Lab 4 Analyzing TCP

In this lab, we'll investigate the behavior of the TCP protocol in detail.

Generate the Trace File

- Go to http://gaia.cs.umass.edu/wireshark-labs/alice.txt and download a text file titled "Alice in Wonderland", and store it on your computer.
- Go to http://gaia.cs.umass.edu/wireshark-labs/TCP-wireshark-file1.html.
- Use *Browse* button to select the alice.txt file you just downloaded but don't yet press the "*Upload alice.txt file*" button.
- Start up Wireshark and begin packet capturing.
- Returning to browser, press the "*Upload alice.txt file*" button to upload the file to gaia.cs.umass.edu.
- Once the file was uploaded, stop Wireshark packet capture.

Answer Questions via Analyzing Trace File

Answer the following questions by analyzing the trace file you just captured. If you are using desktops in EPS 254, please open/import the trace file (*tcp-trace.pcap*) provided on D2L. While you are answering the questions, please highlight the records from which you get your answers, and take screenshots of the WireShark window. These screenshots should be inserted into your solution file, right before the answer of each question.

1. What is the IP address and TCP port number used by the client (sender) that is transferring the file to gaia.cs.umass.edu?
2. What is the IP address of the receiver, gaia.cs.umass.edu? On what port number is it sending and receiving TCP segments for this connection?
3. What is the sequence number of the TCP SYN segment that is used to build a TCP connection between the client computer and gaia.cs.umass.edu? Which field(s) in this segment is used to indicate that the segment is a SYN segment?
4. What is the sequence number of the SYNACK segment sent from gaia.cs.umass.edu? What is the value of the Acknowledgement field in the SYNACK segment? How did the server determine that value? Which field(s) in this segment is used to indicate that the segment is a SYNACK segment?
5. What is the sequence number of the TCP segment containing the HTTP POST command? [Hint: You need to look into DATA field]
6. Assume the TCP segment containing the HTTP POST as the first segment in this TCP connection. What are the sequence numbers of the first six segments in the TCP connection, including the segment containing the HTTP POST? When was each segment sent? When was the ACK of each segment received? What is the RTT value for each of the six segments?
7. What is the `EstimatedRTT` value after the receipt of each ACK? Assume that the value of the `EstimatedRTT` is computed from the following equation:

$$EstimatedRTT = 0.875 * EstimatedRTT + 0.125\ SampleRTT$$

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

9. What is the minimum available buffer space advertised at the receiver (server) in this connection?

10. Are there any retransmitted segments in the trace file? Justify your answer.

11. How much data does the receiver typically acknowledge in an ACK? Can you identify cases where the receiver is acknowledging every other received segment?

12. What is the throughput (bytes/sec) for the TCP connection? Justify your answer.