OFF sources [10][18]

Hurst parameter ***H*** is the parameter to characterize a self-similar random process. Gomez and Santonja [19] enumerated three methods to estimate ***H***:

- R/S analysis
- Variance-time plot
- Periodogram-based analysis (wavelet, energy-scale index relation)

In order to provide qualitative insights of traffic and network, the following parameters need to be collected and analyzed:

1) Parameters to characterize IP traffic patterns:

- Primary data that can be collected
  - Packet arrival rate
  - Packet inter-arrival time
  - Packet length distribution
  - Link lifetime
- Statistical data
  - Mean
  - Peak
  - Burstiness (standard deviation)
  - Self-similarity (Hurst parameter ***H***)

2) Parameters to characterize networks (not only in Internet):

- Utilization and throughput
- Quiescence (indicates the occupancy of a link) [6]
- Unpredictability (indicates the stability and consistency of a link) [6]
- Responsiveness to the change of IP traffic
- Routing stability
- Reliability (ability to pinpoint some anomalous traffic conditions and block them)
- Granularity

3) Parameters to characterize the QoS of a link:

- End-to-end delay
- Delay jitter
- Packet loss rate
- Round trip time (RTT)

IPPM (IP Performance Metrics) working group of IETF has developed some metrics of quantities to characterize the performance and reliability of the Internet [22].

4. The Infrastructure and Methodology of IP Traffic Measurement

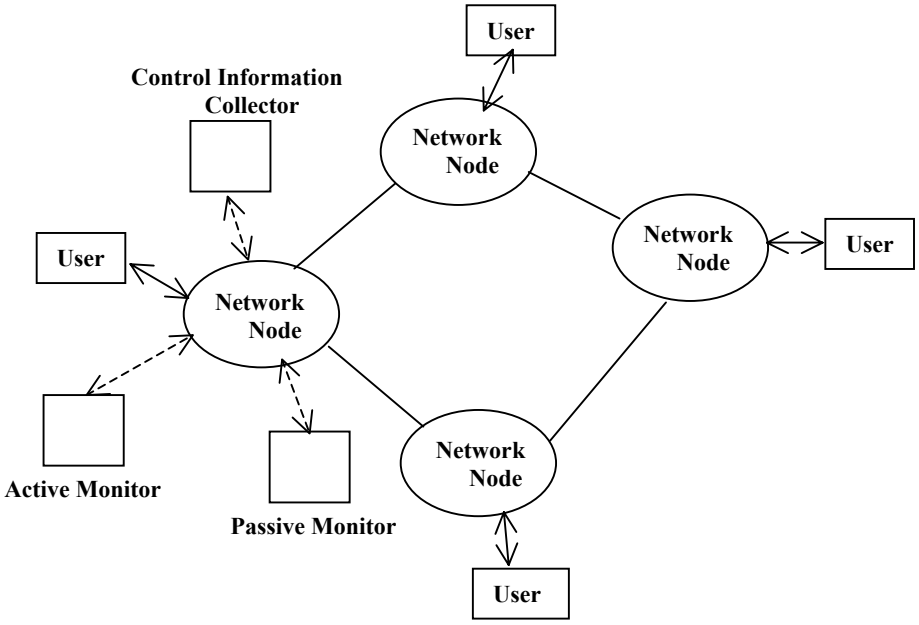

Fig. 2. Infrastructure of IP Traffic Measurement

Some parameters, such as delay jitter and H, are not observable directly. These parameters could be calculated from other measurements.

There are three methods of collecting data of network behavior [1][5]:

- Passive measurement: a probe, which resides at the import of a network node, and records network activities, is inserted into this node. Most commonly, the probe is attached to a link between network nodes, and summarizes and records information about the traffic flowing on that link.
- Active measurement: the behavior of the network is studied by sending data (usually a probing packet, from end to end) through the network and observing the results, including the time taken to send the data. Internet Control Message Protocol (ICMP) and IP Measurement Protocol can be used here.
- Control information monitoring: network control information such as routing or network management information (SNMP derived data and BGP router-based data) is captured and analyzed.

These three approaches focus on different perspectives of network behavior, and each method has its advantages and disadvantages. All of them are often employed together to develop an understanding of the entire network's behavior.

Passive measurement, which is also called per-hop measurement, observes the behavior of a network at a specific point; it does not add to or modify the data carried by the network. Consequently, it has no impact on the behavior of the network. A

very detailed understanding of the behavior at the point of measurement can be developed, but it is difficult to gain an understanding of the network as a whole, or the end-to-end behavior of the network. Passive measurement is often used to measure traffic patterns, such as packet arrival rate, link lifetime, etc.

