Homework 5 assignment for ECE374

Posted: 04/25/15

Due: 05/01/15

Note: *In all written assignments, please show as much of your work as you can. Even if you get a wrong answer, you can get partial credit if you show your work.* If you make a mistake, it will also help the grader show you where you made a mistake.

Problem 1: (15 Points)

a. Suppose we send into the Internet two IP datagrams, each carrying a different UDP segment. The first datagram has source IP address A1, destination IP address B, source port P1, and destination port T. The second datagram has source IP address A2, destination IP address B, source port P2, and destination port T. Suppose that A1 is different from A2 and that P1 is different from P2. Assuming that datagrams reach their final destination, will the two UDP datagrams be received by the same socket? Why or why not?

b. Suppose, Alice, Bob, and Claire want to have an audio conference call and use UDP. How many individual unicast UDP streams need to be set up in this case? (Keep in mind this is conference call where everyone needs to be able to communicate with everyone else.) Would using multicast reduce the number of required streams? Explain your answer briefly!

Problem 2: (20 Points)

Answer the following questions assuming Dynamic Adaptive Streaming over HTTP is used for video streaming.

a. When using DASH for streaming, does this require a dedicated streaming server or can a regular HTTP server be used? Why or why not?

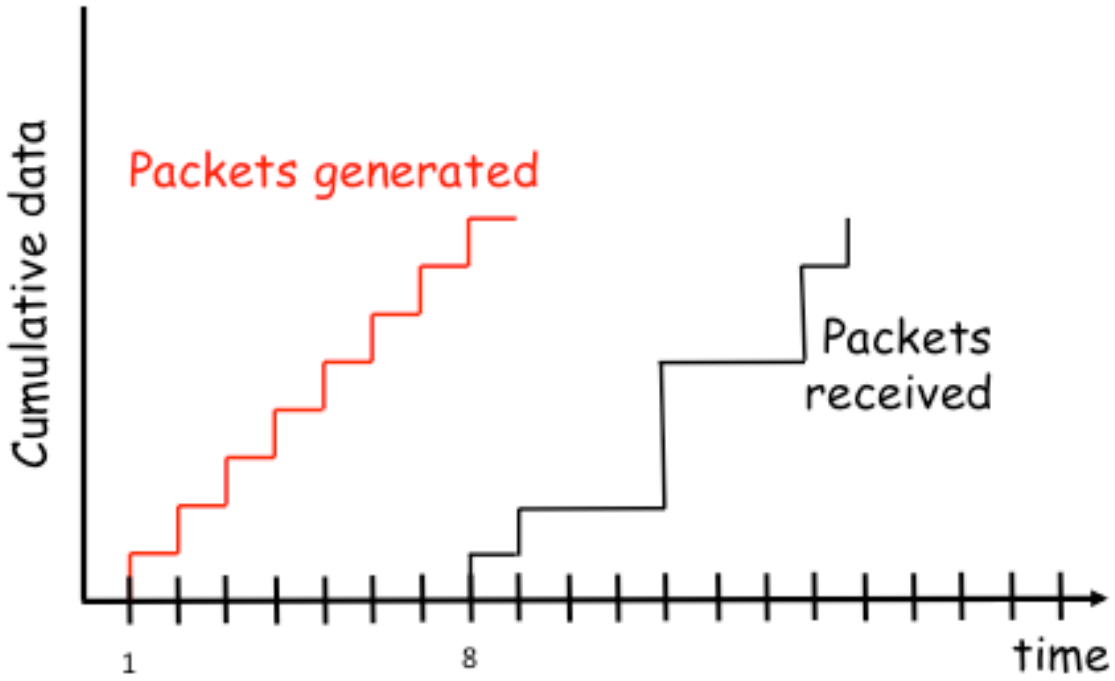
b. Give a brief explanation of the manifest file that's stored on the server in addition to each video.

c. Explain the client behavior in the case where the highest possible quality of the stream is currently transmitted to the client and the buffer fill has fallen below the minimum threshold.

d. Assuming a 5-minute video should be offered in 5 different quality versions and the DASH segment length is 10 seconds. How many individual files will have to be stored on the server if AVC encoding is assumed?

