CO323 - Lab 6
E17219 : K.G.I.S. Nawarathna
Investigating TCP communication using Time-Sequence Diagrams

---

1) We will first upload a file to the Aiken/Tesla server via a TCP connection and observe the network traffic.

a) Follow these steps:

i) Use only the given Zoom installer file (~15MB).

ii) Open Wireshark on your computer and start capturing outgoing packets.

iii) Open a terminal and copy the given Zoom installer file to the Aiken/Tesla server via SSH. (Hint: Look into the `scp` command).

iv) Wait until the upload finishes and stop the Wireshark capture.

v) Apply a filter as necessary to filter only the TCP packets from source to destination.

vi) Obtain the TCP Time-Sequence (Stevens) graph for the TCP communication from YOUR_IP to Aiken/Tesla Server_IP and take a screenshot. (Hint: Look into Wireshark statistics). Note: Make sure the graph is for YOUR_IP => Server_IP, not the other way around.

b) What do you see at the beginning of the TCP Sequence-Time graph when you start transferring data? Explain briefly.

-At first, from the 0 th second up until the 4.5 second the graph tends to be flatten out. There are a few packets sent during this time period here. But after 4.5 seconds the initial number tends to increase as normal.

c) What is the reason for the behavior you observed in part b?

-This has happened due to a few reasons.

1.As the first step , the sender needs to identify the ip address of the receiver. To do this, it uses DNS protocols and this will take a noticeable time. Until that process is done, the file can not be uploaded to the system.

2.After getting the ip address of the destination, the sender needs to establish the tcp connection with the server. To do that, it uses the three way handshake. In the wireshark packet tracing list, SYN, SYN/ACK and ACK packets can be identified clearly.

3.After making the connection , the server needs to authorize the user. For this task , the user is prompted to enter his/her password. For these tasks it would take some time as well. After that, the packets corresponding to this authorization such as Key exchange init will be used.

-Because of the reasons mentioned above, the first few seconds of the graph would tend to flatten out in the first period of the transmission.

d) Obtain the Time-Sequence (TCP trace). Do you see red lines in that? Explain what happens by comparing those with the graph you obtained for Time-sequence (Stevens) graph.

-There are three colored lines in the graph.

1.blue:data line
2.green:receive window of the receiver
3.red:ACKED packets

- The data line represents the data sent by the sender to the receiver. These lines must always stay below the data green line. Because the green line represents the receiving window of the receiver and the receiving window must always greater that data sending.(in flight packets) Otherwise the sender has to stop sending data until the receiving window gets some space.

-The red line represents the ACKED packets for the packets sent by the sender. The Round Trip Time for a certain packet can be calculated by measuring the time between blue line and the red line for a certain packet.

e) Obtain the Window Scaling graph from Wireshark statistics. Explain what happens in the obtained graph.

-There are two lines in this graph.

1.Blue : bytes in flight
2.Green : receive window of the receiver

-This graph shows the receive window and the data in flight. In this graph the green graph always must go higher than the blue graph because the sender can not send more packets than the receiving window.The time between two adjacent blue bursts of inflight packets is the round trip time.