Solved exercises on Computer Networks and Distributed Systems

1. Is TCP a secure transmission protocol?

   No, TCP is a reliable transmission protocol, that is in the sense that TCP can compensate for the omission faults inherent to the Internet Model of Service, however, it does not incorporate any cryptographic algorithms which might confer it the character of secure protocol.

2. Explain what's the basic goal of the UDP protocol.

   UDP is a simple transport multiplexer. It offers a multiplexing key composed of a single 16-bit unsigned integer known as port that serves for locating a receiving thread within the receiving host's stack.

3. Describe the components of the TCP multiplexing key

   Src IP, Src Port, Dst IP, Dst Port

4. The following questions, all refer to the trace in Fig. 1.

   a. What does the sequence of frames from no. 971 through 1441 represent? Explain your answer by describing the most remarkable patterns that appear on that frame sequence.

   This frame sequence consists of a number of repeated connection-requests made by a client. Since the server is not responding to any of them, the client sends several back-to-back connection requests in the hope that the server will eventually respond. In this specific case, each SYN segment (A TCP connection request) sent by the sender (The client) starting with frame #979 is a retry of a connection request. As is usual in Computer Science, the mathematical function that governs the distance (In time) between each two successive retries follows an exponential law (Function). In the case of the considered trace, the inter-distance between each pair of successive frames is twice the preceding one. For example, in the case of frames [971; 979; 989] we have, respectively:

   [284.045661; 285.069382; 287.085273]

   The resulting interdistances are: 1.023721 (First one and second one) and 2.015891 (Second one and third one). Clearly, the latter inter distance is double the former one, roughly, as it were. This pattern can be confirmed in all the remaining cases.

   We observed this behavior in the practices about TCP analysis with Wireshark.

   b. Tell which TCP states must the relevant client, welcome and delegate sockets be in

   No connection established => Client SYN-Sent; Welcome socket: Closed; Delegate socket: closed
   The client socket must be in the Syn-Sent state. As to the Server Socket, we claim it is most likely in the Closed state since the server socket is not responding to the reception of Syn segments, however, we must also observe that it could also be in the Listening state with the backlog (Queue) of pending connections full. Solution Diagram 1 illustrates why the Server Socket (Passive or Welcome, also) could either be closed or created but yet not in the listen state. In both cases, the Passive Socket would not respond with Ack-Syn to receiving a new Syn from a client, which is the behavior we are observing in the TCP trace included in the present question.

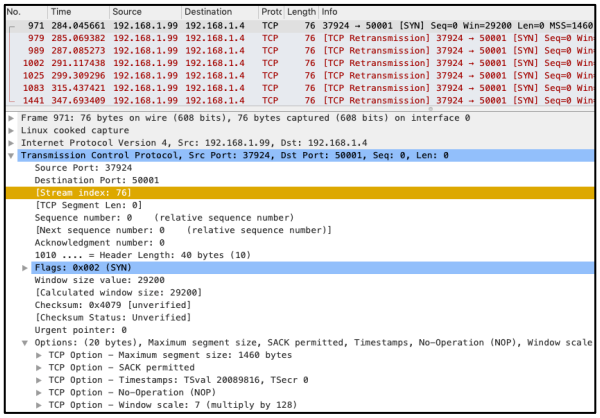

Figure 1. Wireshark trace.

c. Can you tell for sure whether the client host and server host are located in the same network? Explain your answer.

We cannot tell for sure whether both hosts are located within the same IP network because we do not know the network mask (Or the CIDR prefix) to each IP address (Review ch. 3 of CN)

d. *Can* you calculate the average Rtt attained? Explain your answer.

We cannot calculate any of the Rtts because the sending host is not receiving Syn-Ack replies to the Syn segments sent

5. Explain each of the most important Transparencies of Distributed Systems

Access, location, performance, scaling, faults, replication, concurrency, mobility

6. Tick the true characterizations of a TCP connection when a TCP module sends a segment with ACK set and **ACK SN = 2000**

- ☐ a. The last received segment carried data through SN 1999; the SN of the next expected segment is 2000
- ☐ b. That TCP module has successfully received all the segments containing data bytes through SN 2000 and the next expected SN is 2001
- ☐ c. The last received segment contained data bytes through SN 2000
- ☐ d. The TCP module has received all the data bytes from sequence number 0 through SN 2000
- ☐ e. The TCP module has received all the data bytes from the Initial Sequence number through SN 1999
- ☐ f. The last received segment contained the SN 1999
- ☐ g. None of these former options is true

7. Host H_t sends a TCP connection request to host H_r. The connection evolves according to the chronogram in Fig. 2. For simplicity, the example is built such as the only sending host is H_t. As required by TCP, data transmission is initiated in the TCP Slow Start dynamic state (SS) by sending a single full segment in the Rtt following the 3-way handshake. The Estimated Rtt before the first Rtt begins is 1 sec and the value of $\alpha = 0{,}8$. Relevant time points mentioned in the following questions are marked with symbol: N. Respond to the following questions regarding this TCP connection:

a. What is the maximum acceptable amount of bytes that the client can send in any single segment? Compose your solution with sufficient precision.

