/

9561104
陳以深

EE 3650 **Introduction to Computer Networks** (Total 100 points.) June 21, 2010.

1) *(TCP, 20%) Please be brief in answering the following questions.*
   a) *(2%)* In order to support multiple application processes, what are the 4-tuples used as a TCP demux key?
   b) *(2%)* Describe how TCP uses the AIMD algorithm for congestion control?
   c) *(2%)* Why do we need the slow start mechanism in AIMD?
   d) *(2%)* Since TCP is full-duplex, what the two main fields in a TCP header are needed in order to keep packets to be transmitted and received in-order?
   e) *(2%)* Draw the timeline of the three-way handshake algorithm used in TCP.
   f) *(2%)* Figure 1 is the state transition diagram of TCP. Please trace the *normal* three-way handshake of both client and server on Figure 1.
   -2
   (Please **plot on the graph directly** and **send this sheet back** with you name and your student number.)

X

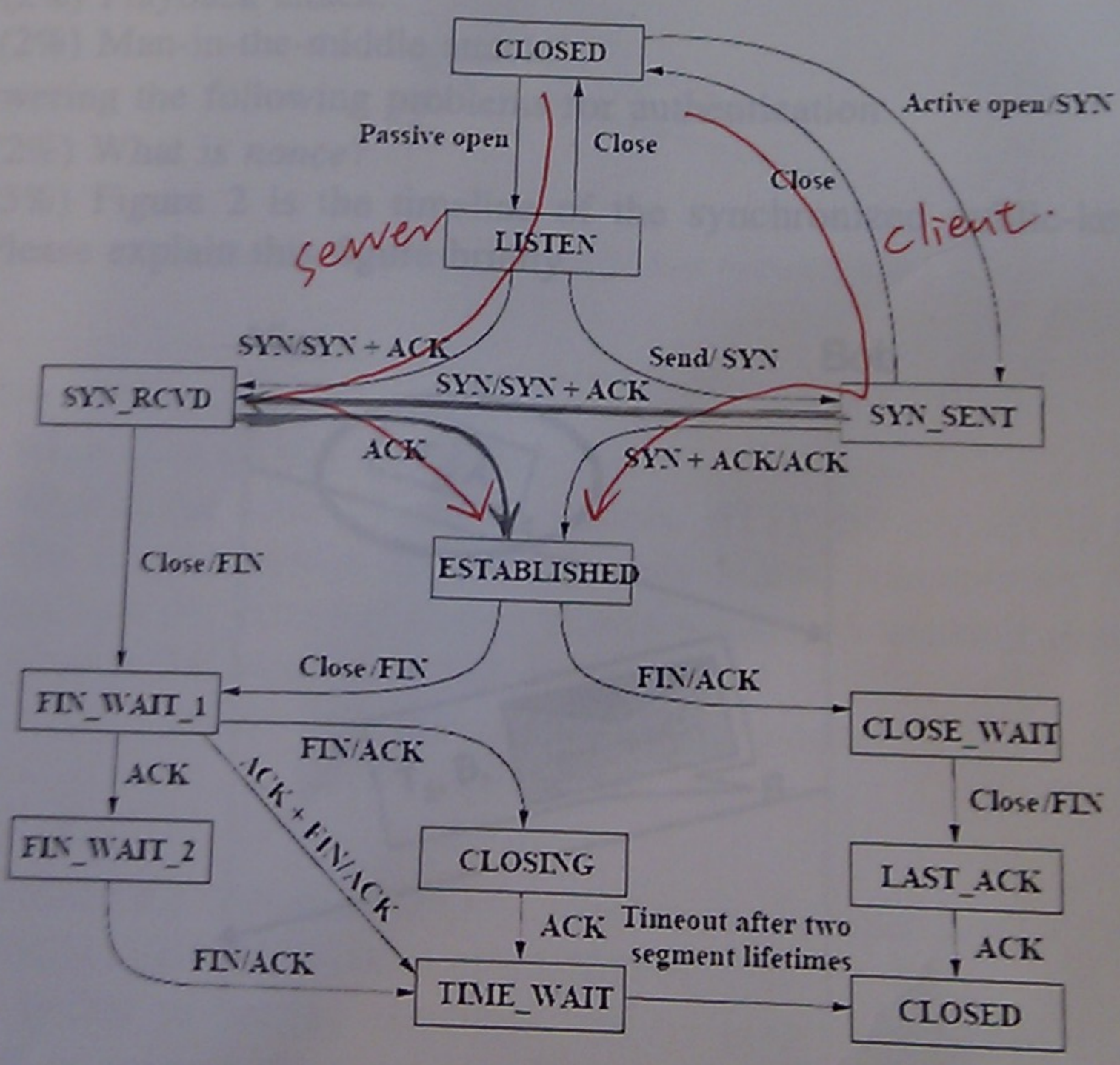

Fig. 1. State Transition Diagram of TCP

   g) *(2%)* Give a reason why TCP has to estimate RTT.
   h) *(2%)*How does TCP compute AdvertisedWindow? (Hint: use the following pointers and parameters: MaxRcvBuffer, MaxSendBuffer, LastByteRead, NextByteExpected, LastByteRcvd, LastByteAcked, LastByteSent and LastByteWritten.)
   i) *(2%)* In TCP, how to solve the silly window syndrome problem? Silly window syndrome: If the sender aggressively fills an empty container as soon as it arrives.
   j) *(2%)* Describe how RED is used in conjunction with TCP to avoid synchronized backoff?

2) (Queueing disciplines and QoS, 10%)
   a) (2%) Describe briefly what a priority queue is.
   b) (2%) Suppose that packet i with packet length P_i arrives at the router at time A_i. If the time stamp of packet $i-1$ is F_{i-1}, find the time stamp F_i for packet i under the *fair queueing* policy.
   c) (2%) Describe the difference between admission control and policing.
   d) (2%) Describe what RSVP does (including the PATH message and the RESV message).
   e) (2%) Describe briefly how self-clocking is used in TCP?

3) (Security, 14%)
   a) (2%) How can a RSA algorithm be used for digital signature?
   b) Describe the following Internet security attacks.
      i) (2%) Playback attack.
      ii) (2%) Man-in-the-middle attack.
   c) Answering the following problems for authentication.
      i) (2%) What is *nonce*?
      ii) (3%) Figure 2 is the timeline of the synchronized public-key authentication, Please explain this figure briefly.