Since active measurement, which is also called end-to-end measurement, observes network behavior by sending probing packets (usually ICMP packets) into the network, it lends itself to measuring parameters that reflect the service the network is offering to its users, including parameters like round-trip time (RTT) and packet loss. However, the traffic added to the network may alter the behavior of the network. Furthermore, if ICMP is used, ISPs could turn off ICMP traffic at selected routers to limit the visibility of their infrastructure. Owing to the general-purpose nature, ICMP has some weaknesses as a measurement protocol. The most important downside is that it can be blocked by ISPs. NLANR (National Laboratory for Applied Network Research) has developed a new protocol – IP Measurement Protocol (IPMP) [20], which is tailored for active measurement and has many features that make it easier to process.

Monitoring the control information of the network provides a ready source of information about those aspects of network behavior described by data transferred as part of the normal network operation. Remote monitoring agent (RMON) [4] employs this approach to configure and instrument SNMP properly and analyze collected data. The RMON MIB Working Group of IETF [21] is chartered to define a set of managed objects for remote network monitoring. Parameters such as link utilization or route stability may be collected this way. However, it is difficult to monitor the control information when the network size is large.

To provision appropriate QoS, traffic pattern should be measured, bandwidth and buffer are reserved accordingly; network status should be monitored to avoid congestion and to balance traffic load to improve the throughput of the entire network.

5. Further Considerations On IP Traffic Monitoring

Owing to the increased need for Internet usage and demand for provisioning quality of service, IP traffic engineering technologies become monumentally important, and thus traffic-engineering-oriented measurement is required. In order to develop general and operational measurement infrastructure and methodology, the following issues should be considered [23]-[26]:

1) Protocol-independent and traffic engineering aware measurements - an IP link can be arbitrarily specific, e.g., via MPLS or DiffServ, and thus IP links have many varieties, supported by different protocols. An efficient measurement should be designed for generic IP traffic, which is independent of protocols and portable across different platforms. Furthermore, the measurement should be traffic engineering aware too. For example, in DiffServ, many packets may pass the same path (from end to end), but they may have different classes of service (CoS), different priority queues, and thus different delay, etc. The measurement methodology should be aware of these classes of service, and collect and analyze data accordingly.

2) Scalability – a measurement infrastructure must be able to scale with the size and speed of a network as it evolves.
3) Timing optimization and orthogonality of collected data – minimize the amount of data to be collected without compromising the necessary accuracy, thus preventing network performance from being adversely affected by unnecessarily loading of processors, memories, transmission facilities and the administrative support systems.
4) Feedback mechanism for topology state – in order to provision appropriate QoS, constraint-based routing measurement is employed, in which all network nodes require topology state information, such as link availability and maximum resource, etc. However, the information could fluctuate immediately while it is distributed in the network. To acquire accurate topology state information, a feedback mechanism can be employed by traversing the IP link.
5) Security – ensure correctness and reliability of the measurements.
6) Active measurements that are less invasive and do not provoke ISPs to block them.
7) Aggregating, mining, and visualizing the massive data sets in ways that are useful to multiple users
8) Traffic prediction based on measurements and modeling – by capturing the statistical nature of traffic from previous measurements, resources can be re-allocated and network can be re-configured accordingly by predicting the subsequent traffic, such that the performance in terms of efficiency and QoS can be improved.
9) Optical consideration – optical network is going to play a major role in the Internet. It is imminent to develop IP traffic monitoring over optical channels and labels. This is an emerging research.

6. Conclusions

With the development of traffic engineering technologies, IP traffic monitoring can have a wide range of influence on network performance. The current infrastructure and methodology of IP traffic monitoring cannot meet the demand for provisioning appropriate QoS for IP applications. Some issues, which need to be considered when the new infrastructure and methodology of IP traffic monitoring are developed, have been discussed in this paper.

References

1. K.C. Claffy, “Measuring the Internet,” *IEEE Internet Computing*, vol.4, no.1, Jan.-Feb. 2000, pp. 73 – 75.
2. A. Adams, *et al*, “The Use of End-to-End Multicast Measurements for Characterizing Internal Network Behavior,” *IEEE Communications Magazine*, vol.38, no.5, May 2000, pp.152-158.
3. R. Caceres, *et al*, “Measurement and Analysis of IP Network Usage and Behavior,” *IEEE Communications Magazine*, vol.38, no.5, May 2000, pp.144-151.