Server's MSS is 1000 *as announced in the 3-way handshake*

b. When is the RTO timer created and started (Use a symbol ⊗)?

c. Mark the points in time when the RTO timer is reset (Use a symbol ®)

d. Mark the points in time when RTO timer is stopped (Use a symbol ©)

e. Mark the points in time when RTO timer fires (Use a symbol [F])

f. Mark the points in time when the a new Rtt_{sample} is taken (Use a symbol >)

g. Assume that three samples of Rtt are taken along the evolution of the connection at time points 1, 2 and 4 which values are: RttSample[1] = 70 ms; RttSample[2] = 50 ms and RttSample[3] = 60 ms[1]. Calculate the length of the RTO timer scheduled after RttSample[3] is taken and which will protect the loss of the segment sent after time point 5. The initial value of EstimatedRtt is 1 sec.

$\alpha = 0,8$

Index	EstimatedRtt[n+1]	0,8·EstimatedRtt[n]	0,2·RttSample[n]	RTO[n+1]
0	1	-	-	2
1	0,814	0,8 · 1	0,2 · 0,07	1,628
2	0,6612	0,8 · 0,814	0,2 · 0,05	1,3224
3	0,54096	0,8 · 0,6612	0,2 · 0,06	**1,08192**

h. What's the value of TCP state variable snd.una in host Ht right after time point 4?

7001

i. Explain what is the maximum number of bytes that *can be* sent after ACK 3001 is received at time point 2, that is, within the Rtt just initiated?

SS, 2 ·2000 = 4000

j. [1] Explain the situation marked by time point no. 3.

Stretch ACK worth [3001, 7000]

[1] Note that the index used for the samples represents the relative order of the samples, not the time points in the diagram when they were taken.

