15-441: Computer Networks
Homework 4

Assigned: Nov 25th, 2013
Due: Dec 3rd, 2013 1:30 PM in class

Name:	Andrew ID:

1 Quality of Service

1. A link shared by each of the clients listed in the table below is rate-limited by a token bucket with depth D = 10 packets and Rate R = 1 packet / sec. (The shaping is per-client: each client gets its own D=10,R=1. Assume that the link is not the bottleneck, only the token bucket rate-limiting is.)

   (a) (5 points) Each row in the table describes the sending behavior of a particular client over a 10 second period. Each column is a one second slot, where that client's entry in the column describes how many packets it sends during that slot. For each client, you must decide if the token bucket will allow all packets to be sent, or if the traffic will be limited. Circle either "allowed" or "limited" for each client in the far-right column of the table. Assume the token bucket has 10 tokens at time 0.

Time	0	1	2	3	4	5	6	7	8	9	Result
client A	1	1	1	1	1	1	1	1	1	1	allowed / limited
client B	2	2	2	2	2	2	2	2	2	3	allowed / limited
client C	10	1	10	1	10	1	10	1	10	1	allowed / limited
client D	10	0	0	0	0	1	1	1	2	2	allowed / limited
client E	0	0	0	0	0	0	15	1	1	1	allowed / limited

   (b) (3 points) Do token buckets ensure consistent instananeous throughput? Why or why not? What is the maximum throughput obtained by any of the above flows (in packets per second)?

   (c) (2 points) Which of the following two applications is more likely to benefit from a token bucket scheme compared to using a simple constant rate-limit? Circle your answer **and briefly explain why.**

   - HTTP requests from a web-browser
   - Voice-over-IP (VOIP) traffic from a Internet phone

2 Cryptography

2. In class we discussed a handful of cryptographic primitives (cryptographic hashes, message authentication codes, digital signatures, symmetric/asymmetric encryption). However, using these primitives as building blocks to construct a secure protocol can be exceedingly difficult; it is easy to overlook small details and wind up with an unsecure protocol.

   For each of the simple protocols described below, state whether or not it is secure and briefly argue why or why not. Assume that the underlying cryptogrphic primitives are themselves secure and that the attacker is computationally constrained (i.e., not the NSA).

   Notation:

   - $||$ indicates concatenation.
   - $H(M)$ indicates the cryptographic hash of M.
   - $MAC(K, M)$ indidcates the message authentication code of M computed with key K.
   - K_{XY} indicates a symmetric key shared by X and Y.
   - K_X indicates X's public key.
   - K_X^{-1} indicates X's private key.

   Recall that the meaning of $\{M\}_K$ depends on the type of key:

   - Encrypt M with shared key K if K is a symmetric key.
   - Encrypt M with public key K if K is a public key.
   - Sign M with private key K if K is a private key.

   Part 1: Consider the following protocol for an online shopping system. Suppose the client (C) and the server (S) already share a symmetric key K_{CS}. The client wants to send a message, M, containing information about quantities of items to purchase plus a credit card number. The server wants to ensure that M really came from C and was not modified. Consider the following protocol:

   $$\begin{array}{ll} C \rightarrow S: & \{M\}_{K_{CS}} || MAC(K_{CS}, M) \\ S: & \text{decrypt } M \text{ and verify the MAC using } K_{CS} \end{array}$$

   (a) (2.5 points) Is the protocol secure against an attacker stealing the user's credit card information?

   (b) (2.5 points) Is the protocol secure against an attacker changing the order or making additional orders?

Part 2: Alice and Bob use the following Diffie-Hellman-based protocol to establish a shared secret key. Assume Alice knows Bob's public key, K_B. Bob knows nothing about Alice. Consider the following protocol:

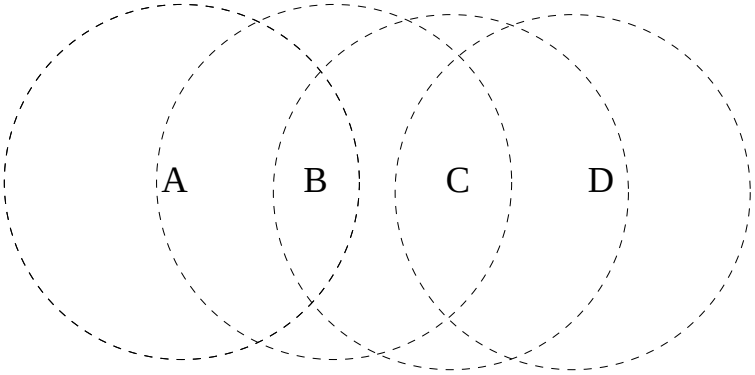
$A:$	picks secret a
$B:$	picks secret b and public DH values p and g
$B \rightarrow A:$	$g\|\|p\|\|g^b \mod p \|\| \{g\|\|p\|\|g^b \mod p\}_{K_B^{-1}}$
$A:$	verify $\{g\|\|p\|\|g^b \mod p\}_{K_B^{-1}}$ using K_B
$A \rightarrow B:$	$g^a \mod p$
$A:$	calculate secret key $K_{AB} = (g^b \mod p)^a = g^{ab} \mod p$
$B:$	calculate secret key $K_{AB} = (g^a \mod p)^b = g^{ab} \mod p$
$A \rightarrow B:$	$\{H(K_{AB})\}_{K_{AB}}$
$B:$	verify the hash sent by A matches the hash of the key B computed