Problem 3: (25 Points)

Consider the figure below. A sender begins sending packetized audio periodically at *t=1*. The first packet arrives at *t=8* at the receiver.



a) What are the delays (from sender to receiver, ignoring any playout delays) of packets 2 through 8? Note that each vertical and horizontal line segment in the figure has length of 1,2, or 3 time units.
b) If audio playout begins as soon as the first packet arrives at the receiver at *t=8*, which of the first eight packets sent will *not* arrive in time for playout?
c) If audio playout begins at *t=9*, which of the first eight packets sent will *not* arrive in time for playout?
d) What is the minimum playout delay at the receiver that results in all of the first eight packets arriving in time for their playout?

Problem 4: (20 Points)

a. Figure 1 shows a mobile handover scenario. In this figure, indicate the right sequence in which the handoff with a common MSC is performed by indicating the correct sequence in the empty circles. Explain briefly the procedure that is carried out in each step.

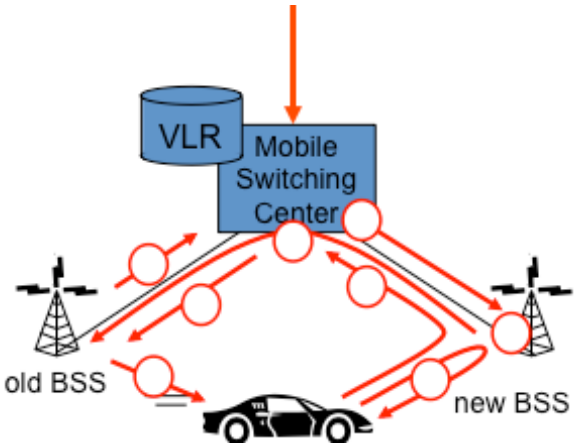


Figure 1: Mobile handover

b. In Figure 2, indicate the correct sequence in which the steps for a "handover" in a mobile Internet scenario are performed.

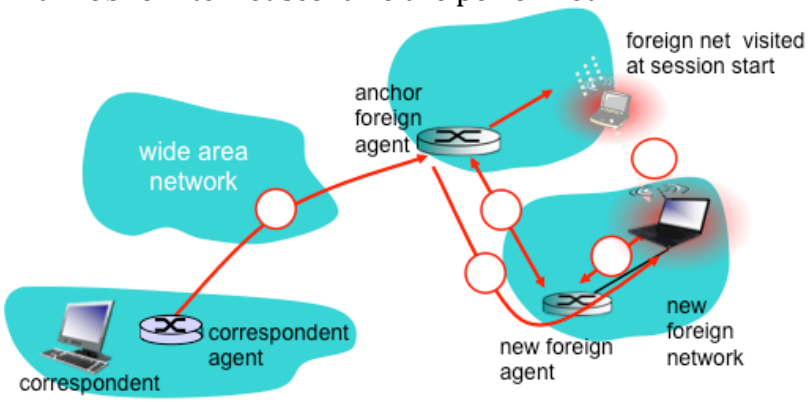


Figure 2: Mobile Internet hand over

Problem 5: (10 Points)

Suppose Alice wants to send an email to Bob. Bob has a public-private key pair (K^+_B, K^-_B), and Alice has Bob's certificate. But Alice does not have a public, private key pair. Alice and Bob (and the entire world) share the same hash function H(.).

a. In this situation, is it possible to design a scheme so that Bob can verify that Alice created the message? If so, show how with a block diagram for Alice and Bob.
b. Is it possible to design a scheme that provides confidentiality for sending the message from Alice to Bob? If so, show how with a block diagram for Alice and Bob.

Problem 6: (10 Points)

Suppose Alice and Bob are communicating over an SSL session. Suppose an attacker, who does not have any of the shared keys, inserts a bogus TCP segment into a packet stream with correct TCP checksum and sequence number (and correct IP

address and port numbers). Will SSL at the receiving side accept the bogus packet and pass the payload to the receiving application? Why or why not?