A Network Monitoring System for High Speed Network Traffic

Barış Kurt[1], Engin Zeydan[2], Utku Yabas[2], Ilyas Alper Karatepe[2], Güneş Karabulut Kurt[3], and Ali Taylan Cemgil [1]

[1]Department of Computer Engineering, Bogazici University, Istanbul, Turkey.
[2]Türk Telekom Labs, Istanbul, Turkey.
[3]Department of Electronics and Communication Engineering, Istanbul Technical University, Istanbul, Turkey.

***Abstract*—Monitoring network statistics is important for the maintenance and infrastructure planning for the network service providers. In this demonstration, we will showcase an initial analysis of a general purpose network monitoring platform for high speed mobile networks. The developed platform is the basis for performing complex real-time analysis such as application usage behaviour, security analysis, infrastructure planning. We have used the platform for real-time flow size and length monitoring with packet sampling.**

***Keywords*—Network monitoring, mobile operators, visualization, real-time**

I. Introduction

Passive monitoring, where the measuring beacons inactively watch the traffic passing by [1] is an important method for collecting packet and flow level statistical information in communication networks. Such information helps a service provider to characterize its network resource usage and user behavior, infer future traffic demands, detect traffic/usage anomalies, and possibly provide insights to improve the performance of the network [2].

We designed a passive network monitoring infrastructure to provide packet and flow level information for possible higher-level applications such as security monitors, application classifiers, billing systems, etc. The system is implemented on a Commercial-off-the-shelf (COTS) hardware. For demonstration, we used this infrastructure to monitor and visualize the flow size distribution on the network in real time.

II. Network Monitoring System

The system is designed as a client-server model, with two main components: *Monitor Server* and *Monitor Client* as shown in Figure 1. The monitor server captures the traffic between the Serving GPRS Support Node (SGSN) and the Gateway GPRS Support Node (GGSN) network modules and is responsible for processing packets and collecting network statistics. The monitoring client, which is a simple thin client designed as web a application, is used by system administrators to control the monitor server, and fetch and visualize collected statistics.

[1] baris.kurt@boun.edu.tr
[2] engin.zeydan@turktelekom.com.tr
[2] utku.yabas@turktelekom.com.tr
[2] IlyasAlper.Karatepe@turktelekom.com.tr
[3] gkurt@itu.edu.tr
[1] taylan.cemgil@boun.edu.tr

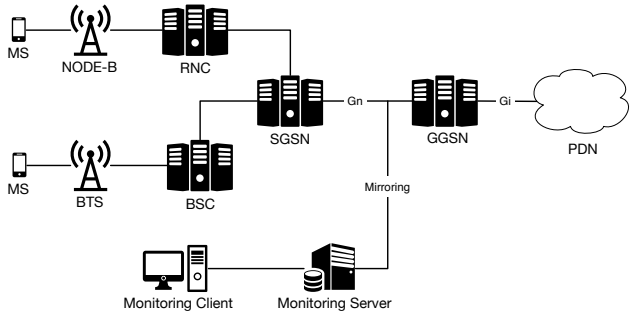

Fig. 1: Physical implementation of the monitoring system.

A. Monitor Server

The server listens to the Ethernet link on which the Gn [1] interface is mirrored. The fundamental data objects in the system are network packets and network flows. The monitor server is composed of network analyzer and server manager sub-modules as shown in Figure 2.

The network analyzer sub-module is responsible for capturing and processing the network packets and extracting packet and flow level statistics. The module includes a ring buffer to prevent packet drop and is capable of doing packet sampling, i.e. selecting a subset of incoming packets for processing due to a sampling scheme such as random, periodic or interval [1].

A monitor manager sub-module, which is implemented as a web application that runs on Tomcat 7 server, is an interface between the Monitor Client and the Monitor Server. The manager receives requests and configuration parameters from the user and runs the network manager accordingly. The manager redirects the statistics collected by the network analyzer to the monitor client and/or a MySQL database stored on a Hadoop Distributed File System (HDFS).

B. Monitor Client

The monitor client is used for sending user requests to the monitor server and real-time and offline visualization of the packet and flow statistics. The user can request both real-time and past network statistics by selecting the time interval that they want to inspect. After the user request is sent, the client listens to the Web Socket 9001 for network statistics in

[1]Gn is an interface between SGSN and GGSN where GPRS Tunneling Protocol (GTP) is the main protocol for network packets flowing through.