(a) (2.5 points) Is this secure against attackers learning K_{AB}?

(b) (2.5 points) Is this secure against man-in-the-middle attacks?

3 Wireless & Mobile

3. Consider the following topology of wireless laptops A, B, C and D. The dotted lines indicate the range of wireless transmissions from each node. For example, B is within range of A, A & C are within range of B, B & D are within range of C and only C is within range of D.



Assume that each node uses an RTS/CTS based MAC protocol (i.e. like MACAW)

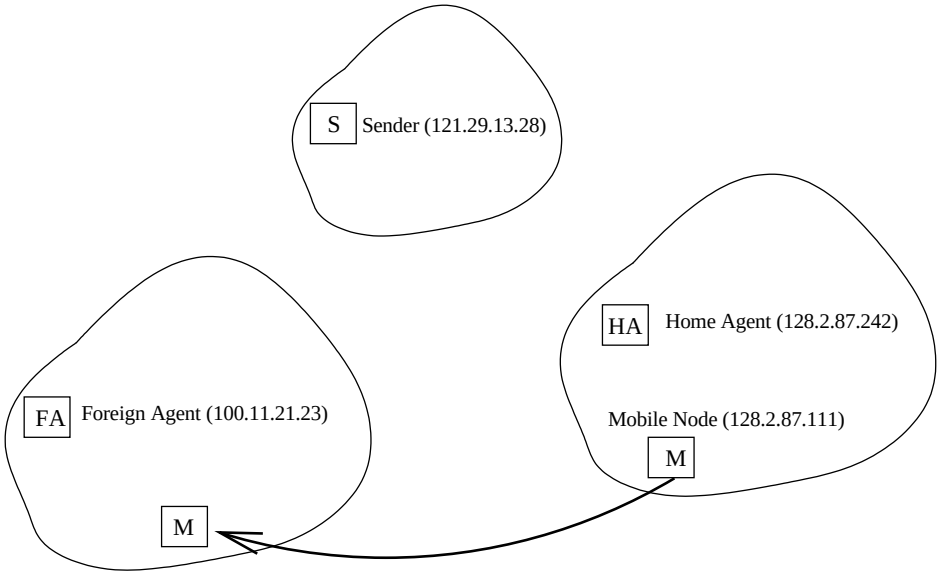
(a) (2 points) If C is sending B an RTS, why does A know not to transmit?

(b) (2 points) If B is sending data to C, why does D know not to transmit?

(c) (2 points) Using the nodes above, give an example of the hidden terminal problem.

(d) (2 points) David is considering implementing a walkie-talkie service for his wireless PDAs. His program largely uses small packets to avoid delaying any voice. Should he use RTS/CTS for his deployment? Why?

(e) (2 points) After collision detection was developed for Ethernet, its technique was not adopted by wireless networks. Why is it not possible to achieve true collision detection in wireless networks?



4. A sender S is sending TCP data to a mobile host M (see Figure). Initially the mobile host is in its home network. Later on it moves to a different network and needs to use Mobile IP in order to receive data from S. All local area networks are Ethernets.

   Part 1: The sender S sends TCP data to M while is in its home network.

   (a) (2 points) What headers does each packet have (names only [e.g., 'ethernet']), starting with the layer 2 header and up to the transport layer header?

   (b) (2 points) What are the source and destination IP addresses in the packet?

   Part 2: Now M has moved to the foreign network. S still wants to send packets to M.

   (c) (2 points) What headers does each packet have (names only), starting with the layer 2 header and up to the transport layer header, as the packets arrive at the M's home agent (HA)?

   (d) (2 points) What headers does each packet have (names only), starting with the layer 2 header and up to the transport layer header, as the packets arrive at the M's foreign agent (FA)?

   (e) (2 points) What are the source and destination IP addresses in the packet in (d)?