4. Luca Deri, Stefano Suin, “Effective Traffic Measurement Using ntop,” *IEEE Communications Magazine*, vol.38, no.5, May 2000, pp.138-143.
5. T. McGregor, H. Braun, J. Brown, “The NLANR Network Analysis Infrastructure,” *IEEE Communications Magazine*, vol.38, no.5, May 2000, pp.122-128.
6. W. Matthews, Les Cottrell, “The PingER Project: Active Internet Performance Monitoring for the HENP Community,” *IEEE Communications Magazine*, vol.38, no.5, May 2000, pp.130-136.
7. Gil Held, *Voice & Data Internetworking*, McGraw-Hill, 1998, pp.35.
8. Jim W. Roberts, “Traffic Theory and The Internet,” *IEEE Communications Magazine*, vol.39, no.1, Jan. 2001, pp.94-99.
9. Thompson, K.; Miller, G.J.; Wilder, R., “Wide-area Internet traffic patterns and characteristics**,**” *IEEE Network*, vol.11, no.6, Nov.-Dec.1997, pp. 10 –23.
10. W.E. Leland, W. Willinger, *et al,* “On the self-similar nature of Ethernet traffic (Extended Version),” *IEEE/ACM Transaction on Networking*, vol.2, no.1, Feb.1994, pp. 1-15.
11. V. Paxson and Sally Floyd, “Wide Area Traffic: The Failure of Poisson Modeling,” *IEEE/ACM Transaction on Networking*, vol.3, no.3, June 1995, pp.226-244.
12. W. Willinger et al, “Self-Similarity Through High-Variability: Statistical Analysis of Ethernet LAN Traffic at the Source Level,” *IEEE/ACM Transaction on Networking*, vol.5, no.1, Feb.1997, pp.71-86.
13. J. Beran, R. Sherman, M.S. Taqqu, W. Willinger, “Long-Range Dependence in Variable-Bit-Rate Video Traffic,” *IEEE/ACM Transaction on Communications*, vol.43, no.2, Feb.-March-April 1995, pp. 1566-1579.
14. M. Crovella and A.Bestavros, “Self-Similarity in World Wide Web Traffic: Evidence and Possible Causes,” *IEEE/ACM Transaction on Networking*, vol.5, no.6, June 1997, pp. 835-846.
15. B. Tsybakov and N. Georganas, “Self-Similar Processes in Communications Network,” *IEEE Transaction on Information Theory*, vol.44, no.5, Sep.1998, pp.1713-1725.
16. W. Willinger *et al*, “Self-Similar Traffic Generation: The Random Midpoint Displacement Algorithm and Its Properties,” *1995 IEEE International Conference on Communications*, vol. 1, pp. 466-472.
17. F. Chen, *et al*, “A Hybrid Approach for Generating Fractional Brownian Motion,” GLOBECOM '96, Communications, vol.1, pp. 591–595.
18. P. Pruthi and A. Erramilli, “Heavy-Tailed ON/OFF Source Behavior and Self-Similar Traffic,” *ICC '95 Seattle*, vol. 1, pp.445–450.
19. M.E. Gomez and V. Santonja, “Self-Similarity in I/O Workload: Analysis and Modeling,” *Workload Characterization: Methodology and Case Studies*, 1999, pp. 97-104.
20. http://www.nlanr.net/ActMon/IPMP/
21. http://www.ietf.org/html.charters/rmonmib-charter.html
22. Paxson V., Almes G., Mahdavi J., Mathis M., "Framework for IP Performance Metrics," http://www.ietf.org/rfc/rfc2330.txt
23. Christian B., Davies B., Tse, H., "Operational measurements for Traffic Engineering," http://search.ietf.org/internet-drafts/draft-christian-tewg-measurement-00.txt
24. Lai W.S., "A Framework for Internet Traffic Measurement," http://www.ietf.org/internet-drafts/draft-wlai-tewg-measure-00.txt
25. Awduche, Elwalid, Widjaja, Xiao, "A Framework for Internet Traffic Engineering," http://search.ietf.org/internet-drafts/draft-ietf-tewg-framework-02.txt
26. Van den Berghe S., Vanheuven P., Demeester P., Asgari H., "Some Issues for Designing a Measurement Architecture for Traffic Engineered IP Networks," http://search.ietf.org/internet-drafts/draft-svdberg-temon-00.txt