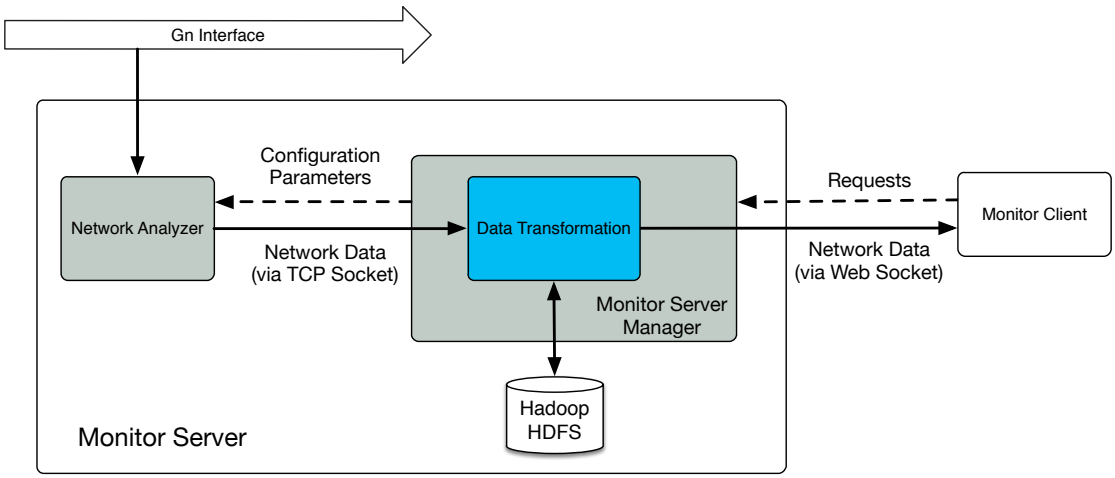

Fig. 2: Flow Size Distribution Architecture Design

JavaScript Object Notation (JSON) format. JavaServer Pages (JSP) files are used for web pages and dynamic charts are implemented with JavaScript. The *HighCharts* Javascript library is used for the implementation of dynamic charts [3].

C. Hardware and Software Specifications

The monitor server runs on a stand alone machine that has 8 64 bit Intel(R) Xeon(R) CPU, E5540, @ 2.53GHz, with 8192 KB cache size processors, 8GB DDR2 RAM, and 2TB hard disk. Monitor clients run on our personal devices with Google Chrome(R) web browser installed.

The monitor server software is written in C++ using the C++11 standard library containers and the open source *libpcap* [4] network packet capture library. The server software runs on Red Hat Enterprise Linux Server release 7.

III. Sample Application: Flow Size Distribution Monitoring

A network flow is defined as a collection of Internet Protocol (IP) packets with the same signature i.e. IP and port source and destination pairs together with level-3 protocol type, traveling bidirectionally in the network. A flow information, such as the number of packets and bytes, is a good summary of the transaction between communicating pairs. The distribution of the flow sizes and volumes are important statistics that helps network service providers detect network anomalies, infrastructure planning and accounting. We have used our monitoring system to track the network flow size and length distributions in real-time. Since the brute force collection of the flow statistics on COTS hardware is not possible in high speed networks [5], we employed packet sampling and recovered the flow statistics via maximum likelihood estimation as described in [6] and [7].

In this application, the network analyzer sub-module in the server selects packets randomly according to the sampling rate adjusted by the user through the monitor client. A flow record table is maintained and updated for each processed packet. In order to terminate the flows, the record table has a time-out mechanism that deletes the flows that does not receive a new packet for the last 30 seconds. In every 5 seconds, the sampled distribution of the flow size and lengths are processed and estimations of the true distributions are calculated and sent to the monitor client. The client visualizes the distributions as shown in Figure 3. Offline visualization of the flow trends in last 24 hours is shown in Figure 4.

IV. Conclusions and Discussions

In this demo, we show the design the implementation of a network monitoring system for mobile providers that provides a network statistics for the higher-level data-driven network applications. The system monitors the Gn interface between SGSN and GGSN of cellular network, on which mobile operator's real time network traffic is flowing, and visualizes real time network statistics through a visualization dashboard in client side. As an example application, we have employed the system for estimating the flow size and length distributions via packet sampling.

Acknowledgments

This work has been performed in the framework of TÜBİTAK TEYDEB (project no 3130726) project.

References

[1] N. Duffield, "Sampling for passive internet measurement: A review," *Statistical Science*, vol. 19, no. 3, pp. 472–498, 2004.

[2] G. Varghese and C. Estan, "The measurement manifesto," *SIGCOMM Comput. Commun. Rev.*, vol. 34, no. 1, pp. 9–14, 2004.

[3] "Highcharts: Interactive JavaScript charts for your webpage." http://www.highcharts.com/, 2016. [Online; accessed 24-April-2016].

[4] "Libpcap." http://www.tcpdump.org/, 2016. [Online; accessed 24-April-2016].

