UNIVERSITY OF CALIFORNIA, DAVIS

BERKELEY • DAVIS • IRVINE • LOS ANGELES • RIVERSIDE • SAN DIEGO • SAN FRANCISCO SANTA BARBARA • SANTA CRUZ

EEC173B/ECS152C **Winter 2006**

Homework 2 (due Jan 26, 2006)

1. **(20%) ALOHA and its variations**
   a) **(10%)** Assume for simplicity that each transmitted packet in a Slotted Aloha system is successful with some fixed probability p. New packets are assumed to arrive at the beginning of a slot and are transmitted immediately. If a packet is unsuccessful, it is retransmitted with probability q_r in each successive slot until successfully received.

      Find the expected delay T from the arrival of a packet until the completion of its successful transmission.

   b) **(10%)** In one variation of Slotted Aloha, the packet transmission time is 1 ms and the slot length is chosen to be 0.5 ms. Packets can arrive for transmission at any time, but are transmitted only on slot boundaries.
      NOTE: In regular Slotted Aloha, packet transmission should complete within a slot.

      i. **(5%)** What is the length of the "vulnerable period" for the protocol at hand? Remember that the vulnerable period for Pure/Slotted Aloha refers to the time around the transmission period of a packet during which if transmission of another packet begins, there will be a collision.

      ii. **(5%)** What do you expect the efficiency of this protocol to be compared to regular Aloha and Slotted Aloha?

2. **(18%) Improving the Throughput of Wireless LAN**
   IEEE 802.11n is a new standardization initiative to achieve over 100 Mbps throughput over Wireless LAN. Throughput improvement can be achieved via both Physical and MAC layer enhancement. This problem challenges you to consider MAC improvement for throughput enhancement.

   The following are three observations that recent researchers have made:
   - One of the factors that affect throughput is the large fixed overheads of 802.11 MAC/PHY layers (e.g., MAC header, ACK, etc associated with individual data unit).
     - Assume that packet size = size of data frame + size of MAC/PHY header
   - The following figure shows the theoretical throughput for 54Mbps WLAN.
     - Note that the fixed overheads in (1) are not useful data. When the packet size increases, the amount of overhead relative to the size of data frame decreases (resulting in higher throughput).
     - Ideally, you would want to operate in the range where packet is around 1900 to 2200 bytes.

- Unfortunately, the size of data frame is application-specific. Based on a measurement taken in the 802.11 standard meeting room in 2003, the data frame size follows the following statistics:
    - Less than 64 bytes: 49.5%
    - 64 – 127 bytes: 26.45%
    - 128-255 bytes: 6.27%
    - 256-511 bytes: 2.38%
    - 512-1023 bytes: 1.17%
    - 1024-2047 bytes: 14.31%
    - 2048-2346 bytes: 2.38%

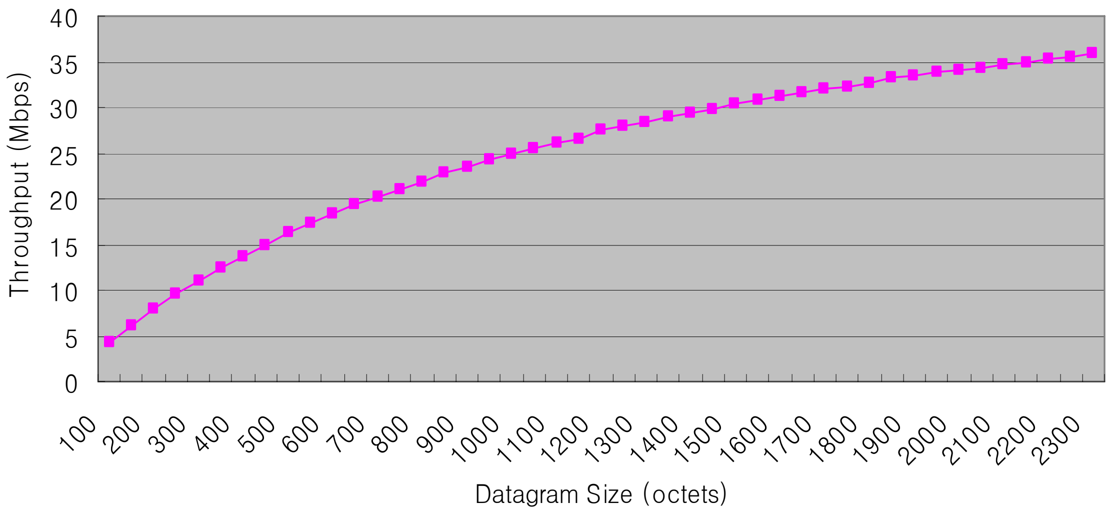

Figure 1

Based on these given facts, try to answer questions on the following page:

(a) (6%) Assume you can introduce changes in various layers (physical, link, MAC, etc) but you have to keep the physical & MAC layer headers per packet. Sketch a solution to improve throughput.

Hint: What can you do to achieve the optimal operating point (packet size) for achieving high throughput?

(b) (6%) What are the limitations of your approach in (a)?

(c) (6%) Does your approach perform differently depending on applications (e.g., ftp vs. voice over IP or multimedia streaming)?

3. **(12%) Hands-on: Investigation of Routing Paths**

   a) (6%) Go through the handout on *traceroute* (*traceroute* on Unix and *tracert* on Windows). In addition to running traceroute from your own machine, you can gather traceroute results launched from different sites by using ***www.traceroute.org***.

   Collect traces for *two* different source-destination pairs (choose some symmetric paths as well). For each path, collect results at three or more different hours of the day. Present the results in suitable form. You can be creative here. Comment on:

   - Average and standard deviation of the round-trip delays for each path.
   - Number of routers in the path for each measurement. Did the paths change during any of the hours?
   - Number of ISP networks that traceroute packets pass through from source to destination. Routers with similar names and/or similar IP addresses could be considered as part of the same ISP.

   b) (6%) Now, repeat (a) for a *mobile device*, e.g., your laptop or PDA. First, associate your laptop or PDA to a wireless LAN. Use traceroute to discover the routing path from the mobile node to a server at ***www.traceroute.org*****.** Repeat the experiments by launching traceroute from the server to your mobile node. Now switch your mobile node to another wireless network. Repeat the traceroute experiments from and to your mobile node. What is the data path that is returned? Is routing optimization being performed? How can you tell?

4. **Investigate the flaw in WEP (Bonus - 10%)**

   Due to certain vulnerability of WEP, programs like Airsnort (http://airsnort.shmoo.com) can be used to crack a WEP key given enough data.

   - How much data must be captured?
   - Estimate how long it would take to gather that data if the user did one FTP download of 255 Kbytes every hour. What does this say about how often you should change the WEP key on your home network?