Comp 7005 – Data Communication Principles

Assignment Two – October, 2009

Due Date: 1730 hrs - Tuesday, October 20, 2009

Criteria: You may work in groups of two. Assignments must be word-processed and submitted by the date and time specified above.

Note: Clearly state any assumptions that you make in the solution of any of the questions. Substantiate your answers and show all your work for each problem – the answer alone is insufficient to receive credit for the question.

Chapter 1: P5, P16, P24

Problem 5

a) $d_{prop} = \frac{m}{s} seconds$

b) $d_{prop} = \frac{L}{R} seconds$

c) $d_{end-to-end} = \left(\frac{m}{s} + \frac{L}{R} \right) \text{sec}onds$

d) The bit is just leaving Host A.
e) The first bit is in the link and has not reached Host B.
f) The first bit has reached Host B.
g) Distance is:

$$m = \frac{L}{R} S = \frac{100}{28 \times 10^3} \left(2.5 \times 10^8 \right) = 893 Km$$

Problem 16

Answers will vary depending on which site you picked. For example the following command:

```
traceroute -q 20 www.eurecom.fr
```

will get 20 delay measurements from the issuing host to the host, www.eurecom.fr. The
average and standard deviation of these 20 measurements can then be collected. You should also see differences in your answers at different times of the day.

Problem 24

a) Time to send message from source host to first packet switch:

$$\frac{7.5\times10^6}{1.5\times10^6}\,sec = 5sec$$

With store-and-forward switching, the total time to move message from source host to destination host = 5sec×3 *hops* = 15sec

b) Time to send 1st packet from source host to first packet switch:

$$\frac{1.5\times10^3}{1.5\times10^6}\,sec = 1msec$$

Time at which 2nd packet is received at the first switch =
time at which 1st packet is received at the second switch = 2×1*m*sec = 2
*m*sec

c) Time at which 1st packet is received at the destination host = .
1*m*sec× 3 *hops* = 3 *m*sec .

After this, every 1msec one packet will be received; thus time at which last
(5000th) packet is received = 3 *m*sec+ 4999*1*m*sec = 5.002sec .
It can be seen that delay in using message segmentation is significantly
less (almost 1/3rd).

d) Drawbacks:
i. Packets have to be put in sequence at the destination.
ii. Message segmentation results in many smaller packets.

Since
header size is usually the same for all packets regardless of their
size, with message segmentation the total amount of header bytes
is more.

Chapter 2: P3, P9

Problem 3

Application layer protocols: DNS and HTTP
Transport layer protocols: UDP for DNS; TCP for HTTP

Problem 9

a) The time to transmit an object of size L over a link or rate R is L/R. The average time
is the average size of the object divided by R:

Δ= (900,000 bits)/(1,500,000 bits/sec) = .6 sec

The traffic intensity on the link is (1.5 requests/sec)(.6 msec/request) = .9. Thus, the average access delay is (.6 sec)/(1 - .9) = 6 seconds. The total average response time is therefore 6 sec + 2 sec = 8 sec.

b) The traffic intensity on the access link is reduced by 40% since the 40% of the
requests are satisfied within the institutional network. Thus the average access delay is (.6 sec)/[1 – (.6)(.9)] = 1.2 seconds. The response time is approximately zero if the request is satisfied by the cache (which happens with probability .4); the average response time is 1.2 sec + 2 sec = 3.2 sec for cache misses (which happens 60% of the time). So the average response time is (.4)(0 sec) + (.6)(3.2 sec) = 1.92 seconds. Thus the average response time is reduced from 8 sec to 1.92 sec.

Chapter 3: P2, P3, P7, P9, P13, P14, P23, P24, P33, P41

Problem 2

Suppose the IP addresses of the hosts A, B, and C are a, b, c, respectively. (Note that
a,b,c are distinct.)

To host A: Source port =80, source IP address = b, dest port = 26145, dest IP address = a

To host C, left process: Source port =80, source IP address = b, dest port = 7532, dest IP
address = c

To host C, right process: Source port =80, source IP address = b, dest port = 26145, dest
IP address = c

Problem 3

```
 1 1 0 0 0 1 0 1
+  0 1 1 1 0 0 0 0

 0 1 0 1 0 1 0 1


 0 0 0 1 0 0 0 1
+ 0 1 0 0 1 1 0 0

 1 1 0 0 0 1 0 1
```

One's complement = 1 1 1 0 1 1 1 0.

To detect errors, the receiver adds the four words (the three original words and the checksum). If the sum contains a zero, the receiver knows there has been an error. All one-bit errors will be detected, but two-bit errors can be undetected (e.g., if the last digit of the first word is converted to a 0 and the last digit of the second word is converted to a 1).

Problem 7

To best answer this question, consider why we needed sequence numbers in the first place. We saw that the sender needs sequence numbers so that the receiver can tell if a data packet is a duplicate of an already received data packet. In the case of ACKs, the sender does not need this info (i.e., a sequence number on an ACK) to tell detect a duplicate ACK.