[5] F. Fusco and L. Deri, "High speed network traffic analysis with commodity multi-core systems," in *Proceedings of the 10th ACM SIGCOMM Conference on Internet Measurement*, IMC '10, (New York, NY, USA), pp. 218–224, ACM, 2010.

[6] N. Duffield, C. Lund, and M. Thorup, "Estimating flow distributions from sampled flow statistics," *IEEE/ACM Transactions on Networking*, vol. 13, no. 5, pp. 933–946, 2005.

[7] L. Yang and G. Michailidis, "Sampled based estimation of network traffic flow characteristics," in *INFOCOM 2007, 26th IEEE International Conference on Computer Communications*, pp. 1775–1783, May 2007.

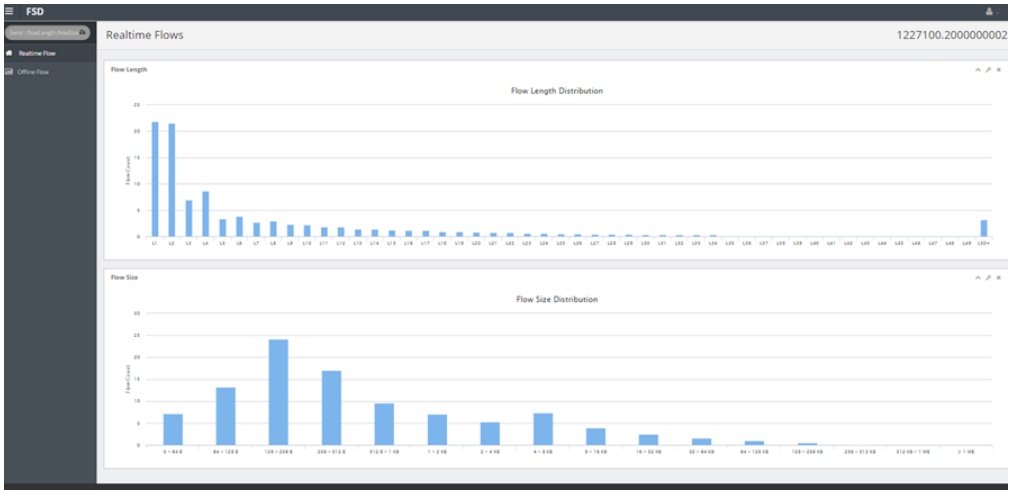

Fig. 3: Dashboard for visualizing flow size and length distributions of mobile operator's high speed traffic over Gn interface. Flow length distribution is shown at the top panel. The bottom panel shows the flow size distribution.

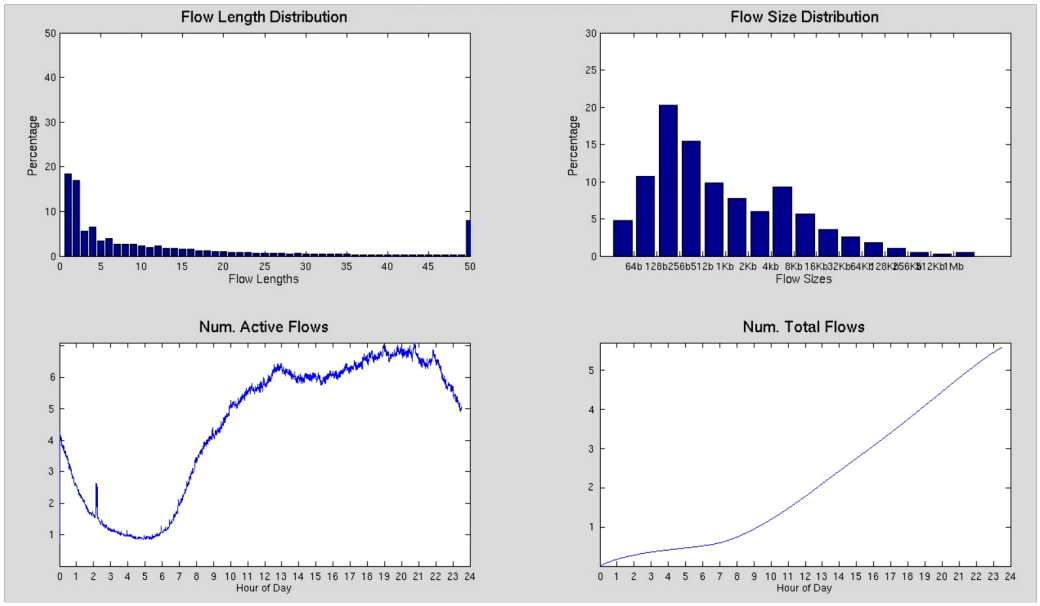

Fig. 4: Monitoring summary for 24 hour data. Top panels show the flow size and length distributions of the active flows, and the bottom panels shows the trend in the number of active flows.