CSE/EE 461 Homework 1

Due 6pm, Friday, January 21, 2000.

1. Interplanetary Networking

Vint Cert and others have begun exploring the technical issues that arise in an Interplanetary Internet. (Seriously!) Consider the path between the Earth and Mars. The planets are 78.39 x 10^9 m apart (mean distance). The speed of light is 3 x 10^8 m/s in space. You may assume that we can successfully send and receive data along this path at 1 Gbps (10^9 bits per second). In your answers to the following questions, describe each calculation.

a) How long will it take to send a short message from Earth to Mars and receive a short reply?

b) How long will it take to send a large gigabyte file from Earth to Mars and receive a short reply?

c) How long is a bit while in transit between the Earth and Mars?

d) How much data could be in transit from Earth to Mars at any given time?

2. Framing Overhead

Practical byte stuffing algorithms are slightly more complicated than we discussed in class because of the need to distinguish between back-to-back frames. Consider the following two schemes.

PPP Here, the byte 0x7E is added at the sender to mark the end of the previous packet and the beginning of the current one. Within the payload, the sender replaces 0x7E with 0x7D, 0x5E. Occurances of 0x7D must also be escaped; they are replaced with 0x7D, 0x5D. At the receiver, 0x7D and the following byte are replaced with one byte which is the XOR of the second byte with 0x20. Thus 0x7D, 0x5D is replaced with a single 0x7D and 0x7D, 0x5E with a single 0x7E, reversing the process.

COBS Here, the byte 0x00 (that is, zero) is added at the sender to mark the end of the previous packet and the beginning of the current packet. Zeros must now be removed from the payload. First, a start byte is added to indicate the number of bytes until a zero is encountered. That zero is replaced with the number of bytes until the next zero, and so forth until the end of the packet. To handle the last zero in the packet, we pretend that there is an extra zero just off the end of the real packet. For example, the packet 0x22, 0x00, 0x00, 0x55 becomes 0x00, 0x02, 0x22, 0x01, 0x02, 0x55. We must also handle the situation in which there are no zeros in the payload. To do this we use 0xFF to indicate a run of 254 consecutive non-zero bytes without a following zero; after the 254 bytes there is a count of bytes until a zero or a another 0xFF. At the receiver the reverse process is performed.

a) What is the worst case expansion of a packet of length L using PPP and COBS? In what scenario do these worst cases occur?

b) What is the best case expansion of a packet of length L using PPP and COBS? In what scenario do these best cases occur?

c) Your answers above should show that COBS gives good all round performance. Despite this, give one reason why we might prefer PPP to COBS.

3. Properties of 2D Parity

Consider a 2D parity code in which a block of *n x n* bits has added to it one row of parity bits and one column of parity bits. See example below.

1010 …… 010 1
0010 …… 101 0
:
:
1100 ……. 111 1

1001 ……. 001 0

Fig 1. This is *(n+1) x (n+1)* matrix. The upper-leftmost block of n x n bits are the data bits. The *(n+1)th* column is the parity column and the *(n+1)th* row is the parity row.

We are interested in the protection that this code gives against burst errors. For this purpose, we define a burst error of length *b* to be a sequence of consecutive bits in which the first, last and any number of middle bits (but not necessarily all) are in error. You can further assume that the 2D block is transmitted in left to right, top to bottom fashion. In your answers below, do NOT rely on the known properties of 2D parity with respect to random errors; derive any results on which you rely. You may rely on the properties of single bit parity, which detects an odd number of errors in either the data or parity bit.

a) What lengths of burst error will always be detected? Explain with a concise, logical argument.

b) What lengths of burst error will only sometimes be detected? Again, explain.

c) What lengths of burst error can be corrected? Explain.

4. Ethernet

Consider a classic Ethernet in which all hosts are connected to the same shared cable and run the CSMA/CD algorithm.

a) Why is a minimum packet size needed? Describe what would go wrong if it were possible to send packets shorter than the allowed minimum.

b) Give a formula that shows the required minimum packet length in terms of physical Ethernet parameters, such as distance (D), bit rate (R) and propagation speed (S). Explain how you derived this formula.