COMP 5622 (Spring 2013) Homework #2

Due Date: 15:00 May. 10, 2013

1. (20 marks) Answer the following questions.
   1) In RPF, is every link traversed? Give a proof for your answer.

   Yes.
   (1) Consider the shortest paths from the source to all other nodes in the network. The shortest paths form a tree (shortest path tree).
   (2) When the source sends a broadcast/multicast message, the message propagates to the entire shortest path tree because every node forwards the message to all its links (except for the one from which it receives the message) and thus must forward to the links in the shortest path tree.
   (3) The broadcast/multicast message reaches all nodes in the network because the nodes in the shortest path tree are the nodes in the network.
   (4) Each node receives the broadcast/multicast message from its shortest-path link at least once. (Follows (2) and (3)).
   (5) Each node forwards the broadcast/multicast message to all its links (except for the link from which it receives the message) at least once. (Follows (4)).
   (6) The broadcast/multicast message is sent on each link at least once because every link is connected to two nodes. That is, every link is traversed.

   2) In RPF, can there be a cycle of packet forwarding? Give a proof for your answer.

   No.
   If there is a circle and all nodes on the circle forwards the broadcast/multicast messages, all the links in the circle are in the shortest-path tree. Hence, the shortest-path three has a circle. This contradicts the definition of the shortest path tree. Hence, it is impossible that there be a circle in RPF.

   3) What are the advantages and disadvantages of direct routing in mobile networks?

   Advantage: The mobile can directly communicate with the correspondent without intermediate relays at home. This reduces overhead.

   Disadvantage: The care-of address is visible to the correspondent, and additional measures should be taken to accommodate continuous mobility of the mobile.

2. (12 marks) Answer the following questions. **Please describe the reasons for your answers and show the steps of developing your answers.**

   1) (8 marks) Alice wants to send a message **m** to Bob with secrecy, sender authentication, message integrity, and sender non-repudiation (the sender could not deny that he or she has sent the message). Can you help Alice design a solution that satisfies these

requirements? Please describe your solution.

Alice can generate a signature of **m** *by encrypting a digest of* **m** *with her private key, then encrypt* **m** *and the signature with Bob's public key, and send the encrypted ciphertext,* K_B^+ *(***m***,* K_A^- *(H(***m***))), to Bob.*

Or, if Alice would like to minimize the use of heavy public-key encryption, she can generate a symmetric key, Ks, for encrypting the message and the signature, and use Bob's public key to encrypt Ks. That is, Alice sends the following data to Bob.

K_B^+ *(Ks), Ks(***m***,* K_A^- *(H(***m***)))*

Note: other solutions exist.

2) (4 marks) Suppose there are 100,000,000 PCs and 10,000,000 web servers on the Internet, and we re-engineer the Internet to use IPsec on all PCs and web servers. We set up SA information on every PC and server so that any PC can communicate with any web server without conducting additional authentication or key exchanges. Without using SSL, can IPsec ensure the secrecy and authentication of the PCs and web servers in their communication? How many SAs does each PC need to record at the minimum?

Yes, IPsec can ensure secrecy and authentication of PCs and web servers in their communication.
Since any PC can communicate with any of the 10,000,000 web servers and each SA handles one direction in the communication, a PC needs to record totally 20,000,000 SAs.

3. (16 marks) Queueing theory

This question assumes an M/M/1 model. A network bridge receives packets at a mean rate of 450 packets per second (pps) and the bridge takes 2 ms to process and forward a packet.

Hint: M/M1 queueing

Probability of 0 jobs in the system	$P_0 = 1-\rho$
Probability of n jobs in the system	$P_n = \rho^n(1-\rho)$
Mean queue length	$L = \frac{\rho}{(1-\rho)}$

1) (3 marks) What is the bridge's utilization?

λ = 450 pps
μ = 1/ (2 x 10^{-3}) pps = 500 pps
$\rho = \lambda / \mu$ = 90%

2) (3 marks) What is the average number of packets in the system (the bridge)?

$L = \rho / (1 - \rho)$ = 0.9/0.1 = 9

3) (5 marks) What is the average waiting time for packets in the system (the bridge)?

$W = L / \lambda = 1 / (\mu - \lambda) = 1 / 50$ s = 20 ms

4) (5 marks) What is the probability that there are 5 or more packets in the system (the bridge)?

$P(n >= 5)$
$= 1 - (P(0) + P(1) + P(2) + P(3) + P(4))$
$= \rho^5$
$= 0.9^5$
$= 0.59049$

4. (16 marks) Consider the figure below. A sender begins sending packetized audio periodically at t=1. The first packet arrives at the receiver at t=8.

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 a length of 1, 2, 3, or 4 time units.

Packets 2 through 8 have delays of 7, 8, 7, 10, 9, 8, and 8 time units, respectively.

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?

Packets 3, 5, 6, 7, and 8.

