Programming Assignment 3: TCP and Wireshark
CSE 310, Spring 2019
Instructor: Aruna Balasubramanian
Due date: April 15 2010, 9.00pm

The goal of this assignment is to dissect the TCP protocol using the Wireshark tool. To do this, you should be familiar with the packet formats, PCAP files, TCPDump, and Wireshark. Briefly, TCPdump/Wireshark are both tools to capture packets going on the wire. When you exchange packets between A and B, Wireshark/TCPDump will let you capture the packets that are being sent out and received at the node. PCAP is the file format used to store the captured packets. PCAP library is a library that you can use to parse the packet capture.

Part A Wireshark Programming Task (70 points)
Your task is to write a program `` analysis_pcap_tcp" that analyzes a Wireshark/TCPdump trace to characterize the TCP flows in the trace. A TCP flow starts with a TCP "SYN" and ends at a TCP "FIN".

You may use a PCAP library to analyze the trace. You may only use the PCAP library to get each packet in byte format. The PCAP library can be used to figure out where the first packet ends and the second packet starts. You need to then write code to analyze the bytes to get the information about the packet.

[Hint: You can create your own packet structures and read the bytes into the structure. However, you cannot convert the PCAP file into text and perform the analysis. This is important because the main goal of this homework is to learn how to parse network packets.]

Attached to the homework is a file assignment3.pcap. In this file, we have captured packets sent between 130.245.145.12 and 128.208.2.198. Node 130.245.145.12 establishes the connection (let's call it sender) with 128.208.2.198 (let's call is receiver) and then sends data. The trace was captured at the sender. Use your `` analysis_pcap_tcp" code to analyze assignment3.pcap and answer the following questions (Ignore any traffic that is not TCP). Each of these needs to be done empirically:

1. Count the number of TCP flows initiated from the sender
2. For each TCP flow

(a) For the first 2 transactions after the TCP connection is set up (from sender to receiver), get the values of the Sequence number, Ack number, and Receive Window size. Explain these values.

(b) Compute the sender throughput for data sent from sender to receiver. The throughput is the total amount of data sent by the sender over the period of time. The period is the time between sending the first byte to receiving the last acknowledgement.

(c) Compute the loss rate for each flow. Loss rate is the number of packets not received divided by the number of packets sent. Loss rate is an application layer metric.

Submit (i) the high level summary of the analysis_pcap_tcp code, (ii) the analysis_pcap_tcp program, and (iii) the answers to each question and a brief note about how you estimated each value, (iv) instructions on how to run your code

Part B Congestion control (30 points)

Using the same assignment2.pcap file and your analysis_pcap_tcp program, answer the following questions about congestion control

For each TCP flow:

(1) Print the first five congestion window sizes (or till the end of the flow, if there are less than five congestion windows). The congestion window is estimated at the sender. What is the size of the initial congestion window. You need to estimate the congestion window size empirically since the information is not available in the packet. Comment on how the congestion window size grows. Remember that your estimation may not be perfect, but that is ok. Congestion window sizes are estimated per RTT.

(2) Compute the number of times a retransmission occurred due to triple duplicate ack and the number of time a retransmission occurred due to timeout.

Submit (i) the answers to each question and a brief note about how you estimated each value, (ii) the program if any you used to answer the two questions.

Submission instruction

As before, you may write your programs in the following languages: Python, Java, and C/C++. If you want to write in any other language, please talk to me. Note that viewing these traces on Wireshark is helpful but you need to use the pcap library.

You need to submit your homework in a single zip file as follows:

- The zip file and (the root folder inside) should be named using your last name, first name, and the assignment numner, all separated by a dash ('-') e.g. lastname-firstname-assignment3.zip
- The zip file should contain all submissions for parts A and B.

Some example pcap libraries that you can use:
C/C++ - libpcap
Java - jnetpcap
Python - dpkt