

CSE370 Spring 2007 Wireless and mobile networking

Midterm Solution

1. **CDMA.** (7pts) Consider a Direct Sequence CDMA system where user i uses the i th row of the following Hadamard matrix as its chipping sequence:

$$\begin{pmatrix} +1 & +1 & +1 & +1 \\ +1 & -1 & +1 & -1 \\ +1 & +1 & -1 & -1 \\ +1 & -1 & -1 & +1 \end{pmatrix}$$

Assume that user 1 and 3 are transmitting simultaneously:

user 1 data sequence: +1 -1 -1 +1

user 3 data sequence: +1 +1 -1 -1

(For this problem we will use the vector representation. Essentially a data bit of 1 is represented by +1 and a data bit of 0 is represented by -1.)

- (a) (2pts) Show the signal sent by each user and the signal received at the receivers.

Answer:

User 1: +1 +1 +1 +1 -1 -1 -1 -1 -1 -1 -1 -1 +1 +1 +1 +1

User 3: +1 +1 -1 -1 +1 +1 -1 -1 -1 -1 +1 +1 -1 -1 +1 +1

Received signal: +2 +2 0 0 0 0 -2 -2 -2 -2 0 0 0 0 2 2

- (b) (2pts) Assume that the receiver wants to extract information from user 3. Show how this is done.

Answer: Take the received signal and take dot product with the chipping sequence of user 3 for each consecutive 4 bits. This will arrive at:

$$4, 4, -4, -4.$$

Each positive number is considered as 1 and each negative number is considered as 0. Thus the data sent by user 3 is recovered as 1100.

(c) (1pts) How many error bits can be tolerated?

Answer: 1 bit.

(d) (2pts) Can there be interference if all 4 users transmit simultaneously? Why?

Answer: No. Each pair of the chipping sequence is orthogonal to each other, i.e., their dot product is 0. So the data sent by other users will be canceled out.

2. Mobile IP (7pts)

(a) (2pts) Explain what is tunneling in Mobile IP.

Answer: The packets addressed to the mobile node will be intercepted by the home agent. The home agent encapsulates the packet by putting another IP header ahead of it. The new IP header has source as the IP of home agent and destination as the IP of the foreign agent. This packet is delivered by the IP protocol as usual. The foreign agent decapsulates the packet and delivers it to the mobile node.

(b) (2pts) What are the advantages and disadvantages of tunneling in Mobile IP?

Answer:

Advantage: the mobile node does not change its IP address. This is a minimalist approach to incorporate mobility in the current Internet.

Disadvantage: this introduces triangular routing, thus extra delay and routing inefficiency. It may potentially cause security problems.

(c) (3pt) What is reverse tunneling? Give one reason for reverse tunneling.

Answer: Reverse tunneling means packets from mobile node is also tunneled by the foreign agent to the home agent. Here are two reasons. First, the mobile nodes is holding the IP address of the home network. Thus it is not topologically correct in the foreign network. Many networks use firewalls for security purposes. Thus packets from a topologically incorrect address can be blocked at the firewall. Second, a packet carries a TTL (Time-to-live) to avoid routing loops. If the home network is much closer to the correspondent node. The TTL is too small that packets from the mobile node at the foreign network can not reach the

destination. By using reverse tunneling the entire path through the tunnel is considered as one hop. Thus TTL is only reduced by 1.

3. **CSMA** (5pts) In CSMA (Carrier Sense Multiple Access) for wireless networks, why can there still be collision even if a sender sensed an idle channel? (2pts) How to resolve this? (3pts)

Answer: This is because of the hidden terminal problem. The sender A may sense an idle channel but the receiver B is receiving packets from another sender C that is outside the transmission range of A. Thus A will send a packet and this causes collision at the receiver B.

The way to avoid this is by introducing RTS/CTS scheme. The sender sends a RTS (Request to Send) to the receiver. The receiver returns CTS (Clear to Send) if it detects an idle channel. The sender will send after it receives the confirmation CTS from the receiver. This way we put the control and carrier sense at the receiver side, for which we truly care.

4. **Coding** (6pts) Suppose we are using Reed Solomon code for wireless communication through a channel of capacity 56K (this means each second one can send through 56,000 bits). The adversary uses a one-time jammer and is able to jam the channel for up to 2 milliseconds (1 millisecond= 10^{-3} second). Now we have a password we want to send through this channel. This password is a sequence of 7 numbers. Each number is represented by 8-bits. Explain briefly how to use Reed Solomon code to successfully deliver this password. (3pts) And how long does it take. (3pts)

Answer: The adversary can destroy at most $56000 \times 0.002 = 112$ consecutive bits. This translates to 14 bytes. The password is encoded by Reed Solomon code into $14 + 7$ bytes such that at least 7 bytes can survive the jamming. Thus the receiver can decode the original 7 passwords with the 7 numbers received successfully. The time used for transmission is $21 \times 8 / 56,000 = 3$ milliseconds.

5. **Extra credit problem.** (5pts) The Hamming code (7, 4) takes a string of length 4 and outputs a codeword of length 7. This is by

taking the multiplication of the input string with the encoding matrix:

$$H = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix}$$

For example, an input string $x = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}$ will be encoded to

$$Hx = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \end{pmatrix}$$

Here sum is in fact XOR (i.e., sum with mod 2). The question is, how many flip errors can be detected by this code?

Answer: As can be verified that the minimum Hamming distance of the codewords is 3. Thus this code can be used to detect 2 bits flip error and can correct 1 bit error.