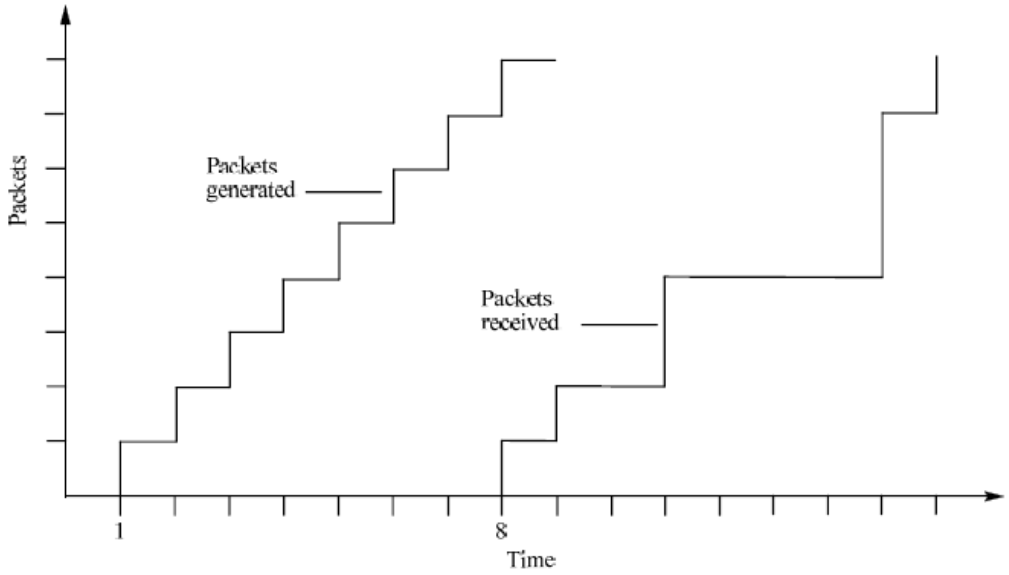
If we assume the playback software plays all packets in order and increases the playout delay as it waits for packets to arrive, the following packets will not arrive in time: packets 3 and 5. The playback software has to introduce interrupts in the playback to wait for these packets.

c. If audio playout begins at t=9, which of the first eight packets sent will *not* arrive in time for playout?

Packet 5 and 6.

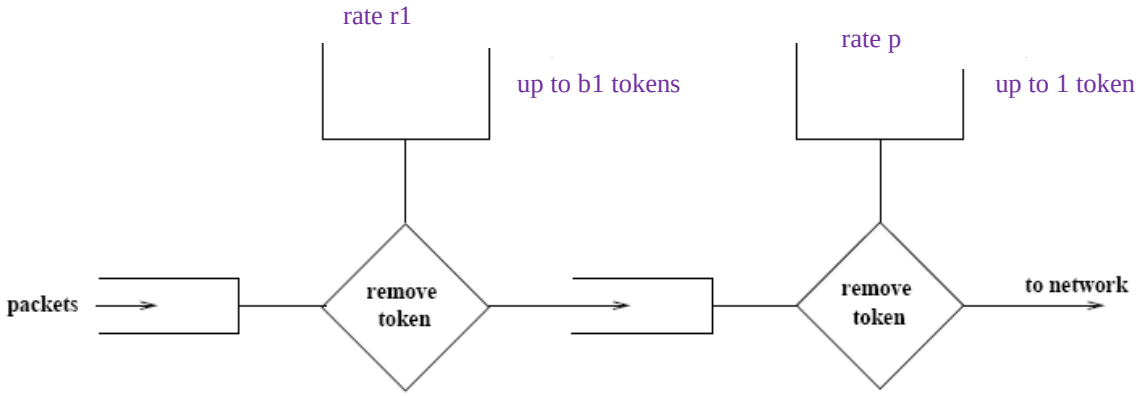
d. What's the minimum playout delay at the receiver that results in all of the first eight packets arriving in time for their playout?

3 time units for the playout delay.



5. (18 marks) A leaky bucket is specified as (r, b) where r is the rate at which tokens are added to the bucket and b is the capacity of the bucket. Consider a leaky bucket B1 with specification (r1, b1). r1 and b1 determine the average rate and burst size of the packet flow policed by B1. We now want to police the peak rate, p, as well. Show how the output of the leaky bucket B1 can be fed into a second leaky bucket, B2, so that the two leaky buckets in series police the average rate, peak rate, and burst size. Be sure to give the bucket size and the token generation rate for B2.

The token generation rate of B2 is p
The bucket size of B2 is 1



6. (18 marks) What is bi-section bandwidth? Compute the bi-section bandwidth of a hypercube with 32 nodes assuming every link has 1Gbps bandwidth.

The bisection bandwidth of a network is the minimum bandwidth between two partitions of the network where each partition contains half of the nodes in the network.

The bisection bandwidth of the 32-node hypercube is 16Gbps.