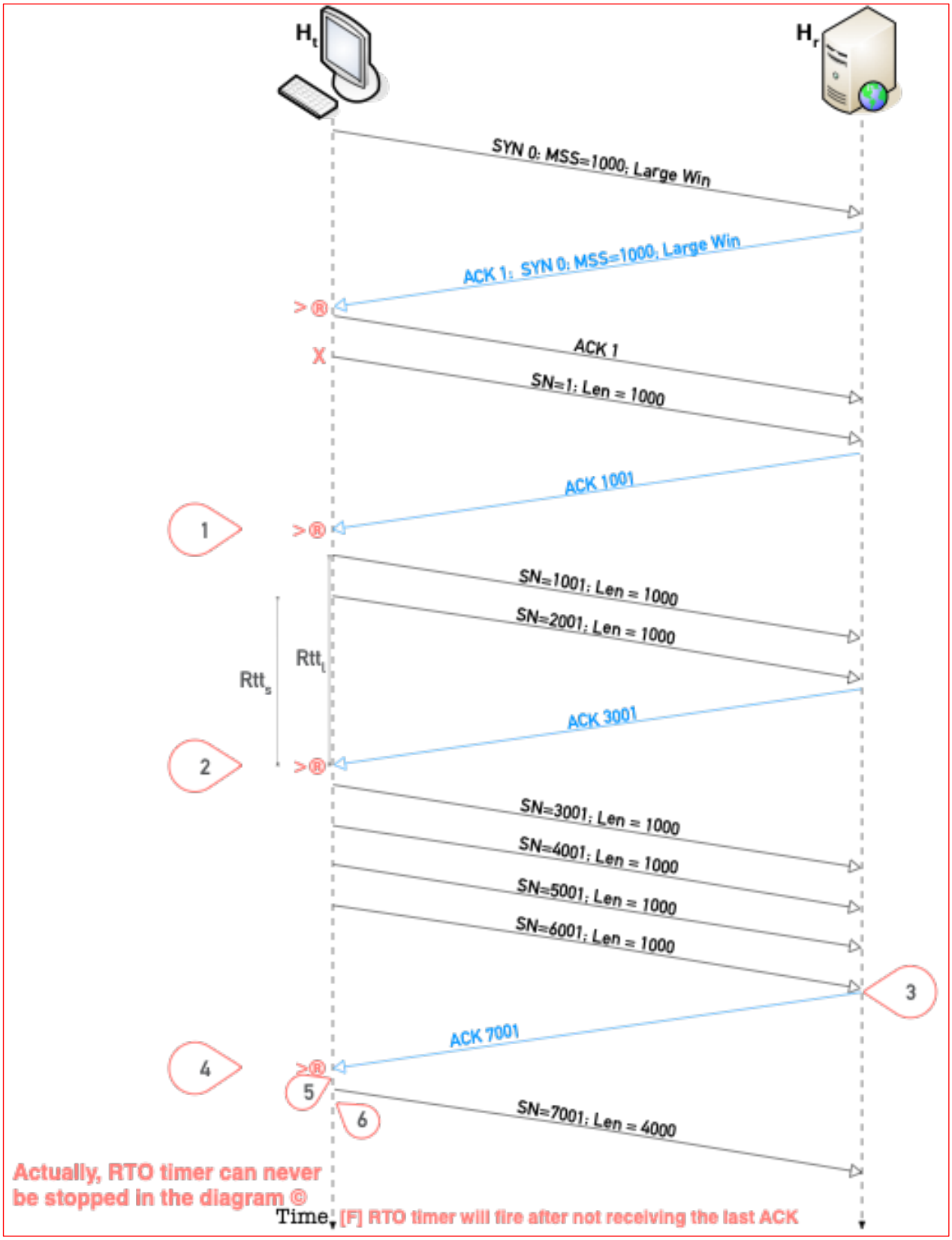

Figure 2. Transmission diagram for TCP connection

8. When a new TCP segment is received, the receiver copies the timestamp TSVal received into the ACK sent back field TSEcr, this will allow the transmitter to compute the Rtt achieved in the transmission. The text fragment in Fig. 3 was extracted from RFC 7323 (*TCP options for performance*), it specifies which value of TSVal should be copied into the ACK sent back when a that ACK has been delayed (A DelAck), and consequently covers two back-to-back segments. Read the fragment and explain the solution that it proposes. Include a diagram that illustrates the problem and that highlights the solution.

```
4.3.  Which Timestamp to Echo

   If more than one Timestamps option is received before a reply segment
   is sent, the TCP must choose only one of the TSvals to echo, ignoring
   the others.  To minimize the state kept in the receiver (i.e., the
   number of unprocessed TSvals), the receiver should be required to
   retain at most one timestamp in the connection control block.

   There are three situations to consider:

   (A)  Delayed ACKs.

        Many TCPs acknowledge only every second segment out of a group
        of segments arriving within a short time interval; this policy
        is known generally as "delayed ACKs".  The data-sender TCP must
        measure the effective RTT, including the additional time due to
        delayed ACKs, or else it will retransmit unnecessarily.  Thus,
        when delayed ACKs are in use, the receiver SHOULD reply with the
        TSval field from the earliest unacknowledged segment.
```

Figure 3. Text fragment from RFC 7323, pg. 16.

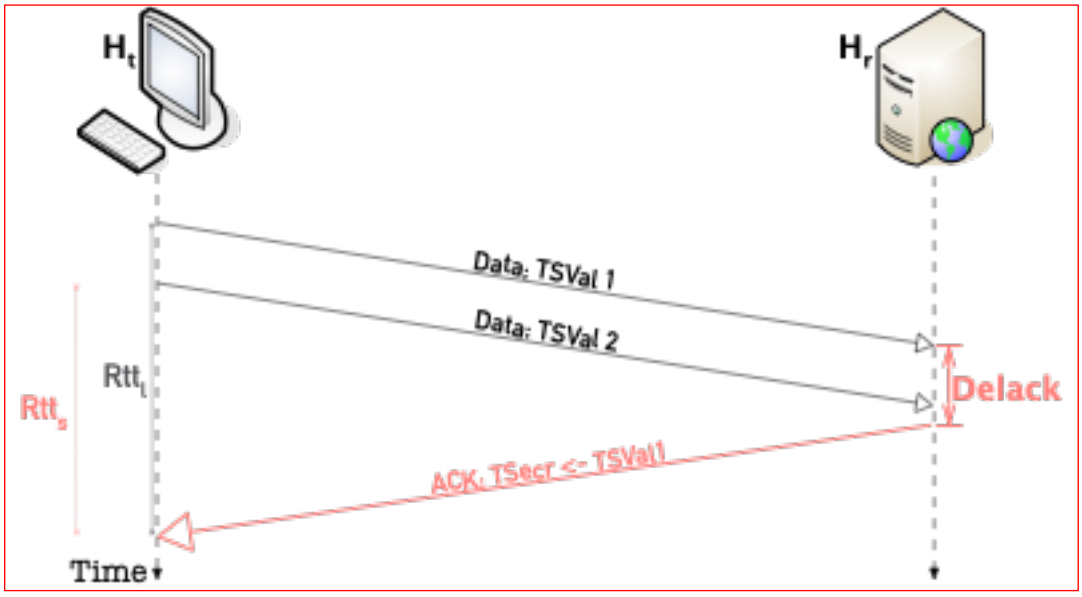

Figure 3'. Solution