CSC3371 - COMPUTER COMMUNICATIONS and NETWORKS

Midterm Test

STUDENT NAME	STUDENT ID NO

Question-1

Explain the operation principles of CSMA protocol.

[20 Marks]

Answers to Question-3:

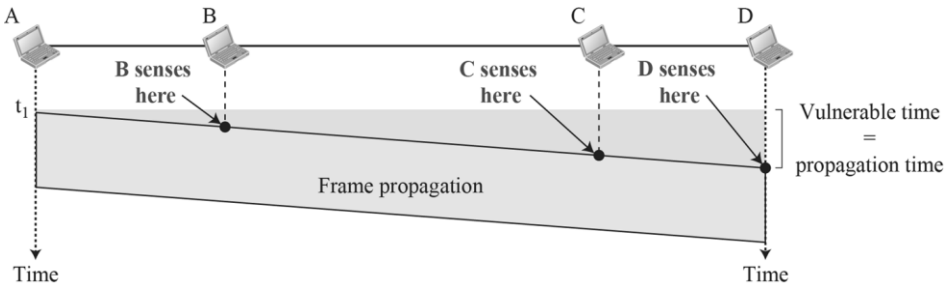
In order to minimize the chance of collision and to increase the performance, the CSMA method was developed. In Carrier sensing: means stations first listen to the channel or the medium to check whether it is busy or idle. Before they send something on it. Multiple access means that more than one device is trying to access the same medium.

So, there is a competition to access the channel.

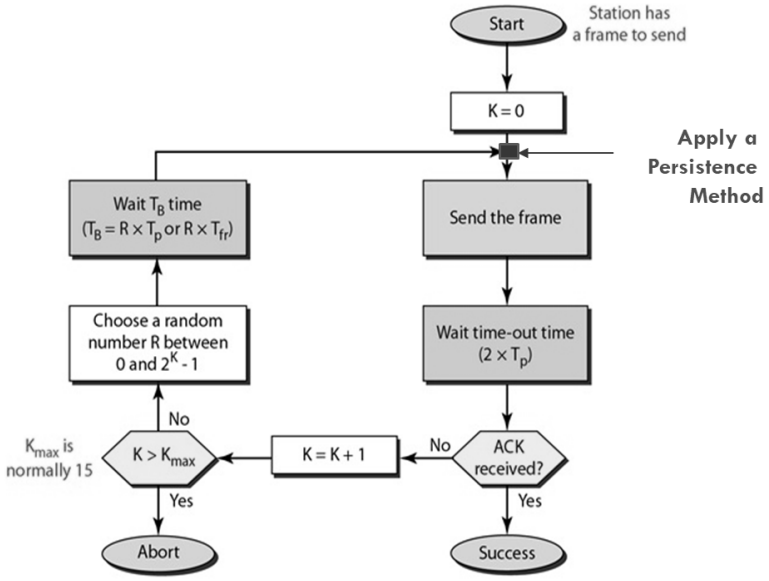
- Carrier sensing
- Stations first listen to the medium
- to determine if another transmission is in progress (carrier sense)
- Multiple access

A persistence method is applied

Vulnerable Time in CSMA



In order to reduce the possibility of collision, Persistence methods are used. So, when a station finds that the channel busy, it applies one of the persistence methods: there are three common persistence methods: 1-persistent method, nonpersistent method, and p-persistent method.



CSMA Protocol Flow diagram

Question-2

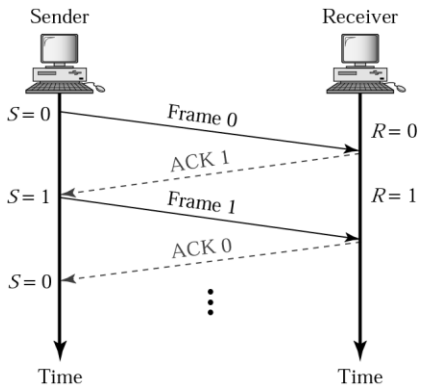
With the help of block diagrams explain Stop and Wait and Sliding Window flow control protocols

[20 Marks]

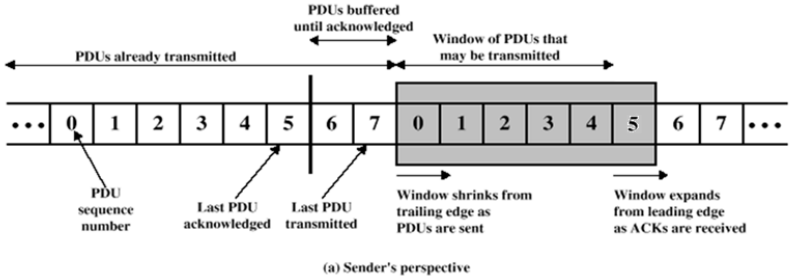
Answers to Question-2:

Both data frames and acknowledgement (ACK) frames are numbered alternately 0 and 1.

A data frame 0 is acknowledged by an ACK 1 frame.



The shaded rectangle indicates that the sender may transmit 6 frames, beginning with frame 0. The window expands to include new unsent frames when the correct acknowledgements are received.



Question-3

A transmitter and a receiver have agreed to use a generator with divisor: 1001. Suppose that the receiver has received the following frame: 11001001010. Compute the CRC frame check sequence for the received data-stream and state whether the receiver should accept or reject the received frame.