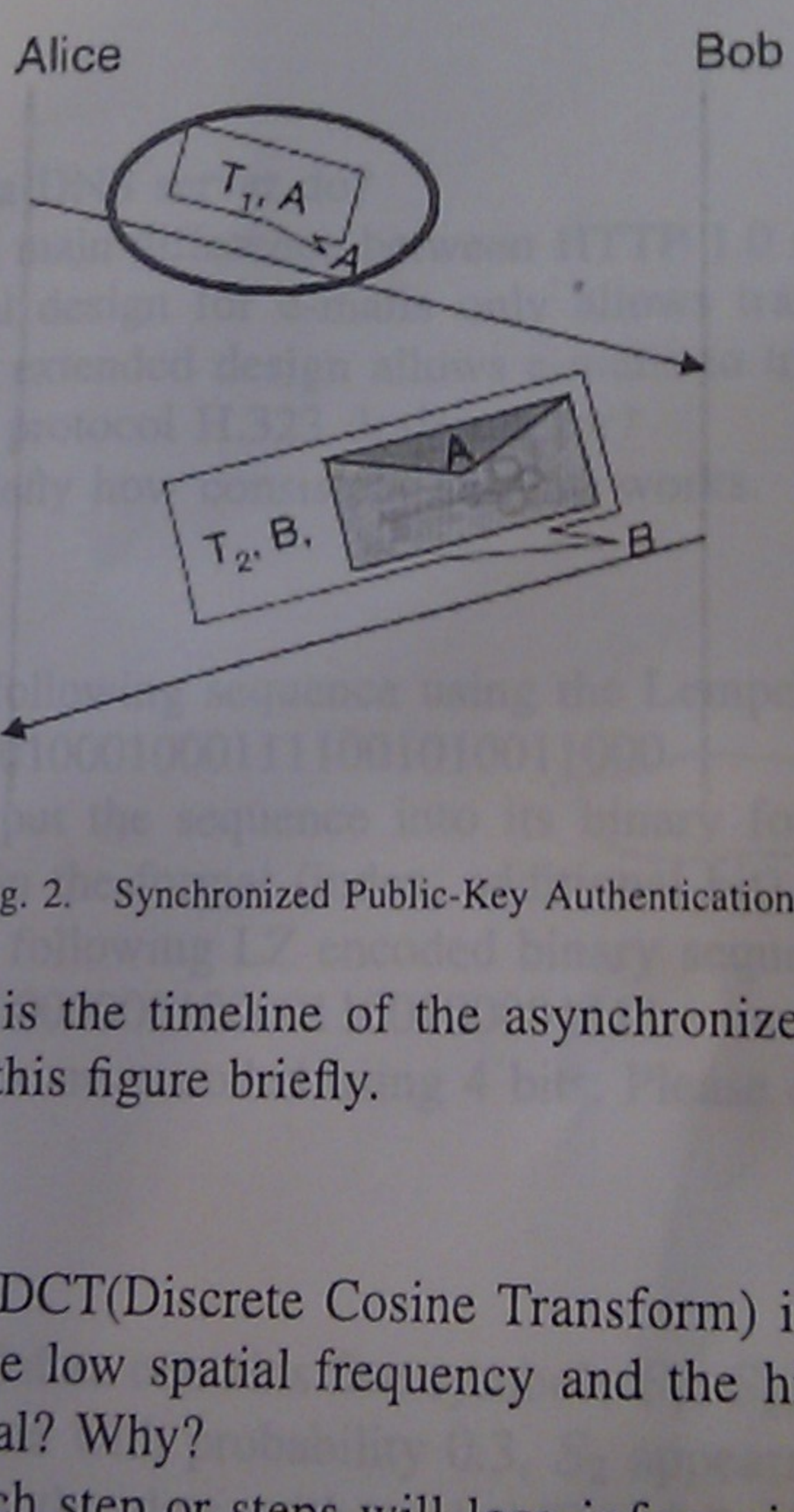

Fig. 2. Synchronized Public-Key Authentication

      iii) (3%) Figure 3 is the timeline of the asynchronized public-key authentication, Please explain this figure briefly.

4) (JPEG and MPEG, 6%)
   a) (2%) Consider the DCT(Discrete Cosine Transform) in JPEG, after the transform, it has two parts: the low spatial frequency and the high spatial frequency, which one is more essential? Why?
   b) (2%) In JPEG, which step or steps will lose informaion?
   c) (2%) There are three kinds of frames in MPEG. Which one of them can be decoded independently?

