תרגיל בית תיאורטי מס' 4

להגשה עד 15.6.2011

TCP Reliable Data Transfer

1) (taken from Kurose & Ross, 5th ed.)
   Consider transferring an enormous file of L bytes from A to B.

   a) What is the maximum value of L such that TCP sequence numbers are not exhausted? Recall that TCP sequence number field has 4 bytes.

   b) For the L you obtain in (a), find how long it takes to transmit the file. Assume that a total of 66 bytes of transport, network, and datalink headers are added to each segment before the resulting packet is sent out over a 10Mbps link. Ignore flow and congestion control, so A can send the segments back to back continuously.

TCP Congestion Control

Note: In the following questions congestion control is assumed to work as follows:

- At each stage a set of segments of total data size CWIN (also called cwnd) is sent and CWIN is evaluated again only after receiving ACKs for all these segments, or receiving a timeout on one of them.
- We assume that there is no case of triple duplicate, so we have no difference btw Reno and Tahoe. In question 3: The flow control window is always larger than CWIN.

2) In a TCP connection, A sends information to B and its parameters are: MSS=1000, THR=16,000, WIN=58,000, CWIN=18,000. Host A sends information according to these parameters and all the segments sent by A are acknowledged on time. What will be A's CWIN after receiving all the acknowledgements? Explain.

3) We are looking at a TCP connection between A to B that has been already running for some time, and consider only data transfer from A to B.
   Points (a) to (h) below show consecutive values of CWIN used by the congestion control algorithm at A. These values are updated every RTT approximately, as discussed in class.

   a. X (unknown)
   b. Y (unknown)
   c. 4000
   d. 8000
   e. 16000
   f. 20000
   g. 22000

h. 24000
j. Z (unknown)

NOTE:

- in (f) the update of CWIN does not necessarily happen after a complete RTT as we assume to be the case for all other stages.
- Duplicate acks could have happened during the lifetime of the session before the events described in this question. Duplicate acks do not occur during the time frame to which the question refers (stages a – j).

Answer the following questions, and explain your answers.

(i) Can we determine the value of MSS from these data? If we can, what is it?
(ii) For each of the stages (c) to (h), write whether congestion control at A is in state SS or CA. Explain your answer.
(iii) Can we determine the value of THR at any of the stages (c) to (h)? For each stage for which we can, state it and explain your answer. For the stages for which we cannot – explain why.
(iv) Can we determine the value of Y? If we can, give it and explain your answer. If we cannot, explain why.
(v) Can we determine the value of THR at stage (b) and/or the state of congestion control at that stage? Give the values we can determine and explain your answer. For the values we cannot determine – explain why.
(vi) Answer questions (iv),(v) for the value X in stage (a).
(vii) Find the value of Z. If there are several possibilities, give all of them and explain in which scenario each of them occurs.

RSA

4) נתונים המספרים הראשוניים $p = 7, q = 13$.

a) מצאו מפתח פומבי ומפתח פרטי מתאימים.

b) השתמשו במפתח הפומבי כדי להצפין ב – RSA את ההודעה "m = "RSA, מקודדת ב – ASCII.
הצפינו כל אות בנפרד.
שימו לב שתצטרכו לערוך חישובים מדוייקים על מספרים שלמים גדולים. ניתן לעשות זאת למשל באמצעות BigInteger של Java או C#. תוכלו להשתמש בכל כלי שתבחרו, אך פרטו את כל החישובים שביצעתם.

c) השתמשו במפתח הפרטי כדי לפענח את ההודעה המוצפנת.

d) האם התהליך היה עובד לו הייתם מצפינים במפתח הפרטי ופותחים במפתח הפומבי? האם יש הגיון לעשות כזה דבר לצורך כלשהו? (רמז: תראו שימוש כזה בהרצאה על Network Security).