[20 Marks]

Answers to Question-3:

The CRC frame check sequence is 0001, the frame should be rejected

```
1 1 0 0 1 0 0 1 0 1 0 | 1 0 0 1
1 0 0 1               | 1 1 0 1 0 0 1 1
0 1 0 1 1             |
  1 0 0 1             |
  0 0 1 0 0 0         |
      1 0 0 1         |
      0 0 0 1 1 0 1   |
            1 0 0 1   |
            0 1 0 0 0 |
              1 0 0 1 |
              0 0 0 1 |
```

The remainder is not equal to zero, hence the packet should be rejected.

Question-4

With the help of block diagram explain the operation principle of Pure Aloha protocol

[20 Marks]

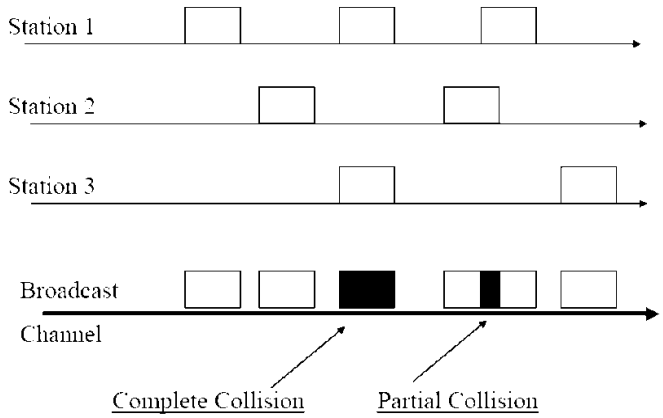
Answers to Question-4:

Pure Aloha medium access control protocol

Developed at the University of Hawaii for packet radio network.

When station has frame, it sends, then monitors the signal sent by the central station for a bit over max round trip time waiting for an acknowledgement, if it does not receive an acknowledgement, it assumes that the frame is lost, then it tries sending again after a random amount of time.

Collision in Pure ALOHA



Vulnerable period: 2X

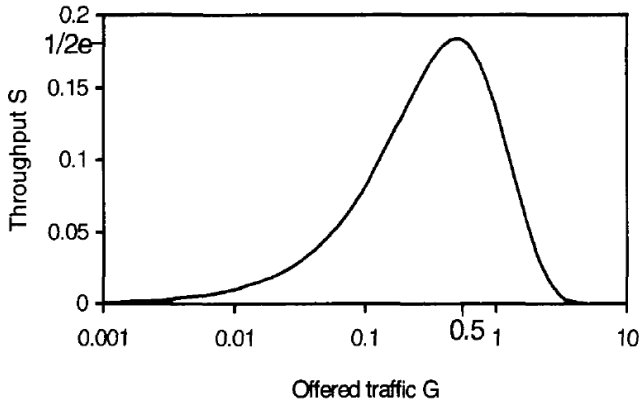
Probability of no other packet generated during the vulnerable period is:

Pr{a successful transmission} = Pr{no arrivals in X seconds before the reference packet} × Pr {no arrivals in X seconds after the reference packet} = $e^{-AX} \times e^{-AX}$

$= e^{-2AX} = e^{-2G} = S/G$

Hence the throughput $S = G\, e^{-2G}$

Throughput Versus Offered Traffic for Aloha



Question-4

(a) Consider a data communication channel using Pure Aloha medium access control protocol, whereby 500 kbps is shared among certain number of stations. Each station will send a 1300-byte frame on average every 4 seconds. Find the maximum number of stations that this data communication system can support.

[10 Marks]

Answers to Question-5:

The average amount of data each station is transmitting:

$1300 \times 8 = 10400$ bits

10400/4= 2600 bits/second

Max channel bandwidth for pure ALOHA is 18.2% of channel bandwidth:

500 kbps $\times$ 18.2% = 91000 bps

91000/ 2600 = 35 stations. The maximum number of stations is 35

(b) Suppose that an initial IP datagram containing 3824 bytes of data is divided into 2 fragments with an MTU of 1460 bytes each, whereby the rest of the datagram was subject to additional fragmentation required by the X.25 IP network router. Fill in the following table and explain your answer.

[10 Marks]

Answers to Question-3:

Table

Header field	Datagram	Fragment 1	Fragment 2	Fragment 3-1	Fragment 3-2
Header length	**15**	**15**	**15**	**15**	**15**
Total length	**3,884**	**1460**	**1460**	**572**	**572**
Identification	**111111**	**111111**	**111111**	**111111**	**111111**
MF	**0**	**1**	**1**	**1**	**0**
Fragment offset	**0**	**0**	**175**	**350**	**414**

Analysis: the MTU X.25 is 576. So, 576-60=516 bytes.
516 is not the multiple of 8, thus set data length to 512 break 1023 into 512+511. Therefore 2 fragments. The bytes in the original datagram are numbered 0 to 3823.

- The header length is 15 bytes but measured in units of 4 bytes.
- Identification number: 111111, is the same in all fragments to indicate that they belong to the same original datagram.
- Fragment offset indicates where the fragment's data belongs in the original datagram measured in units of 8 bytes.
- MF bit (0 = "last fragment," 1 = "more fragments").

1400 bytes.

0 ……1399 Offset: 0/8=0

1400 bytes

1400 ……2799 Offset: 1400/8=175

512 bytes

2800 …… 3311 Offset: 2800/8= 350

512 bytes

3312 ……3823 Offset: 3312/8=414