A duplicate ACK is obvious to the rdt3.0 receiver, since when it has received the original ACK it transitioned to the next state. The duplicate ACK is not the ACK that the sender needs and hence is ignored by the rdt3.0 sender.

Problem 9

Suppose the protocol has been in operation for some time. The sender is in state “Wait for call from above” (top left hand corner) and the receiver is in state “Wait for 0 from below”. The scenarios for corrupted data and corrupted ACK are shown in Figure 1.

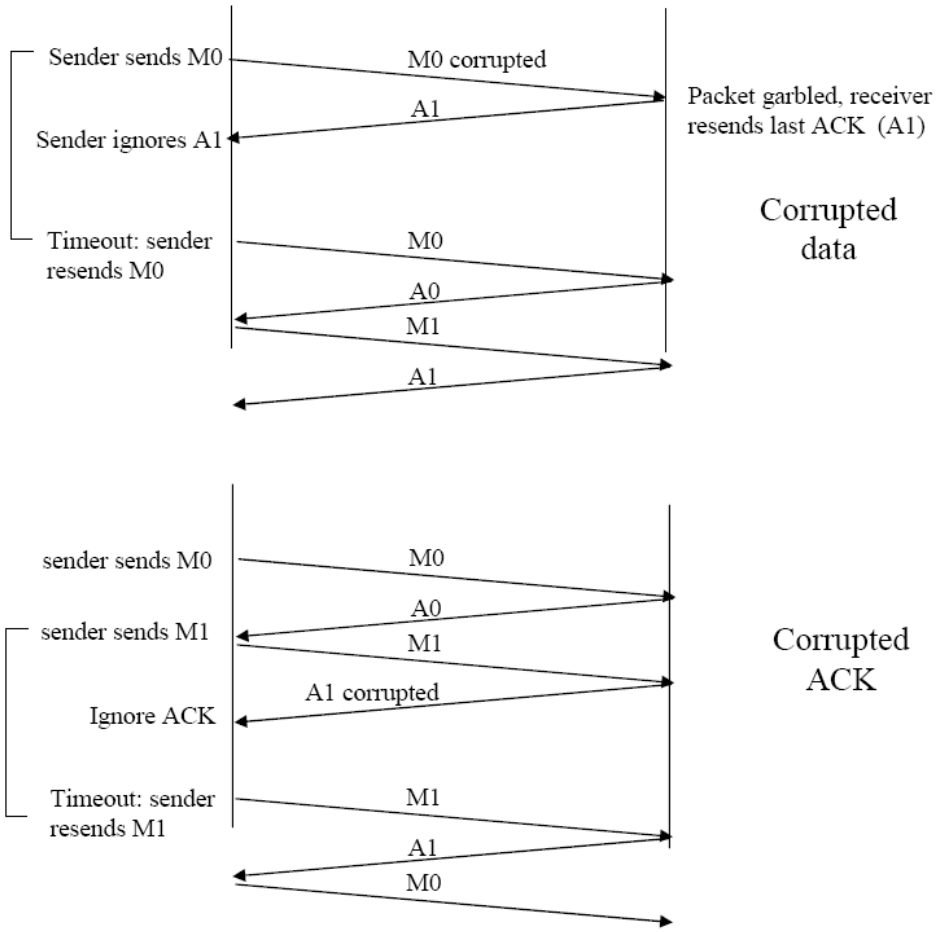


Figure 1: rdt 3.0 scenarios: corrupted data, corrupted ACK

Problem 13

In a NAK only protocol, the loss of packet *x* is only detected by the receiver when packet *x+1* is received. That is, the receivers receives *x-1* and then *x+1*, only when *x+1 is* received does the receiver realize that *x* was missed. If there is a long delay between the transmission of x and

the transmission of $x+1$, then it will be a long time until x can be recovered, under a NAK only protocol.

On the other hand, if data is being sent often, then recovery under a NAK-only scheme could happen quickly. Moreover, if errors are infrequent, then NAKs are only occasionally sent (when needed), and ACK are never sent – a significant reduction in feedback in the NAK-only case over the ACK-only case.

Problem 14

It takes 8 microseconds (or 0.008 milliseconds) to send a packet. In order for the sender
to be busy 90 percent of the time, we must have

$$util = 0.9 = (0.008n) / 30.016$$

or n approximately 3377 packets.

Problem 23

There are $2^{32} = 4{,}294{,}967{,}296$ possible sequence numbers.

a) The sequence number does not increment by one with each segment. Rather, is
increments by the number of bytes of data sent. So the size of the MSS is irrelevant – the maximum size file that can be sent from A to B is simply the number of bytes representable by 2^{32} = 4.29 Gbytes .

b) The number of segments is

66 bytes of header get added to each segment giving a total of 194,156,028 bytes of header. The total number of bytes transmitted is 2^{32} + 194,156,028 = $3{,}591 \times 10^7$ bits.

Thus it would take 3,591 seconds = 59 minutes to transmit the file over a 10~Mbps link.

