Indian Institute of Technology Roorkee

Department of Computer Science and Engineering

CSN-361: Computer Networks Laboratory (Autumn 2019-2020)

Lab Assignment-9 (L9) **Date: October 3, 2019** **Duration: 2 Weeks**

General Instructions:

1. Every Lab Assignment will be performed by the students individually**.** No group formation is required and the evaluations will be done every week for the students individually**.**

Submission and Evaluation Instructions:

1. **Submit your** zipped folder (**<filename>.zip** or **<filename>.tar.gz**) through your account in Moodle through the submission link for this Lab Assignment in Moodle course site: https://moodle.iitr.ac.in/course/view.php?id=47
2. **Hard deadline for Final submission in Moodle: October 17, 2019 (9:00 am Indian Time).** For any submission after Final Deadline, 20% marks will be deducted (irrespective of it is delayed by a few seconds or a few days). The key to success is starting early. You can always take a break, if you finish early.
3. The submitted zipped folder (**<filename>.zip** or **<filename>.tar.gz**) must contain the following:
   (a) The source code files in a folder.
   (b) A report file (**<filename>.DOC** or **<filename>.PDF**) should contain the details like:
      i. Title page with details of the student
      ii. Problem statements
      iii. Answer of each problem statement with the snapshots of the obtained results from the Wireshark trace file.
4. The submission by each student will be checked with others' submission to identify any copy case (using such detection software). If we detect that the code submitted by a student is a copy (partially or fully) of other's code, then the total marks obtained by one student will be divided by the total number of students sharing the same code.

Instructions for L9:

1. Objective of this Lab Assignment is to make the students familiar with the hardware and software aspects of computer networking and extracting information related to computer networking using Wireshark.
2. The student will have to demonstrate and explain the coding done for this Lab Assignment in the next laboratory class to be held on **October 17, 2019** for evaluation**.**

Problem Statement 1:

Install **Wireshark** and explore its uses to capture network traffic. You have to capture normal internet traffic for 20-30 minutes from your system using Wireshark.
You need to copy this data in CSV / TXT file.

Problem Statement 2:

Take the CSV / TXT, which is generated in Problem Statement 1 as an input. Write a code (in any programming language of your choice) to extract the following 11 features given below in the table:

Average Packet Size	Average Flow Duration
Average no of Packets Sent per Flow	Average no of Packets Received per Flow
Average amount of Bytes Sent per Flow	Average amount of Bytes Received per Flow
Average Ratio of Incoming to Outgoing Packets	Average Ratio of Incoming to Outgoing Bytes
Average Time Interval b/w Packets Sent	Average Time Interval b/w Packets Received
Average Ratio of Connections to Number of Destination IPs	

Problem Statement 3:

In this problem, the behavior of TCP protocol will be studied using Wireshark. For this assignment download the Wireshark captured trace file named as ***tcpethe-trace*** from Piazza, which is a packet trace of TCP transfer of a file from a client system to a remote server (named as *ser1*), obtained by running Wireshark on the client machine. Open ***tcpethe-trace*** file in Wireshark and answer the following question:

a. What is the IP address and TCP port number used by the client computer (source) that is transferring the file to server (*ser1)*?

b. What is the IP address of server (*ser1*)? On what port number it is sending and receiving the TCP segments for this connection?

c. What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client computer and *ser1*? What is it in the segment that identifies the segment as a SYN segment?

d. What is the sequence number of the SYNACK segment sent by ser1 to the client computer in reply to the SYN? What is the value of the Acknowledgement field in the SYNACK segment? How did ser1 determine that value? What is it in the segment that identifies the segment as a SYNACK segment?

e. What is the sequence number of the TCP segment containing the HTTP POST command? Note that in order to find the POST command; you'll need to dig into the packet content field at the bottom of the Wireshark window, looking for a segment with a "POST" within its DATA field.

f. Consider the TCP segment containing the HTTP POST as the first segment in the TCP connection. What are the sequence numbers of the first six segments in the TCP connection (including the segment containing the HTTP POST)? At what time was each segment sent? When was the ACK for each segment received? Given the difference between when each TCP segment was sent, and when its acknowledgement was received, what is the Round Trip Time (RTT) value for each of the six segments? What is the Estimated RTT value after the receipt of each ACK? Assume that the value of the Estimated RTT is equal to the measured RTT for the first segment, and then is computed using the following Estimated RTT equation for all subsequent segments.

Estimated RTT = (1 – α) * Estimated RTT + α * SampleRTT

where, the new value of Estimated RTT is a weighted combination of the previous value of Estimated RTT and the new value for SampleRTT. The recommended value of $\alpha = 0.125$.

> Note: Wireshark has a nice feature that allows you to plot the RTT for each of the TCP segments sent. Select a TCP segment in the "listing of captured packets" window that is being sent from the client to the ser1 server. Then select: Statistics→TCP Stream Graph→Round Trip Time Graph.

g. What is the length of each of the first six TCP segments?

h. What is the minimum amount of available buffer space advertised at the received for the entire trace? Does the lack of receiver buffer space ever throttle the sender?

i. What is the throughput (bytes transferred per unit time) for the TCP connection? Explain how you calculated this value.