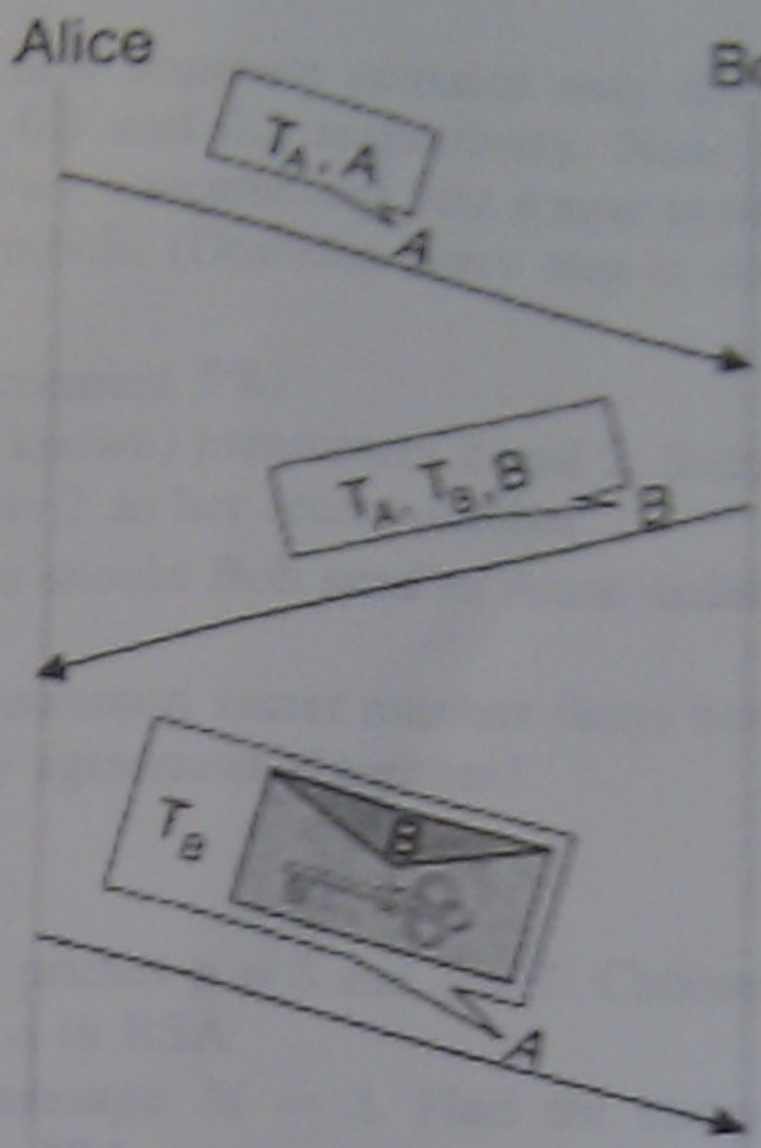

Fig. 3. Asynchronized Public-Key Authentication

5) (Applications 10%)
   a) (2%) What does a DNS server do?
   b) (2%) What is the main difference between HTTP 1.0 and HTTP 1.1?
   c) (2%) The original design for e-mails only allows transmitting ASCII characters. Describe how the extended design allows e-mails to transmit multimedia data.
   d) (2%) What is the protocol H.323 designed for?
   e) (2%) Describe briefly how consistent hashing works.

6) (LZ coding, 10%)
   a) (5%) Encode the following sequence using the Lempel-Ziv(LZ) algorithm.
   0101100101110100100010001111001010011000
   Do not bother to put the sequence into its binary form, but simply state it as a sequence of pairs in the format (index, additional bit).
   b) (5%) Consider the following LZ encoded binary sequence.
   00001000110010100000001000011001000011111
   Suppose the indeces are encoded using 4 bits. Please decode it to find the original sequence.

7) (Huffman coding, 10%)
   a) (5%) A sequence of data contains five symbols S_1, S_2, S_3, S_4 and S_5. Suppose that S_1 appears in the data with probability 0.3, S_2 appears in the data with probability 0.25, S_3 appears in the data with probability 0.2, S_4 appears in the data with probability 0.15, and S_5 appears in the data with probability 0.1. Use the Huffman coding to represent these five symbols. (Describe every step in details.)

b) (5%) Consider a new sequence contains only three symbols S_1, S_2 and S_3 with probabilities 0.5, 0.3 and 0.2 respectively. Now, for achieving better efficiency, each two symbols are concatenated into a new symbol. Use the Huffman coding to represent these symbols. (Describe every step in details.)

8) (Diffie-Hellman key agreement 5%)
Consider two (publicly known) parameters 2 and 5. Suppose Bob selects 3 as his secret number and Alice selects 2 as her secret number.

a) (2%) What number should Bob send to Alice under the Diffie-Hellman key agreement algorithm?

b) (3%) What is the common secret number (key) between Bob and Alice under the Diffie-Hellman key agreement algorithm?

9) (RSA and security, 15%)

a) (5%) Consider two primes $p = 3$ and $q = 7$. Choose an encryption key $e = 5$. Find the decryption key d in RSA.

b) (5%) Consider a message $M = 3$. Find the encrypted message C by using the encryption key e in RSA.

c) (5%) Show how you decrypt C to get $M = 3$.