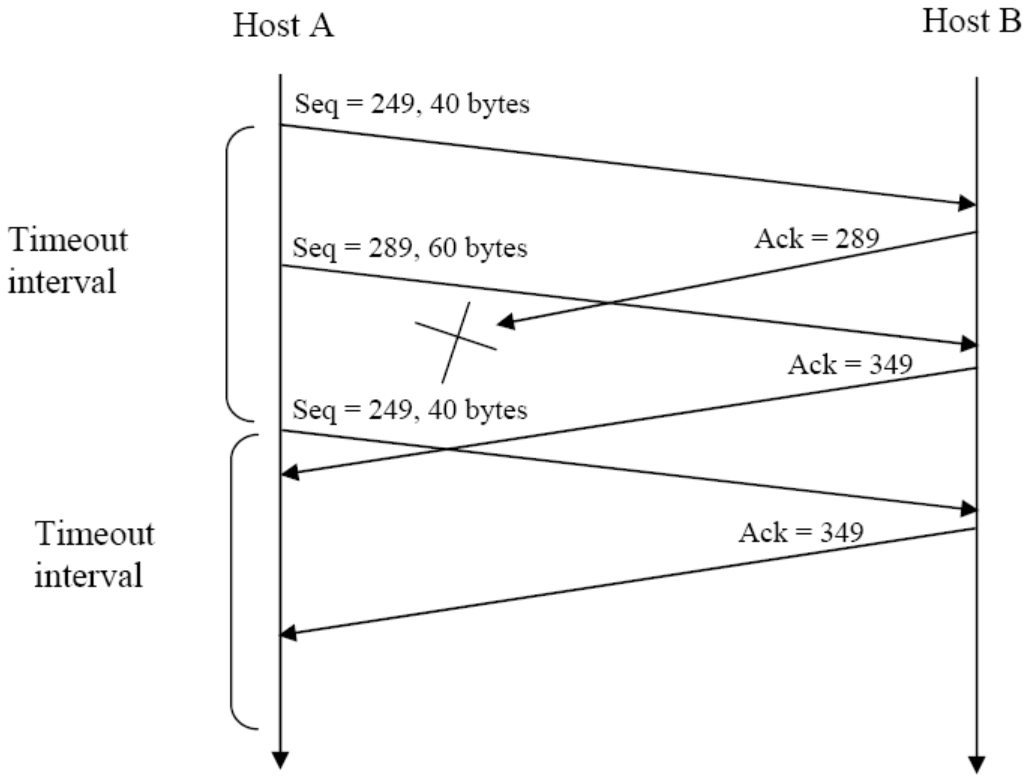
Problem 24

a. In the second segment from Host A to B, the sequence number is 289,
source port number is 503 and destination port number is 80.

b. If the first segment arrives before the second, in the acknowledgement of
the first arriving segment, the acknowledgement number is 289, the source
port number is 80 and the destination port number is 503.

c. If the second segment arrives before the first segment, in the acknowledgement of the first arriving segment, the acknowledgement number is 249, indicating that it is still waiting for bytes 249 and onwards.

d.



Problem 33

a) TCP slowstart is operating in the intervals [1,6] and [23,26]

b) TCP congestion advoidance is operating in the intervals [6,16] and [17,22]

c) After the 16th transmission round, packet loss is recognized by a triple duplicate ACK. If there was a timeout, the congestion window size would have dropped to 1.

d) After the 22nd transmission round, segment loss is detected due to timeout, and hence the congestion window size is set to 1.

e) The threshold is initially 32, since it is at this window size that slowtart stops and congestion avoidance begins.

f) The threshold is set to half the value of the congestion window when packet loss is detected. When loss is detected during transmission round 16, the congestion windows size is 42. Hence the threshold is 21 during the 18th transmission round.

g) The threshold is set to half the value of the congestion window when packet loss is detected. When loss is detected during transmission round 16, the congestion windows size is 42. Hence the threshold is 21 during the 18th transmission round.

h) During the 1st transmission round, packet 1 is sent; packet 2-3 are sent in the 2nd transmission round; packets 4-7 are sent in the 3rd transmission round; packets 8-15 are sent in the 4th transmission round; packets15-31 are sent in the 5th transmission round; packets 32-63 are sent in the 6th transmission round; packets 64 – 96 are sent in the 7th transmission round. Thus packet 70 is sent in the 7th transmission round.

i) The congestion window and threshold will be set to half the current value of the
congestion window (8) when the loss occurred. Thus the new values of the
threshold and window will be 4.

Problem 41

a) The server will send its response to Y.

b) No. In this case, if the client spoofs its IP to Y, she cannot complete the three-way handshake with the server and so no further responses will be sent from the server to the spoofed address Y.

c) The server can be certain that the client is indeed at Y. If it were at some other address spoofing Y, the SYNACK would have been sent to the address Y, and the TCP in that host would not send the TCP ACK segment back. Even if the attacker were to send an appropriately timed TCP ACK segment, it would not know the correct server sequence number (since the server uses random initial sequence numbers.)